European Center for
Not-for-Profit Law

IRAN: DIGITAL SPACES OF PROTEST AND CONTROL

PILOTING REPORT ON THE GUIDE ON DIGITALLY-MEDIATED ASSEMBLIES

Dr Azadeh Akbari

30 November 2022

European Center for
Not-for-Profit Law

European Center for Not-for-Profit Law Stichting
5 Riviervismarkt, 2513 AM The Hague, Netherlands
www.ecnl.org twitter.com/enablingNGOlaw

About the author:
Dr Azadeh Akbari is Assistant Professor in Public Administration and Digital Transformation at the University of Twente, the Netherlands. She has been a journalist, feminist activist, and UN employee in Iran. Azadeh Akbari is the co-director of the Surveillance Studies Network and the founder of Surveillance in the Global South research network. She is co-editing two books, Critical ICTs for Development and Handbook of Critical Surveillance Studies. Her current research focuses on authoritarian smart cities.

This is a piloting report based on the Guide on digitally-mediated assemblies and how to monitor them, published by the European Center for Not-for-Profit Law Stichting (ECNL).

30 November 2022

Sweden
Sverige

ICNL
INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW

This report was developed as part of the "Strengthening Standards and Implementation of the Rights to Association and Assembly" 'project, managed by ECNL. The project is made possible by the International Center for Not-for-Profit Law (ICNL) through the Civic Space Initiative. This report is wholly financed by the Government of Sweden. The Government of Sweden does not necessarily share opinions here within expressed. The author bears the sole responsibility for the content.

Cover illustration by ECNL.

CONTENTS

SUMMARY

- Freedom of assembly and freedom of expression have a twofold relationship. They co-construct the possibility for different socio-political movements to communicate their objectives, mobilise the public or their networks, and make decisions in digitally-mediated spaces. Therefore, digitally-mediated assemblies are also likely to be controlled, surveilled, or banned in an environment of censorship.
- Freedom of assembly in digitally-mediated spaces is situated in a matrix of variables such as the degree of planning (spontaneous, contingent, or planned), the participants' connectedness (individuals, networks, or communities), assembly's objective (communication, mobilisation, decision-making), and issues of access to cyberspaces and the digital divide (open unlimited access, partial access, controlled/blocked access). These factors play a vital role in understanding the pragmatic aspects of how digitally-mediated assemblies are organised and run and if they can have a representative function.
- In an authoritarian system of (internet) governance such as Iran, the government disrupts the right to freedom of expression and digitally-mediated assemblies on many levels:

    1. at the infrastructural level, through the development of National Internet Network, internet shutdowns, controlling the bandwidth, etc.;
    2. at the interactive level through interceptive and surveillance technologies;
    3. at the intra-spatial level between the physical and the cyberspace, by extending oppressive measures to acts of resistance in the digital space.

INTRODUCTION

On 16 September 2022, Mahsa Jina Amini, a 22-year-old Iranian of Kurdish origin, died three days after being arrested and beaten by the Iranian moral police for breaching the Islamic dress code for women. Her murder prompted widespread protests across Iran with the slogan "woman, life, freedom." According to the United Nations experts[1] (stand 12 Nov 2022), at least 304 people were killed during the protests, including 41 children. Thousands of people have been arrested, including 51 journalists. The severity of the situation led to the establishment of a fact-finding mission by the Human Rights Council following calls from the UN human rights chief for an "independent investigation into ongoing deadly violence against protesters in Iran"[2].

From the first days of the protests, Mahsa Amini's name became the leading hashtag on all social media platforms. Her name became the emblem of a women-led movement (Figure 1) that protested against decades of oppression against women and soon spread to all areas of injustice and turned to a revolution for regime change. Parallel to the nationwide demonstrations on the streets, cyberspace has played a vital role in helping protesters communicate, mobilise, and extend their networks of resistance to the larger Iranian diaspora communities. For this reason, the Iranian regime has long used different methods of digital suppression.
The following section describes a repository of such measures summarily.

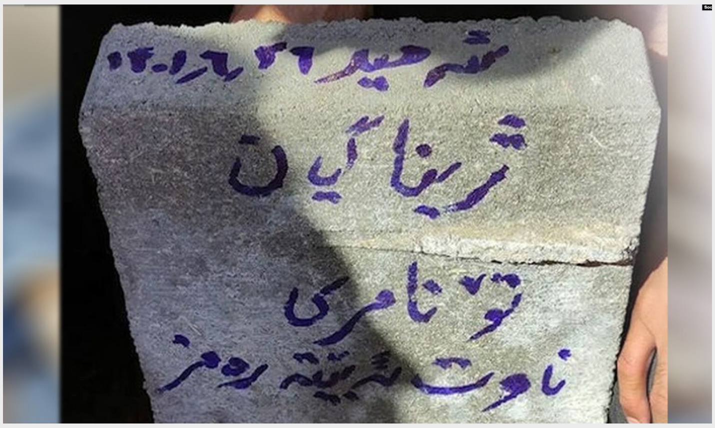


Figure 1. Mahsa Jina Amini's Tombstone:
"Dear Jina, You will never die, Your name becomes our emblem."

[1] https://www.ohchr.org/en/press-releases/2022/11/iran-stop-sentencing-peaceful-protesters-death-say-un-experts

[2] https://news.un.org/en/story/2022/11/1131022

Digital Governance in Iran

Access to the internet was restricted to specific groups or had controlled features from its arrival in Iran.

Iran has always been exemplified as one of the world's most closed systems of internet governance. Reporters Without Borders ranked Iran as one of the 15 enemies of the internet[3]. However, this animosity is hard to grasp when one looks at the massive budget spent every year by the Iranian ICT ministry to expand the internet infrastructure to the remotest villages in the country[4]. Access to the internet was restricted to specific groups or had controlled features from its arrival in Iran. The Institute for Studies in Theoretical Physics and Mathematics launched the first internet connection in the country in 1993 for academic and scientific purposes[5]. A year later, private internet use outside universities and research institutes was allowed. Until the controversial student uprisings in 1999, the few who could afford an internet connection enjoyed relative freedom that was never to experience again. The uprising showcased the mobilising power of the new discussion spaces on the internet. In response, the Supreme Leader issued a decree regarding general policies of information and computing networks in the same year[6]. This marked the beginning of the organised filtering of internet websites in the country.

In 2001 the Supreme Council for Cultural Revolution, the newly appointed regulator for internet content, ruled that all internet service providers (ISP) should be placed under state control and remove anti-government and anti-Islamic sites from their servers[5]. Subsequently, the Council for Cultural Revolution started to send lists of designated websites for filtering to the ISPs regularly. The controlling effect soon approached the users' activity. In 2002, the Iranian Parliament ratified a law that provided principles to determine criminal internet activities[7], including sharing classified secrets, fraud, hacking, privacy, and pornography; also forbidding any insults against the Supreme Leader and high-ranking officials. In 2006 and during the conservative government of President Ahmadinejad, all Iranian

[3] Reporters without Borders. The 15 enemies of the internet and other countries to watch, https://rsf.org/en/news/15-enemies-internet-and-other-countries-watch (25/1/2016) last accessed 2019/8/7.

[4] Mehr News Agency: ICT Ministry's Budget Estimated 3,753 Billion Tooman, https://bit.ly/355jtWJ (2018/12/22), last accessed 2019/10/5.

[5] Rahimi, B.: Cyberdissent: The internet in revolutionary Iran. Middle East Review of International Affairs 7(3), (2003)

[6] Golkar, S.: Liberation or suppression technologies? The internet, the green movement and the regime in Iran. International Journal of Emerging Technologies and Society 9(1), 50-70 (2011).

[7] International Campaign for Human Rights in Iran. internet in chains: The front line of state repression in Iran, https://www.iranhumanrights.org/wp-content/uploads/Internet_report-En.pdf (2014) last accessed 2019/10/6.

websites were required to register at the Ministry of Culture and Islamic Guidance; otherwise, their activity would be forcefully ceased[8].

Eventually, to bring all scattered surveillance institutions under one umbrella, especially considering the decisive role of social media in the nationwide uprisings of 2009, the Iranian Parliament ratified the Computer Crimes Law and established the Working Group to Determine the Instances of Criminal Content in 2009[9]. To tighten his grip on general policies regarding internet governance, the Supreme Leader commanded the establishment of the Supreme Council of Cyberspace in 2012[10], responsible for general policies regarding cyberspace with seven members directly appointed by him in addition to other institutional members. The duties of the Working Group to Determine the Instances of Criminal Content and the Supreme Council of Cyberspace are immensely similar. Therefore, some have diagnosed an "institutional chaos" in internet governance in Iran[11]. Others have argued that such strategic overlaps keep the liabilities of each body in a blurry zone[12]. Additionally, "technical assessments of internet censorship in Iran have unanimously reported that there seems to be a central censorship node on a national level"[13].

National Internet Network

In addition to all the aforementioned restrictions on the content and access to the internet, the 2009 uprising in Iran, which took the state months to suppress, made speculations of launching a "Halal Internet"[14] bordering reality in 2011. The idea of setting up a network with access and content tailored to the ideological preferences of the Iranian state evolved to become the National Information Network (NIN).

[8] About Us: The Center for Regulating Content in the Cyberspace. https://samandehi.ir/SitePages/Info.aspx (last accessed 2019/10/6)

[9] BBC Persian. Distribution of anti-filtering and internet links are forbidden, http://www.bbc.com/persian/iran/2009/12/091229_ka_internet_iran.shtml (2009/12/29), last accessed 2019/10/5.

[10] National Cyberspace Centre. Decree to establish the Supreme Council of Cyberspace, https://bit.ly/2AY9OUp (2012/3/7), last accessed 2019/10/5.

[11] Robertson, B., Marchant, J. (eds.). Revolution decoded: Iran's digital landscape, https://smallmedia.org.uk/revolutiondecoded/ (2014) last accessed 2019/10/5.

[12] Akbari, A.: Follow the thing: Data. Antipode, 52(2), 408-429 (2020).

[13] Aryan, S., Aryan, H., Halderman, A.: internet censorship in Iran: A first look. 3rd USENIX Workshop on Free and Open Communications on the internet (FOCI '13), https://www.usenix.org/system/files/conference/foci13/foci13-aryan.pdf (2013).

[14] Gambrell, J.: 'Halal' internet means more control in Iran after unrest. AP, https://www.apnews.com/c02a320725fc4afda305a0f3a660dbe6 (2018), last accessed 2019/8/7.

NIN is a state-controlled network that acts as a passageway to the global internet while providing services such as email accounts and search engines on a local level. The network, therefore, divides access to the internet into one internal and one international space. The ability to separate international from national traffic was first manifested on 30 December 2017, as the state completely cut access to the global internet network after widespread riots in Iran[15]. The first official definitions and descriptions of NIN were more focused on the security features of an independent national internet[16], especially in light of cyber-attacks against Iran's nuclear facilities. However, the discourse of defence against foreign threats soon changed to a discourse of privacy and developed into an internal promise for a fast, reliable, and secure domestic network independently managed from the global internet[17].

NIN is a state-controlled network that acts as a passageway to the global internet while providing services such as email accounts and search engines on a local level. The network, therefore, divides access to the internet into one internal and one international space.

NIN pursues four significant transformations in internet governance in Iran[18]. Firstly, it provides physical infrastructure such as optical fibre cables and satellites. Secondly, it improves services at a functional level, such as domestic DNS servers, Internet Exchange Points, Content Delivery Networks (CDN), etc. It also enhances access to the 3G and 4G mobile telecommunications technologies. These components will increase internet access's bandwidth, speed, and security. Thirdly, NIN services include email services, national search engines, domestic social media platforms, and services such as issuing SSL certificates and a national operating system. The fourth objective is aimed at the content level, including data collection, categorisation, and summarization. Although all these layers are pursued simultaneously, some components have proved easier to deliver. For example, the limitation on internet speed faster than 128 kbps for regular end-users is removed, and higher speeds have become available[19]. Users can also use NIN for a price of 50% cheaper than connections to the global internet[20].

[15] Center for Human Rights in Iran. Report: Guards at the gate: the expanding state control over the internet in Iran. https://www.iranhumanrights.org/wp-content/uploads/EN-Guards-at-the-gate-High-quality.pdf (2018), last accessed 2019/8/7.

[16] Islamic Republic of Iran's 5th five-year development plan, https://rc.majlis.ir/fa/law/show/790196 (20/1/2011), last accessed 2019/8/7.

[17] The Supreme Council of Cyberspace. Ratifications of the 15th session on definition and prerequisites of establishing the national information network. Official Publication on Governmental Ratifications, http://www.rrk.ir/Laws/ShowLaw.aspx?Code=1640 (22/12/2013), last accessed 2019/8/7.

[18] The National Information Network Homepage, https://bit.ly/2H10ZMJ, last accessed 2019/8/7.

[19] Mashregh News. Limitation on internet speed is removed for domestic ADSL connections, https://bit.ly/2LRmd2E (2015/7/28), last accessed 2019/10/6.

[20] Mehr News Agency. Rates of using the National Information Network is reduced to half, https://bit.ly/31yQMiz (20/1/2017), last accessed 2019/8/7.

Lower prices and higher speeds are used as incentives to encourage people to change to the national network and have resulted in better coverage, especially in rural areas. The Iranian ICT Minister announced in 2019 that 80% of NIN's infrastructure is successfully implemented, and the country must now prepare itself for content-related projects[21]. Considering Iran's history of undemocratic internet governance[22], the country's interference in content control can benefit from a closed domestic network and new technologies such as artificial intelligence. The government has already announced plans for intelligent filtering of internet content in 2015[23]. Still, the project has remained pending due to the end-to-end encryption of most global social media platforms. Intelligent filtering is designed to improve keyword filtering from headers and web addresses to a smarter filtering system that only blocks undesirable parts of a website, not the complete address. Upon NIN's full establishment, applying intelligent algorithms to find and block undesirable content would become possible. During the current uprising, users have often reported sole access to the National Network while access to the global internet has been blocked[24]. The effects of NIN are discussed in detail in the section on internet shutdowns.

Layers of Digital Censorship & Control

The Iranian regime uses various technologies, interception methods and oppressive measures to control cyberspace. These control and surveillance approaches are divided into three layers in this section.

1. Infrastructural Level

As already mentioned in the previous sections, the development of the National Internet Network (NIN) curbs, controls, and surveils users' access at an infrastructural level. Other methods to prevent forbidden content from reaching Iranian users in the first place include[25]:

[21] Tasnim News. 80% of the National Information Network's infrastructure is delivered, https://bit.ly/2x0GvOX (21/4/2019), last accessed 2019/8/7.

[22] Akbari, A. Gabdulhakov, R.: Platform surveillance and resistance in Iran and Russia. Surveillance and Society,17(1/2), 223–231 (2019).

[23] Mehr News Agency. 200 billion Rials for intelligent filtering in the country, https://bit.ly/2yMimfR (23/9/2015), last accessed 2019/8/7.

[24] https://filter.watch/en/2022/10/17/women-life-and-internet-shutdowns-network-monitor-september-2022/

[25] Robertson, B., Marchant, J. (eds.). Revolution decoded: Iran's digital landscape, https://smallmedia.org.uk/revolutiondecoded/ (2014) last accessed 2019/10/5.

- **URL blacklist:** When a user attempts to access blocked content, they are automatically redirected to a standard webpage offering approved links in general categories;
- **DNS redirection:** Telecommunications Infrastructure Company (TIC) is given a list of URLs, which it blocks before allocating bandwidth to ISPs;
- **Content-control software:** Software used by TIC to automatically inspect, filter, and block sites;
- **HTTP host and keyword filtering:** URLs and headers containing specific text are automatically filtered by TIC;
- **Broadband speed reduction:** In times of political unrest, the broadband speed is reduced to a crippling speed, especially to circumvent the spread of video material;
- **Mobile phone network downgrade:** Through SIAM, a software program with direct governmental access, users are shifted from 4G networks to 2G to increase their mobile phone's vulnerability through slower speeds and make them more susceptible to surveillance[26];
- **Connection throttling and internet shutdowns:** The Iranian regime started its experiments with total internet shutdowns during November 2019 protests[27], where at least 1500 people were killed, and 4800 were injured[28]. With the technological advances in the NIN, complete internet shutdowns have become less prevalent but more intelligent during the ongoing protests. Internet shutdowns are targeted at the areas of unrest during the protest hours and are mainly enforced on mobile phone internet connections[24]. This pattern also shows an increase in the complexity of internet shutdowns to prevent profit loss of digital businesses, as well as the interoperability between mobile and cable internet operators, surveillance technologies, and user behaviour analysis.

2. Interactive Level

This layer focuses on monitoring and blocking content during users' connection to the internet. Several methods are used, including:

- **Deep Packet Inspection (DPI):** Technology used to monitor, track and block internet traffic;

[26] https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/

[27] https://www.article19.org/ttn-iran-november-shutdown/

[28] https://www.wired.co.uk/article/iran-news-internet-shutdown

- **MITM (man-in-the-middle):** Method used to intercept online communications;
- **Periodic blocking of SSL Websites:** SSL security protocols are periodically blocked inside Iran, forcing users to use insecure websites instead[29];
- **Traffic Analysis**[11]**:** Analysis of sites that are being viewed most frequently;
- **Mobile phone network downgrade:** As explained in the last section, the software SIAM uses the vulnerabilities of downgrading to 2G networks to gain direct access to users on mobile phones[26];
- **Access to locally-created applications' user data:** The Iranian regime has supported the development of local social media and applications and has used different incentives such as cheaper data packages, governmental loans for start-ups, and filtering of global competitors to encourage Iranian users to use these platforms. Increasing reports confirm extrajudicial access of security forces to these platforms[30]. Twitter users have reported protestors being arrested based on the data of food delivery apps on their mobile phones[31];
- **Blocking VPN services:** VPN blocking is the ultimate way to prohibit users from establishing any connection to the global internet[32].

3. Intra-spatial Level

The oppressive methods of the Iranian regime are not limited to cyberspace. Systematic torture, execution, and surveillance have been used since the establishment of the Islamic Republic to silence any socio-political resistance. These forms of oppression in the hybrid spaces between the physical and digital worlds and are sarcastically called the lack of "freedom after the expression" in Iran. Some of these measures include:

- **Respond to patterns in user behaviour:** Traffic analysis and DPI surveillance informs the creation of updated blacklists and filtered keywords as well as anti-riot police presence in physical spaces and places of assembly;

[29] https://iranhumanrights.org/2014/02/internet-ssl/

[30] https://www.radiofarda.com/a/internet-restrictive-plan-iran/31752479.html

[31] https://twitter.com/1500tasvir/status/1579434816646549504

[32] https://www.lemonde.fr/en/international/article/2022/10/08/iranian-regime-targets-vpns-to-limit-internet-access_5999586_4.html

- **Arrest of internet activists and developers:** These arrests include political activists and protestors on social media platforms and also target digital rights activists that reveal and analyse the regime's abuse of digital technologies and surveillance methods[33];
- **Forced access to digital accounts:** Arrested protestors have repeatedly reported that they have been tortured to grant access or reveal passwords of their social media and email accounts to security officials. Protestors advise each other in forums to avoid taking a mobile phone to demonstrations[34];
- **Facial recognition through CCTV camera footage:** The footage gathered from CCTV and traffic cameras across cities are used to identify political opponents and protestors[35].

4. A Surveillance Assemblage[36]

These interlinked surveillance, control and censorship layers are also connected to other digital elements, such as biometric national identity cards. Iran has issued smart national IDs with biometric data since 2013[37] that offer e-signature and identity confirmation features[38]. Integrating the national information network with identifiable personal data enables the surveillance apparatus to have unprecedented access to citizens' data and control every possible interaction in cyberspace. Moreover, the biometric databanks facilitate the use of facial recognition technologies to identify protestors on the streets[35]. Currently, the regime's different cyber security authorities surveil online communication, divert public attention, initiate smear campaigns, and harass activists on social media. The Iranian Cyber Army is "an underground network of pro-regime cyber activists, hackers and bloggers" that "monitors the internet and launches cyberattacks on the opposition and anti-Islamic websites"[11]. Additionally, the Cyber Police (FATA) focuses on cybercrimes such as online scams or fraud[39]. Interestingly, despite the Cyber Crime Law, surveillance of cyberspace and widespread blocking of popular social media platforms such as Facebook, Twitter and

Integrating the national information network with identifiable personal data enables the surveillance apparatus to have unprecedented access to citizens' data and control every possible interaction in cyberspace. Moreover, the biometric databanks facilitate the use of facial recognition technologies to identify protestors on the streets.

[33] https://www.rferl.org/a/iran-digital-rights-activists-arrested-protest-internet-shutdown/32069999.html

[34] https://groups.google.com/g/sabz-iran/c/8wGbXi8iArk?pli=1

[35] https://www.theguardian.com/global-development/2022/sep/05/iran-government-facial-recognition-technology-hijab-law-crackdown

[36] Haggerty, K. D., Ericson, R. V.: The surveillant assemblage. British Journal of Sociology 51 (4), 605-622 (2000).

[37] Hamshahri Online. Smart national ID officially issued for the first time in Semnan, https://bit.ly/338Ue41 (2013/8/29) last accessed 2019/10/7.

[38] National Smart Card Project, https://bit.ly/33bvzMc

[39] Official Website of Iranian Cyber Police. www.cyberpolice.ir

YouTube, many high-ranking Iranian officials have certified social media accounts, including the Supreme Leader himself (@ khamenei_ir).

Until today, one of Iran's most significant actions against government censorship and surveillance is the widespread use of VPN and anti-proxy services. According to Iran's Ministry of Youth and Sports, 69.3% of Iranian youth between the ages of 15 and 29 use circumvention technologies to access the internet[40]. Although VPN use is generally linked with more secure internet connections, a closer look at the VPN providers in Iran draws a different picture. The primary VPN providers for Iranian users include a) Western news agencies such as BBC Persian, Euro News Persian, Deutsche Welle Persian, Voice of America, etc. These organisations provide their readers with free VPN services to support freedom of expression; b) a Toronto-based company called Psiphon[41] that was founded in cooperation with ARTICLE 19, an international human rights organisation, to improve freedom of expression . Psiphon also sells Western news agencies VPN services and claims to have three million Iranian users[12]; c) applications with unknown origins and ill-defined data protection terms and conditions that offer free access without registration. These applications target many VPN users unfamiliar with data protection basics; d) domestic companies with permissions from Iran's central bank to run online payment services with a claimed clientele of 5 million Iranian users[42]. The official permissions to run the financial backbone of VPN businesses have raised speculations that the domestic providers of VPN services cooperate with surveillance authorities[12]. These speculations were confirmed during the last months as many IT analysts announced that available VPN applications in the Iranian market are stealing data from users' mobile phones[43]. Additionally, during the current protests, Iran's telecom minister announced that the "use and sale" of VPNs are to be criminalised[44]. Such criminalisation endangers millions of Iranian users in their attempt to connect to the global internet.

[40] ISNA News Agency. The latest results of youth poll announced, https://www.isna.ir/news/93061710204/ (2014/8/9) last accessed 2019/10/7.

[41] https://www.psiphon3.com

[42] Hamshahri Online: Filtering and a Market of Billions, https://bit.ly/2M4gBR7 (2019/1/8) last accessed 2019/10/7.

[43] https://twitter.com/ghazayel/status/1573985755696971777

[44] https://twitter.com/KhosroKalbasi/status/1582647153423712257

PILOTING THE GUIDE ON DIGITALLY-MEDIATED ASSEMBLIES: IRAN

After the introduction to Iran's digital governance, this report takes the case of the current protests in Iran under the motto of "woman, life, freedom" to reflect on the ECNL's Guide on digitally-mediated assemblies and examine if the Guide's objectives (below) are met through Iran's case study:

- Collect data on the new ways digital technologies are used to organise assemblies and protests;
- Uncover any opportunities and challenges that digital technologies present;
- Learn about your rights and freedoms when it comes to digitally-mediated assemblies;
- Explore if and how governmental and private actors enable, facilitate, and protect such assemblies and protests[45].

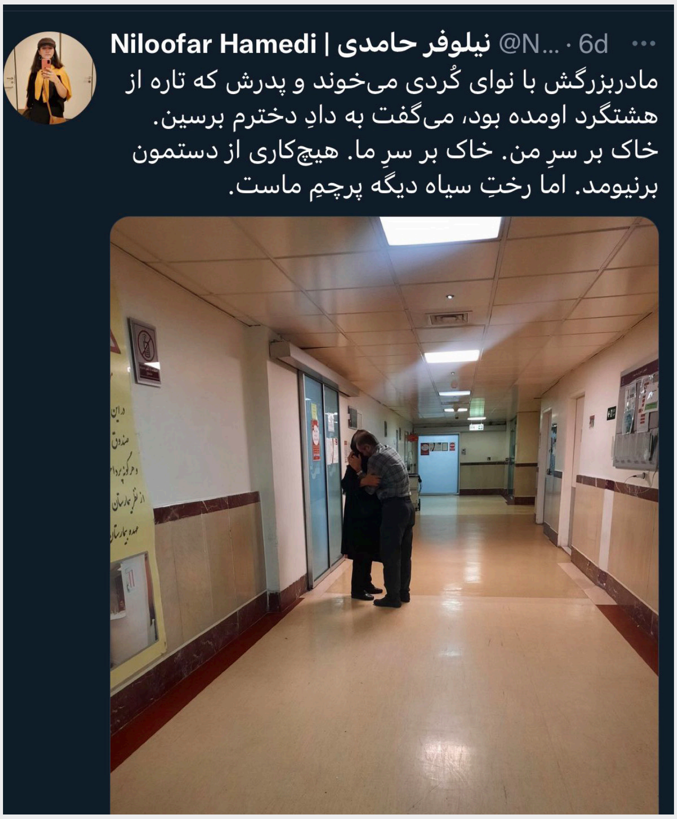
Describing a digitally-mediated assembly

The "woman, life, freedom" movement started concurrently in physical and digital spaces. After Mahsa Amini's death, dozens of people gathered in front of Kasra hospital in Tehran, where she was admitted three days before. Her story and photos of her parents waiting helplessly in hospital corridors went viral on social media. Her name has since remained the primary hashtag for the ongoing revolution in Iran.

During Mahsa Amini's funeral in her hometown of Saqqez (17 September), women removed their headscarves and chanted against the mandatory hijab. The slogan "woman, life, freedom" originated from the Kurdish resistance movement and was picked up by protestors to show their anger against decades of unjust laws and women's oppression. The protests spread to all Iranian cities, university campuses, and even schools. Faced with the brutal violence of police and unofficial militia forces, the movement soon became an anti-regime uprising with a focus on women's rights.

[45] https://ecnl.org/handbook/guide-digitally-mediated-assemblies-and-how-monitor-them

According to a Twitter hashtag analysis, until 27 October 2022 there were 66 million tweets on the #MahsaAmini hashtag and 350 million on #مهسا_امینی (her name in Farsi language)[46]. These numbers are unprecedented when compared to, for example, 63 million Tweets with the hashtag #BlackLivesMatter. It is hard to estimate what percentage of the tweets are coming from within Iran, due to the heavy use of VPNs inside Iran to access Twitter, which has been long blocked. The only international social media platform accessible in Iran was Instagram for a long time, but authorities blocked it on 21 September[24]. Some features, such as Instagram Live were used actively by activists and protestors, especially as a way to respond to questions, for awareness raising, and for political debate. Similar features on Twitter, such as Twitter Space, were employed to organise more targeted digitally-mediated assemblies to debate current events or exchange news[47]. One of the most popular platforms for digitally-mediated assemblies in the last months in Iran is Clubhouse, which provides users with a virtual town hall to listen to, invite people to the stage, and even vote by raising virtual hands. Clubhouse has been extra popular due to its sole use of voice, offering less identity recognisability. Clubhouse's format for debating ideas has even attracted Islamic Republic's politicians to convince public opinion on controversial issues, such as the Foreign Minister's presence on the platform to explain Iran's 25-year deal with China[48].



Niloofar Hamedi | نیلوفر حامدی @N... · 6d

مادربزرگش با نوای کُردی می‌خوند و پدرش که تاره از
هشتگرد اومده بود، می‌گفت به دادِ دخترم برسین.
خاک بر سرِ من. خاک بر سرِ ما. هیچ‌کاری از دستمون
برنیومد. اما رختِ سیاه دیگه پرچمِ ماست.

Figure 2. First reports about Mahsa Amini published by currently jailed Niloofar Hamedi, Shargh Newspaper's journalist

[46] https://twitter.com/marcowenjones/status/1585704740067086337?s=46&t=_aWnuZom6cjbyC9lLcSp2g

[47] See, for example: https://mobile.twitter.com/i/spaces/1gqGvyedpgzKB

[48] https://old.iranintl.com/en/world/zarif-appears-clubhouse-social-media-explain-iran%E2%80%99s-pact-china

Planned vs spontaneous

Both #MahsaAmini and #مهسا_امینی hashtags (and their variations) were spontaneously created to commemorate Mahsa Amini's death. The slogan "woman, life, freedom" (Kurdish: Jin, Jiyan, Azadî, ژن، ژیان، ئازادی) stems from the Kurdish freedom movement and decades of grassroots activities of Kurdish women[49]. Abdullah Öcalan, the leader of the emancipatory Kurdish movement, explained in his 1998 speech that any liberation movement cannot succeed without the emancipation of women. The slogan found resonance in the current movement, especially after years of women's resistance against patriarchal and ideological laws in Iran and their daily struggle to gain control over their bodies, clothing, and public presence[50]. The first demonstration against the compulsory hijab was held on 8 March 1979, just a few months after the revolution. Thousands of women, many with hijab, protested against Ayatollah Khomeini's decree banning women from entering governmental offices and workplaces without hijab. These demonstrations were suppressed brutally and dismissed by other revolutionary groups, predominantly led by men, as not bearing any revolutionary importance. Although it took another year for the Iranian regime to pass laws enquiring about women covering their bodies and hair, the Islamic Republic made it clear from the very beginning that its ideal vision of Muslim women with predetermined gender roles is pivotal to its ideology. The progressive Family Protection Act, granting women equal rights within the institution of marriage, was among the first laws abolished immediately after the revolution's victory.

During the 8-year Iran-Iraq war, women's rights faded further against more urgent and existential issues at hand, but several penal laws were ratified in the meantime to punish "improper clothing." The legal and institutional establishment of compulsory hijab was accompanied by everyday intimidation of women in public spaces by vigilante revolutionary committees. By the war in 1989, compulsory hijab was legislated, normalised and enforced.

With the ratification of the new Islamic Punitive Law in 1993, police forces became legally obliged to enforce hijab-wearing. Since then, and with the establishment of Moral Police Patrols in 2005, surveillance of women in all public spaces has been an ongoing source of tension. Arrested women are transferred to the

[49] https://www.newyorker.com/news/q-and-a/fatemah-shams-how-irans-hijab-protest-movement-became-so-powerful

[50] The following paragraphs were originally written for my Guardian Opinion piece and are published here after editing by The Guardian Opinion editors: https://www.theguardian.com/commentisfree/2022/sep/26/elon-musk-iran-women-mahsa-amini-feminists-morality-police

Bureau against Social Corruption[51]. They are treated like criminals, with their photos taken and their personal information recorded and archived. They are forced to answer questions about their psychological well-being and wait for hours until someone brings them proper clothes. This draconian procedure ends with coercing the women to tear apart their ‘bad’ clothes with scissors. Any repetition of such ‘crimes’ is prosecuted in the courts. Anger is the natural outcome of such humiliating treatment.

Although similar to many other social movements, the women’s movement has been continuously suppressed under the Islamic Republic, but it has never ceased to exist. For example, the One Million Signature Campaign for the Repeal of Discriminatory Laws, initiated in 2006, showcased a non-hierarchical, leaderless movement of hundreds of women advocating for equal rights, talking to citizens at every opportunity, raising awareness, and attempting to bring about change from within the Iranian society. Such campaigns coincided with the first wave of widespread public access to the internet. As much as they negotiated for their rights in public spaces, women were pioneer bloggers. Iranian cyberspace in the 2000s saw an explosion of conversation and argument after decades of silence about the female body, sexuality, pleasure, and women’s rights.

Iranian women have been exemplary proponents of how resistance functions within hybrid physical-virtual spaces. As the Iranian regime tightened its grip on internet freedom, feminist activists seized the possibilities that digital technologies provide.

Since then, Iranian women have been exemplary proponents of how resistance functions within hybrid physical-virtual spaces. As the Iranian regime tightened its grip on internet freedom, feminist activists seized the possibilities that digital technologies provide. The internet facilitated advocacy campaigns, not only for changing laws and policies but for more taboo issues such as discussing the female body[52], sexual health[53], LGBTQ+ forums[54] and counselling, taking action against violence in the workplace[55] and sexual harassment in public spaces[56], and the Iranian #MeToo movement.

Other campaigns specifically targeted resistance against compulsory hijab. The online movement “My Stealthy Freedom campaign”[57], started in 2014 by an Iranian-born journalist and activist outside Iran, encouraged women to stroll the streets without hijab and share videos on social media channels. Gershad app[58] used collective mapping to help women avoid moral police

[51] http://bidarzani.com/20614

[52] https://hamdamapp.com/

[53] https://www.instagram.com/xavishanx/

[54] @queerkadeh and @RainbowHelp on Instagram

[55] https://endworkviolence.org/

[56] https://harasswatch.com/

[57] https://www.instagram.com/masih.alinejad/

[58] https://gershad.com/

patrols. In 2017, Vida Movahed climbed a telecoms box[59] on the busy "Revolution" street, put a white head scarf on top of a stick, and stood there in silence until she was arrested. The following week, the entire country was full of women standing silently on telecoms boxes, waving their headscarves, often being brutally taken down. The winter of 2017–18 was the beginning of an independent movement of ordinary women literally standing their ground. The power of one image travelling through nods and networks of social media and messaging apps questioned all the injustice imposed on women for decades.

This rather lengthy background demonstrates that although the events after the death of Mahsa Amini might seem 'spontaneous,' they are the direct consequence of decades of women's resistance in both physical and digital spaces. As shown elsewhere[60], for example, through the content analysis of the "My Stealthy Freedom" campaign and Gershad app social media accounts, these projects are deeply interlinked with other instances of resistance in areas such as internet freedom, labour movements, religious freedom of expression, ethnic minorities and similar. These interlinkages explain the rapid transformation of "woman, life, freedom" protests to a nationwide revolution against the regime.

Although the events after the death of Mahsa Amini might seem 'spontaneous,' they are the direct consequence of decades of women's resistance in both physical and digital spaces.

Identification of organisers

The digitally-mediated assembly created around Mahsa Amini's hashtag includes thousands of users, which some of whom enjoy a more extensive following due to their previous political activities, academic or social status, or as sources of news. The smaller, more targeted digitally-mediated assemblies, such as the ones on Instagram live, Twitter Space, or Clubhouse, are hosted and facilitated by established figures or experts such as activists, academics, and journalists.

Since Iranian users who access these platforms use circumvention tools such as VPN services, it is difficult to identify the location of all users. Only when the users are formerly known activists or celebrities, their location is clear to the audiences. Many users on Instagram and Twitter have changed their profile pictures to photos of killed protestors or use Mahsa Amini's hashtag in their profile name. They remain intentionally anonymous since the Iranian Cyber Army actively monitors trends, comments, debates, and influential accounts.

[59] https://www.theguardian.com/world/2018/jan/29/second-woman-arrested-tehran-hijab-protest-iran

[60] Akbari, A.: Spatial|Data justice: mapping and digitised strolling against moral police in Iran. In: Heeks, R. (eds.) GDI Development Informatics Working Papers, Paper No. 76, University of Manchester, https://www.gdi.manchester.ac.uk/research/publications/di/di-wp76/ (2019).

Duration of assembly

Since the revolution and widespread demonstrations are still ongoing, digitally-mediated assemblies continue. Mahsa Amini's hashtag is still the leading element of digitally-mediated assembly. Other smaller targeted assemblies are limited in time and depend entirely on their organisers' plans. For example, after the publication of the Intercept's report on Iran's surveillance of mobile phones[26], Filterbaan, an internet freedom NGO, used Twitter Space to explain the technical aspects of the report for journalists, other activists, and interested individuals.

Digital divide

The official Iranian statistics claim that the country's internet penetration rate has surpassed 122 per cent[61]. According to this report, in 2022, the use of fixed broadband internet is about 13 per cent of the total, while the 161 per cent penetration rate of mobile phones (136 million subscriptions) has facilitated widespread internet access. Although the World Bank statistics report a lower penetration rate of 84 per cent[62], internet access has meaningfully grown in Iran. Research on the state of digital divide in Iran has shown a correlation between the level of education and income and the ICT development index[63].

The heavy censorship and blocking of international platforms add to the already existing digital divides, especially between different age groups and tech-savvy people

It is noteworthy that the digital divide and digital literacy are not adequate analytical factors here since the complications of using circumvention technologies to access the global internet are even hard to grasp for average educated users. Therefore, the heavy censorship and blocking of international platforms add to the already existing digital divides, especially between different age groups and tech-savvy people.

Legal framework

The Iranian regime has a long-standing precedence in violating human rights and systematic oppression of socio-political opposition. The regime has repeatedly violated international conventions and does not respect the Iranian constitution on freedom of peaceful assembly and expression. It uses various technologies, policies, and control measures to curb access to the internet, censor digital content, and prosecute digital activists. Recent worrisome legal developments include the preliminary

[61] https://www.iranintl.com/en/202203035872

[62] https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=IR

[63] Qadikolaei, M.R., Zali, N. & Soltani, A. Spatiotemporal investigation of the digital divide, the case study of Iranian Provinces. *Environ Dev Sustain* (2022). https://doi.org/10.1007/s10668-022-02738-0

ratification of the "User Protection Bill" in February 2022. The bill is a successor of a 2018 failed attempt at the "Managing Social Messaging Apps" Bill's ratification. New amendments were introduced in 2020 after the formation of the new parliament not only to extend the restrictions on internet freedom but also to "reshape internet governance in Iran" and "give greater control to the armed forces and push for drastically greater surveillance of the population"[64]. In November 2022, the Supreme Council of Cultural Revolution announced new measures to foresee punishments for students who organise digital student groups with more than 100 members[65]. Group creators need to apply for licenses to be able to have more than 100 students in a digital group. Punishments include suspension, expulsion, and deprivation from studying at any Iranian university.

In November 2022, the Supreme Council of Cultural Revolution announced new measures to foresee punishments for students who organise digital student groups with more than 100 members.

Messaging

There are a variety of messages circulating under Mahsa Amini's hashtag, mainly news (i.e. videos of demonstrations, statements, debates), songs, posters, and other cultural material, political messages from leading figures, mobilisation messages (i.e. information on demonstrations, panels, and debates), and personal opinion. The messages under Mahsa Amini's hashtag are majorly about Iran. Still, they also target international audiences such as the global public, UN and other international authorities, Western politicians, academic communities, international unions, and similar. In many offline assemblies, participants carry placards that contain hashtags. Hashtags are also written next to slogans on walls in different urban areas.

Women's rights and women's narratives of decades of patriarchal and state oppression are central to the digitally-mediated assemblies.

Due to the diversity of messages, they are created by a variety of actors such as activists, protestors, journalists, politicians, artists, etc. The messages are majorly political, demanding political change, respect for human rights and freedoms, and immediate ceasing of violence against protestors. However, women's rights and women's narratives of decades of patriarchal and state oppression are central to the digitally-mediated assemblies. In that sense, the revolution carries a deep social transformation of values and roles in its heart.

Different political opposition groups and cyber army pseudo-accounts run smear campaigns against journalists and activists that they deem 'betrayers.'The height of these smear campaigns was reached when an intercepted mutilated version of a BBC Persian journalist's phone conversations with her mum was released on Iranian state-run TV, where she expressed her worries about separatist activities. She was immediately accused

[64] https://filter.watch/en/2022/04/07/whose-internet-the-battle-over-the-future-of-the-internet-in-iran/

[65] https://twitter.com/Digiato/status/1597178971472678914

of downgrading the revolution's objectives to separatist ideas on social media and closed her social media accounts for good after the online harassment and smear campaigns[66]. The Iranian Cyber Army and other political groups most probably use fake accounts to divert debates and discussions. In one case, a woman sitting with the Iranian delegation at the UN Human Rights Council was falsely identified, but the writer did not delete the Tweet since it had "too many likes"[67]. Since most social media accounts are anonymous, defamation campaigns are hard to tackle and solely depend on each platform's content moderation policies.

The messages have multiple forms, such as videos of demonstrations, audio and video files from activists and politicians, recorded audio versions of offline panels, for example, in universities, clubhouse sessions, journalistic pieces, hashtags, and hacked data sets. Since many hacktivist groups are involved in pursuing the current revolution, datasets from Iranian governmental organisations have been hacked and publicised. In late September, the group Anonymous released all Iranian MPs' contact information on Twitter and urged Iranians not to stop the 'Revolution'[68]. On its Telegram channel, the Iranian group Black Reward has revealed thousands of emails from the Iranian Atomic Energy Organisation[69] or secret news bulletins for the Supreme Leader created by the Fars News Agency, a news agency close to the Iranian Revolutionary Guards[70].

Measuring impact

The hashtags around Mahsa Amini's name reflect the fundamental change in the Iranian socio-political system. Digitally-mediated campaigning, awareness raising, and communication have played a pivotal role in mobilising the protests, spreading the demonstrations, slogans, and symbolic actions such as burning headscarves to the entire country. Some symbolic acts, such as cutting hair, have received international attention and have been performed by many politicians, activists, artists, etc., outside Iran.

As stated before, in addition to pro-regime accounts, the Iranian Cyber Army has years of experience in diverting digitally-mediated assemblies and debates to harm the democratic nature of dialogues, instigate an atmosphere of insecurity, and disturb the trusting relationship between online users. This could be

The Iranian Cyber Army has years of experience in diverting digitally-mediated assemblies and debates to harm the democratic nature of dialogues, instigate an atmosphere of insecurity, and disturb the trusting relationship between online users.

[66] https://www.iranintl.com/202211122532

[67] https://twitter.com/darushmemar/status/1595761281897795584

[68] https://www.iranintl.com/en/202209255133

[69] https://www.hackread.com/black-reward-hackers-iran-atomic-energy-agency/

[70] https://twitter.com/shokrani_maryam/status/1596196124590850048?s=20&t=-GWxCwMOW3EqnQzHf_hpew

observed even in the similar writing style of many anonymous accounts that attack online activists or publish disinformation. In October 2021, Iranian news agencies quoted the commander of the Iranian militia group (Basij), that four million Basij members have performed a cyber manoeuvre in collaboration with the Cyber Army to practice creating trends on social media platforms[71].

Use of digital technologies and social media

Twitter and Instagram, both blocked and only accessible through VPN technologies, were the leading social media platforms used for digitally-mediated assembly. WhatsApp and Telegram groups, although blocked, also play an essential role in spreading the news among the public. Most of the messages were distributed through existing platforms and technologies already familiar to the protestors. The hacktivist attacks to Iranian governmental organisations were unprecedently high during the current protests. Therefore, it was the first time large data sets from such organisations were released for public scrutiny.

Due to the heavy restrictions on internet access and filtering of social media platforms, the participants have exhausted the possible potential each platform offers. Twitter Space, Instagram live, and Clubhouse have been actively used for debates and decision-making. WhatsApp and Telegram groups have become the primary sources of news and information. Mahsa Amini's hashtags have been fundamental to keeping the flow of information organised.

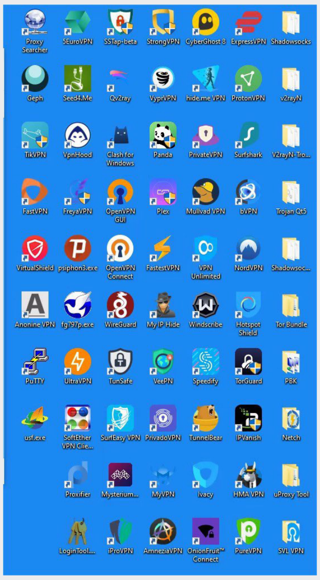


Figure 3. Screenshot of an Iranian user's mobile phone with tens of different VPN applications

Figure 3[72] shows the extreme difficulties in accessing the global internet and international platforms for an Iranian user due to access disruption and VPN blocking. It takes only hours for the regime to block new VPN connections, and users must constantly download newer applications. This constant struggle exposes the users to data protection, and privacy dangers since many of these applications are published by unknown sources and, as explained in the introduction, could be a scam for stealing users' data.

[71] shorturl.at/evAUY

[72] https://twitter.com/Mardetanha/status/1575117341939187714

One of the known tactics of the Iranian Cyber Army is to report undesirable content through its fake users to remove the content from global social media platforms temporarily. Consequently, not content moderation per se but abusing content moderation reporting systems are strategically used against Iranian users.

Role of technology companies

Content moderation in major global platforms is systematically abused by the Iranian Cyber Army. Additionally, at the beginning of the protests in September, the Iranian regime blocked WhatsApp. Iranian users outside Iran who had registered in WhatsApp with their Iranian number (+98) reported a temporary lack of access. This suspicious blocking that seemed centrally performed by Meta enraged many users[73] and caused an immediate apology and continuation of WhatsApp[74] services for users outside Iran.

Due to the massive restrictions on accessing safe internet in Iran, some VPN companies have offered Iranian users free services in solidarity with their cause[75]. Other major companies such as signal and Tor invented extensions and services to help Iranians circumvent Internet censorship. Tor's Snowflake allows users to avoid being noticed by Internet censors by transforming their Internet activity through, for example, redirecting "Internet traffic to appear to be coming from popular cloud providers" or "scrambling Internet traffic to make it appear completely random"[76]. One of the most secure messaging apps, Signal also offered TLS proxies that "can be used to bypass the network block" and "securely route traffic to the Signal service"[77]. It is noteworthy that both later solutions work with the help of users who have access to the global free internet. In doing so, not only do the tech companies offer solutions to circumvent censorship, they base their solution on the collective power of users worldwide.

[73] https://twitter.com/userhomi/status/1572915946762936322

[74] https://twitter.com/WhatsApp/status/1572976018771656706

[75] https://twitter.com/techbubble/status/1595498781507981312

[76] https://snowflake.torproject.org/

[77] https://signal.org/blog/help-iran-reconnect/

Privacy protection of participants

> In both online and offline spaces, privacy and protecting participants' identity have become vital parts of the movement.

Although arranging privacy protection for such a large heterogenous group of people is impossible, many digital rights activists have developed step-by-step guides for securing privacy on mobile phones, especially considering the number of suspicious malware available, such as VPN apps in the current chaotic atmosphere. For example, two websites, Paskoocheh[78] and Iran in Darkness,[79] offer circumvention and VPN apps and a toolbox for times of Internet Shutdowns. Other educational material shows users how to set up vanish mode for Instagram messages and avoid using local government-supported applications that spy on users or delete the mobile phone's content from a distance[80].

Although the messages were majorly similar in online and offline spaces, there is a lively interaction between online and offline components of the uprising. Privacy protecting measures do not remain limited to online privacy and protection, and target the widespread use of CCTV cameras in public spaces. Figure 4 shows the blocking of a CCTV camera in public transportation by menstruation pads. Next to this statement that highlights the gender-related aspects of the ongoing revolution and resistance against surveillance, there is a hashtag for a political prisoner that also highlights the digital presence of the resistance in cyberspaces. Figure 5 shows two posters designed to encourage Iranian protestors to destroy CCTV cameras or the "devil's eye." In both online and offline spaces, privacy and protecting participants' identity have become vital parts of the movement.

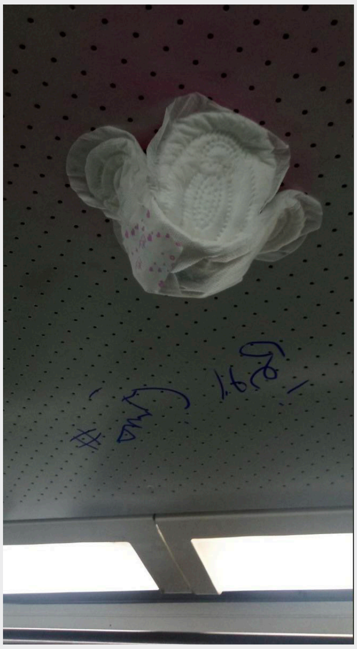


Figure 4. Blocking CCTV cameras in Public transportation with menstruation pads

[78] https://paskoocheh.com

[79] https://irandarkhamooshi.net/

[80] https://twitter.com/filterbaan/status/1595748752521920515

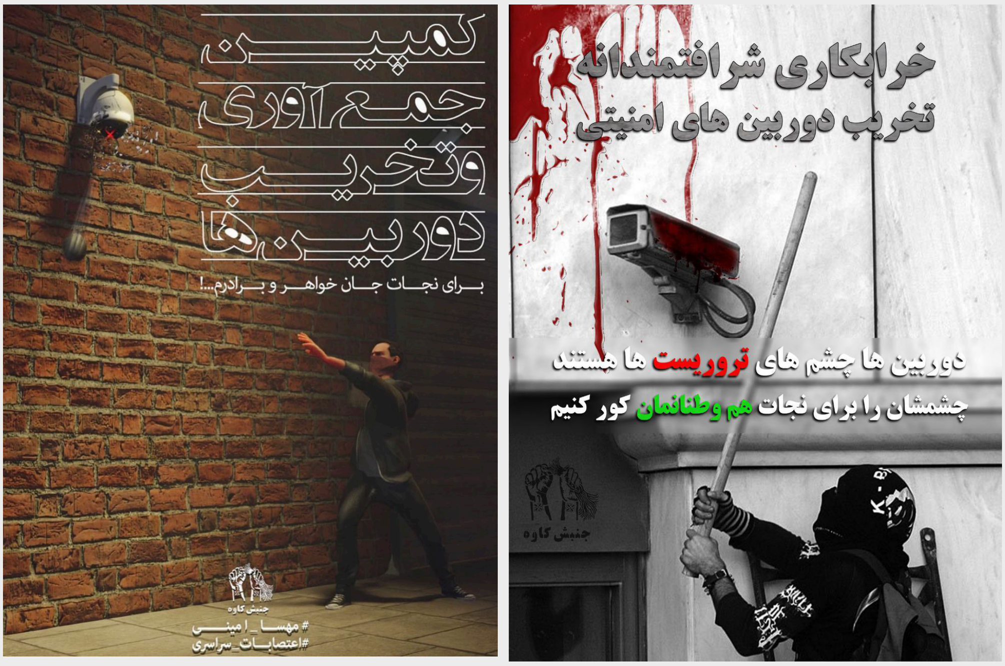


Figure 5. Posters encouraging protesters to destroy surveillance cameras

Media and journalist involvement

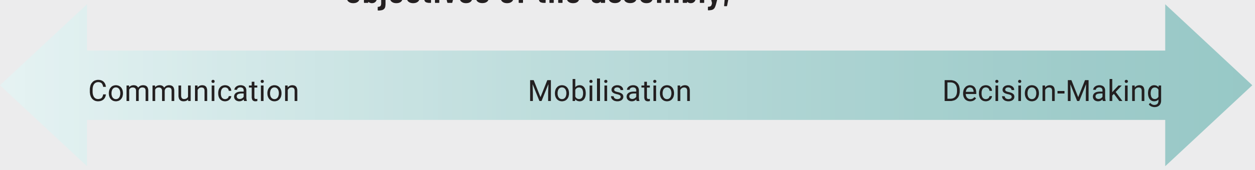
Niloufar Hamedi, the journalist who first published Mahsa Amini's story, was arrested on 20 September 2022. Elaheh Mohammadi, another journalist who covered Amini's funeral in her hometown of Saqqez, was detained on 29 September. On 28 October, the Intelligence Ministry and the Islamic Revolutionary Guard Corps Intelligence Organization issued a joint statement claiming that Hamedi and Mohammadi were "foreign agents" engaged in "multi-dimensional wars" organised by "Western and Zionist intelligence agencies... to carry out serious and uninterrupted planning to influence different social layers, especially in areas related to women"[81]. These accusations could be used for a capital punishment sentence against the two journalists. As already mentioned in the introduction, 51 journalists have been arrested during the protests. Many other activists, artists, and athletes who have openly expressed their support for the revolution in social media have been arrested and face imminent danger.

[81] https://iranhumanrights.org/2022/11/witch-hunt-in-iran-grave-concerns-for-journalists-niloufar-hamedi-and-elahe-mohammadi/

CONCLUSION

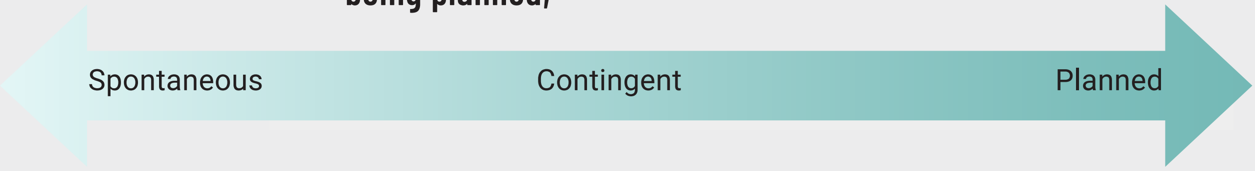
Considering the detailed evaluation of the ECNL's Guide, this report suggests that any assessment of digitally-mediated assemblies is dependent on the folowing:

- **objectives of the assembly;**



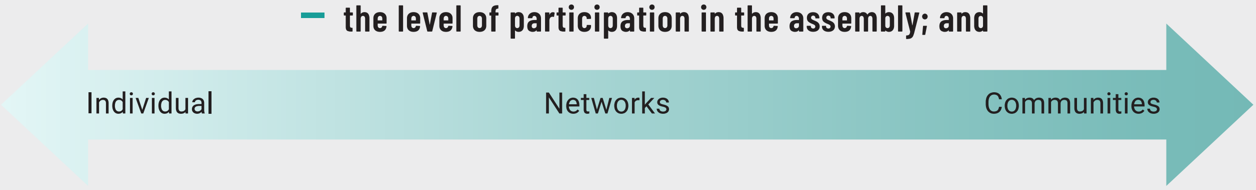
Communication Mobilisation Decision-Making

- **the temporality of the events and the degree of them being planned;**



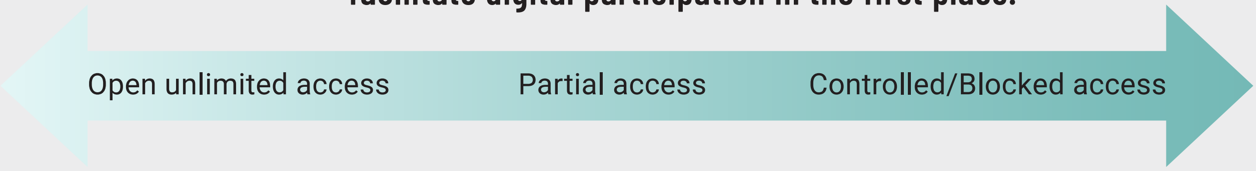
Spontaneous Contingent Planned

- **the level of participation in the assembly; and**



Individual Networks Communities

- **the degree of access to internet and platforms that facilitate digital participation in the first place.**



Open unlimited access Partial access Controlled/Blocked access

These varying degrees should then be contextualised depending on the potentials that specific features of digital platforms offer. Twitter, for example, started Twitter Space in competition with new platforms such as Clubhouse to facilitate online debating. Furthermore, if the digitally-mediated assembly is taking place in a severely controlled and censored digital space, many concepts such as public/private, privacy, use of innovative technologies, legal frameworks, restriction of freedom of expression, and similar should be analysed with a different lens. The overlapping nature of freedom of expression, freedom for peaceful assembly and human rights necessitates a more holistic approach to how digitally-mediated assemblies work, especially in authoritarian contexts.

European Center for
Not-for-Profit Law

European Center for Not-for-ProfLaw Stichting
5 Riviervismarkt, 2513 AM
The Hague, Netherlands
www.ecnl.org
twitter.com/enablingNGOlaw