Commentary

Dialogues on Digital Society
2025, Vol. 1(3) 283–287

DOI: 10.1177/29768640251375558
journals.sagepub.com/home/dds

Smart mandate in Iranian cities: From digital sovereignty to the automated oppression of everyday life

Niloufar Vadiati
Leuphana University Lüneburg

Nassim Mehran
Charite-Universitätsmedizin Berlin

Abstract

Iran's centralized mandate for smartification—spanning fiber-optics, domestic apps, and platform governance—sustains ideological-authoritarian control over urban society, the entrepreneurial ecosystem, and infrastructures of governmentality. This system enables pervasive surveillance, censorship, and ideological discipline, while maintaining a monopolistic grip on the digital economy. This commentary conceptualizes these dynamics as a *smart mandate assemblage* rooted in clerical authority and a militarized oligarchy, diverging from neoliberal models of smartification in (semi-)liberal democracies. From national sovereignty policies to everyday urban life, such assemblage surveils space, disciplines marginalized bodies, and reshapes technological and infrastructural futures under the guise of modernity.

Keywords

Smart city, digital sovereignty, digital entrepreneurship, Iran, ideological-authoritarianism

Introduction

Digital technology has developed in tandem with capitalist expansion, often in co-dependency with state and military power. In the United States, for example, there is ample evidence that major tech elites have long-standing political and financial ties to militarized and state security institutions, both domestically and internationally (Meulbroek and Glassman, 2025). Scholars describe this convergence of powerful tech firms with the old oligarchy as producing "authoritarian practices within (semi) liberal democracies" (Akbari and Murakami Wood, 2025). However, in contexts lacking democratic infrastructure, such as Iran, the entanglement of a utopian agenda of smartification and state power follows what Akbari (2022) refers to as "smart control." Yet this form of control unfolds differently across various authoritarian contexts, shaped by the specific configurations of each regime. This commentary characterizes the Islamic Republic of Iran as an

Corresponding author:
Niloufar Vadiati, Leuphana University, Lüneburg, Germany.
Emails: niloufar.vadiati@leuphana.de; niloufar.vadiati@gmail.com

ideological-authoritarian regime, rooted in the religio-legal doctrine of *Velayat-e Faqih* (Guardianship of the Jurist) (Mehran and Vadiati, 2024). In contrast to authoritarian-neoliberal contexts such as Russia (Morozov, 2011; Soldatov and Borogan, 2017), we argue that Iran's practice of state power and its strategic entanglements with capital and digital technologies are more ambivalent (Mehran and Vadiati, 2024). Against this backdrop, this commentary unpacks how "smart control" unfolds within the infrastructures of governmentality, the entrepreneurial ecosystem, and urban everyday under the Islamic Republic's mandate in Iran.

The intranet and coercive sovereignty

Proponents of Iran's techno-nationalism frequently invoke sanctions as justification for tightening domestic control over digital infrastructure. The National Information Network is a state-controlled *intranet* framed as protecting national sovereignty —the so-called *Halal Internet* designed to shield the nation from external meddling. Yet this narrative hides its factional nature. The Islamic Revolutionary Guard Corps (IRGC) dominates Iran's telecommunications, cloud services, and app stores, creating a form of privatized sovereignty within the regime's power blocs (Conduit, 2025). Far from fostering resilience, this control deepens dependency, corralling any domestic digital activities into an ecosystem of state-sanctioned platforms, where any deviation is criminalized as *a threat to national security* (Wikipedia, 2025). A key example is Iran's controversial cyber bill *Tarh-e Siyanat* (protect users' rights in cyberspace) (Human Rights Watch, 2022). This legislation aims to territorialize connectivity—controlling data flows by keeping Iran's internet traffic within national borders. In practice, however, isolating Iran's networks has made them more vulnerable, technically, socially, discursively, and symbolically. Domestic platforms offer poor usability and security, while filtering failures prompt browsers, flagging them as unsafe. These failures highlight a deeper incapacity within Iran's Information and Communication Technology sector to replicate the interoperability and reliability of the global internet. Moreover, the failure to foster homegrown cyber capabilities—and the suppression of autonomous and undomesticated local initiative—has driven a growing exodus of tech entrepreneurs, as innovation becomes increasingly untenable within the rigid confines of state-controlled infrastructure. This dynamic underscores how Iran's *digital sovereignty* claim is motivated not by market efficiency or neoliberal aspiration, but by ideological fortification of the regime.

Captive digital entrepreneurship

The political agenda of privatization, combined with Islamist state ideology, has fostered competition among various parastatal organizations, from clerical institutions to military entities such as the IRGC (Mehran and Vadiati, 2024). Out of this environment has emerged a "fat capitalist" class that advances the ideological agenda through non-liberal capitalist methods of production (Harris, 2013), the dynamic that is embodied by Iran's tech ecosystem. Major domestic platforms for ride-hailing, e-commerce, and social media in Iran have not arisen from an open digital commons but via a tightly controlled ecosystem (Akbari, 2019). Access to critical infrastructure, licensing, and venture capital is systematically channeled to regime-aligned insiders. In other words, the Iranian case illustrates an *ideological-authoritarian innovation* model: a monopolistic digital entrepreneurship where gatekeeping extends beyond venture capitalists to include military-economic patrons who govern through loyalty, surveillance, and coercion.

In practice, this model turns digital entrepreneurship into a tool of regime consolidation, protecting regime-aligned interests while systematically excluding, silencing, or securitizing oppositional actors. For instance, Snapp, Iran's ride-hailing giant, is formally a private company but operates on state-issued licenses that require political compliance (Harris 2020). Although academic research on this remains limited, Snapp's role in Iran's controlled digital ecosystem has raised concerns about data opacity and

political compliance, especially during the 2019 and 2022 protests. Similarly, Digikala, often dubbed *Iran's Amazon*, has consolidated its position not just through market mechanisms, but via structural advantages afforded by state backing, enjoying privileged access to payment systems, logistics networks, customs processes, and other infrastructure that its peers lack.

Automated oppression of urban everyday

The technological capacity of smart cities' *optimism and ordering* in Iran, such as any other authoritarian context, has become a control grid, systematically blurring the line between urban management and authoritarian enforcement. This transformation embeds ideological policing and disciplinary norms into the mundane rhythms of urban life through digitally mediated surveillance and punishment. Some of the key manifestations of these practices include:

Over-smartification

In Iran, digital access is overtly political rather than merely infrastructural or consumerist. While high-speed internet has expanded to many rural areas (Tehran Times, 2024), connectivity remains under the control of opaque regulatory regimes. Security agencies can throttle bandwidth or shut down services across entire regions during protests. Simultaneously, surveillance and ideological policing are embedded into the routines of city life —what might be described as the *over-smartification* of the everyday. Ordinary needs—such as accessing subsidized bread, fuel, or healthcare—are increasingly mediated through state-mandated smartphone apps. The government hails this over-smartification as technological progress, despite the fragility of daily life amid unreliable power and internet infrastructures.

Surveillance infrastructure as everyday urban management

The ubiquitous surveillance infrastructure embedded in urban systems, while presented as serving public convenience, simultaneously functions as a pervasive tool of control. Tehran's Shahriar and MyTehran service portals, for example, promise seamless access to services—from parking permits to tax records—but they are centralized data repositories, collecting national ID numbers, utility bills, geolocation data, and behavioral metadata. Cross-referencing these data with existing state databases makes individual profiling nearly effortless. Also, the IRGC's economic arms, notably Etemad Mobin and the Bonyad-e Mostazafan, maintain controlling stakes in major telecoms such as TCI and Irancel (Conduit, 2025), giving security forces privileged access to mobile metadata, location tracking, and app usage—blurring the boundaries between civilian infrastructure and military intelligence.

What is presented as efficient urban governance in Iran is, in practice, a form of infrastructural capture—where data flows into centralized command centers, placing urban life under a militarized gaze. For instance, Tehran's Low Emission Zone scheme uses automatic number plate recognition cameras to enforce pollution controls, yet these systems are integrated with law enforcement databases, enabling real-time tracking of vehicles associated with dissidents or protest organizers. More acutely, artificial intelligence-driven facial recognition is deployed across metros, streets, and highways to enforce hijab compliance—transforming smart city infrastructure ostensibly meant for public safety into a tool for surveilling women's bodies. In a context where women's bodily autonomy is already deeply contested, technology becomes a direct instrument of ideological control. Everyday mobility becomes a site of ideological discipline, with violations generating fines and scrutiny —revealing how deeply digital urbanism in Iran is intertwined with authoritarian ideology.

Instrument for protest suppression

The integration of digital infrastructure into protest control directly illustrates Iran's model of smart authoritarianism. During civic unrest, the systems built for urban optimization have been weaponized against dissent. For example, in the protests of

2019 and 2022, Iran's fiber-optic networks—designed for fast, city-wide connectivity—were throttled or shut down in protest-prone neighborhoods. Key communication channels such as Telegram and Waze were blocked, nationwide SMS bans were imposed, and even foreign satellite phones were jammed (Grinko et al., 2022). In addition, Tehran's extensive CCTV and drone surveillance infrastructure has been used to retroactively identify and arrest protesters. In reported cases during the *Mahsa (Jina) Amini* uprising, license plate records and metro card usage were triangulated to reconstruct protest routes and link individuals to demonstration sites. In effect, the city's digital nervous system acts as a *panic button*: when the regime's political control is threatened, the technology shifts from enabling city life, deploying information, mobility, and visibility, to suppressing dissent.

Conclusion

Iran's strategy of smartification is, in many ways, a logical expression of its model of ideological-authoritarian modernization: it merges ambitions of urban efficiency and tech-entrepreneurship with an extension of the state's capacity to govern, exclude, and punish. Yet to view Iran's smart mandate through a generic *authoritarian innovation* lens risks flattening its distinct socio-political terrain. Iran's digital program is not merely about optimizing infrastructure or platformizing markets. It is about forging new horizons for ideological domination and expansion, creating a digital sovereignty that serves as both a geopolitical shield and a domestic cage. In practice, this means that the Islamic Republic's tech-governance strategy selectively rewards compliant actors and punishes visible dissenters. Everyday citizens face opaque surveillance and control, with gendered bodies bearing the brunt of moralized digital control. Amid the regime's tight control, many Iranian digital entrepreneurs and developers migrate—both metaphorically and literally.

It is important to acknowledge that authoritarian forces in Iran severely restrict empirical data access, hindering sustained fieldwork and long-term inquiry. As a result, much of the existing scholarship remains necessarily conceptual or speculative. Our critical stance, for instance, emphasizes the coercive functions of digital infrastructures, leaving less space to explore the ambivalent, adaptive, or resistant practices that may be emerging within everyday urban life. These constraints highlight the urgent need for further empirical and comparative research to understand how digital authoritarianism is localized, contested, and reproduced across Iran's diverse urban and peri-urban geographies.

Declaration of conflicting interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs

Niloufar Vadiati https://orcid.org/0000-0002-7533-3665

Nassim Mehran https://orcid.org/0000-0003-3836-3205

References

Akbari A (2022) Authoritarian smart city: A research agenda. *Surveillance & Society* 20(4): 441–449.

Akbari A and Gabdulhakov R (2019) Platform surveillance and resistance in Iran and Russia: The case of Telegram. *Surveillance & Society* 17(1/2): 223–231.

Akbari A and Murakami Wood D (2025) Towards a critical political economy of surveillance and digital authoritarianism. *Surveillance & Society* 23(1): 152–158.

Conduit D (2025) Digital authoritarianism and the global technology industry: Evidence from Iran. *Government and Opposition* 60(3): 751–772.

Grinko M, Qalandar S and Randall D (2022) Nationalizing the internet to break a protest movement: Internet shutdown and counter-appropriation in Iran of late 2019. Proceedings of the ACM on Human–Computer Interaction 6(CSCW2): 1–21.

Harris K (2013) The rise of the subcontractor state: Politics of pseudo-privatization in the Islamic Republic of Iran. *International Journal of Middle East Studies* 45(1): 45–70.

Harris K (2020) Unravelling the middle classes in post-revolutionary Iran. In: Samiei M and Harris K (eds) *Rethinking Class and Social Difference*. Bingley: Emerald Publishing Limited, 103–134.

Human Rights Watch. (2022) Iran: Human rights groups sound alarm against draconian internet bill. Available at: https://www.hrw.org/news/2022/03/17/iran-human-rights-groups-sound-alarm-against-draconian-internet-bill (accessed 13 August 2025).

Mehran N and Vadiati N (2024) Cities in custody: Urban development as spatial proxy of ideological coloniality · BG · berlinergazette.de · EN|DE. Available at: https://berlinergazette.de/cities-in-custody/ (accessed 12 August 2025).

Meulbroek C and Glassman J (2025) The national security state and the tech city: Social structures of militarisation in Seattle's long cold war. *Antipode* 57(2): 599–621.

Morozov E (2011) *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs.

Soldatov AA and Borogan IP (2017) *The Red Web: The Kremlin's Wars on the Internet*, First trade paperback edition. New York: PublicAffairs.

Tehran Times. (2024) Over 98% of villages have access to high-speed internet. Available at: https://www.tehrantimes.com/news/500766/Over-98-of-villages-have-access-to-high-speed-internet (accessed 12 August 2025).

Wikipedia. (2025) Amir Emad Mirmirani. Wikipedia. Available at: https://en.wikipedia.org/w/index.php?title=Amir_Emad_Mirmirani&oldid=1299300247 (accessed 12 August 2025).