Policymaking and Institutional Mapping of Surveillance and Interception on Citizens under the Islamic Republic of Iran

Part 3: Street Surveillance and Identity Discovery in the Islamic Republic

Privacy Rights and Surveillance Monitoring (PRISM)
Holistic Resilience, Inc., December 2025

Policymaking and Institutional Mapping of "Surveillance and Interception" on Citizens under the Islamic Republic of Iran

***

Part 3: Street Surveillance and Identity Discovery in the Islamic Republic

---

This report investigates how the Islamic Republic of Iran has institutionalized street level surveillance to enforce ideological control over public life. Focusing on the mandatory hijab policy, it examines the gradual shift from human centric enforcement to a hybrid model combining CCTV systems, telecom metadata, national ID databases, and AI enhanced tools. While full fledged facial recognition remains technically out of reach, the regime has created a layered ecosystem capable of semi automated identity discovery linking mobile devices, license plates, and smart ID cards to behavioral monitoring.

December 2025

Privacy Rights and Surveillance Monitoring (PRISM)

***

Holistic Resilience

Abstract

Policymaking and Institutional Mapping of "Surveillance and Interception" on Citizens under the Islamic Republic of Iran; Part 3: Street Surveillance and Identity Discovery in the Islamic Republic

This section analyzes the Islamic Republic's transition from traditional street-level enforcement to a hybrid digital surveillance model aimed at identifying and controlling citizens in public spaces. The report traces how the Islamic Republic of Iran has integrated surveillance cameras, telecom metadata, smart ID systems, and citizen reporting platforms into a layered infrastructure for identity discovery particularly in the context of enforcing mandatory hijab laws.

Evidence suggests that these capabilities remain largely aspirational. Instead, the state relies on a patchwork of localized systems, combining imported Chinese surveillance hardware, pilot AI algorithms, and national identity-linked databases such as SHAHKAR, HAMTA, and SAPTAM. Platforms like the NAZER app facilitate crowdsourced monitoring, while judicial and law enforcement actors exploit middleware systems to cross-reference metadata with personal records, enabling semi-automated sanctions without direct confrontation.

This hybrid approach reflects a broader policy shift: from religious and cultural indoctrination to data driven repression. Legal frameworks such as the Hijab and Chastity Law (2023) institutionalize this model, mandating public and private entities to provide real time access to CCTV footage, location data, and personal identifiers. The Islamic Republic's urban surveillance architecture thus functions not as a unified AI based system, but as a fragmented network of interoperable data points, capable of enforcing ideological norms through digital infrastructure..

Privacy Rights and Surveillance Monitoring (PRISM)

Holistic Resilience, Inc.

December 2025

Table of Contents

Glossary of Abbreviations

Acronyms:	Full Term:

Islamic Republic of Iran Bodies:

CRA	Communications Regulatory Authority
FARAJA	Islamic Republic of Iran's Law Enforcement Forces; Police
FATA	Islamic Republic of Iran's Cyber Police
IRGC	Islamic Revolutionary Guard Corps
IRGC-IO	IRGC Intelligence Organization
ITO	Information Technology Organization of Iran
MIMT	Ministry of Industry, Mine and Trade
Ministry of ICT	Ministry of Information and Communications Technology
MOIS	Ministry of Intelligence
NCC	National Center for Cyberspace
NIN	National Information Network
NOCR	National Organization for Civil Registration of Iran
SCC	Supreme Council of Cyberspace
SCCR	Supreme Council of Cultural revolution
SCNS	Supreme Council of National Security
TCI	Telecommunication Company of Iran
TIC	Telecommunication Infrastructure Company

State-Controlled Surveillance and Interception Systems:

EMTA	E-commerce Customer Authentication System
HAMTA	Smart System of Communication Devices Registry
HODA	Iranian Digital Identity Authentication System
SAMAVA	National Identity and Verification Gateway
SANA	Online Judicial Authentication System
SHAHKAR	Users Authentication Network
SHAMSA	National lawful intercept data archive system
SIAM	Integrated System for Telecommunication Inquiries

General and Technical Terms:

AAA	Authentication, Authorization, Accounting
API	Application Programming Interface
APT	Advanced Persistent Threat
ETSI	European Telecommunications Standards Institute
IMEI	International Mobile Equipment Identity

IMSI	International Mobile Subscriber Identity
ISP	Internet Service Provider
MITM	Man-in-the-Middle
SSO	Single Sign-On
TTPs	Tactics, Techniques, Procedures
VPN	Virtual Private Network
3GPP	3rd Generation Partnership Project

Islamic Republic of Iran Groundplay and Main Actors

Street Surveillance and Identity Discovery in the Islamic Republic

In recent years, particularly following waves of mass protests and shifting public attitudes toward mandatory veiling, the Islamic Republic of Iran has launched a coordinated initiative to deploy identity-recognition and digital surveillance technologies in public spaces. These efforts aim to redefine mechanisms of social control through new regulatory frameworks, expanded data infrastructures, and the integration of identity verification systems across urban monitoring networks.

Security and executive agencies are pursuing this agenda along three primary axes: (1) importing advanced surveillance equipment and smart cameras from China; (2) developing domestic algorithms through university research and government-affiliated knowledge-based firms; and (3) linking existing national service databases such as SHAHKAR, HAMTA, HODA, SANA, and SEPTAM to networks of CCTV cameras, SIM cards, and national ID systems. In many cases, the infrastructure remains in a “pre data” phase: a stage in which visual, audio, and geolocation data are being collected, but full integration with intelligent analytic systems is not yet operational.

Due to persistent algorithmic limitations especially in tasks like accurately detecting veiling status or identifying participants in protests, the regime has adopted hybrid enforcement models. These rely on a mixture of human operated cameras, mobile apps used by field agents, and backend digital platforms. In this architecture, the application of social control policies ranging from facial recognition to SMS based warning systems, takes a decentralized, adaptive form.

Despite its technological shortcomings, the Islamic Republic’s surveillance model is evolving toward a digital authoritarianism structurally aligned with the Chinese approach. It monitors

citizens through their digital identity and enforces ideologically charged laws such as those governing veiling via a complex fusion of data, imagery, behavioral patterns, and coercive regulation. This trajectory carries far reaching consequences for civil liberties, digital rights, and modes of resistance in the Iranian public sphere.

Authoritarianism and Religious Ideology in Surveillance and Identity Verification Strategies

In contemporary authoritarian regimes, particularly in the post-digital era, identity verification in public spaces is no longer merely a security measure. It has become a core mechanism for exercising political power, engineering social behavior, and controlling bodies and everyday actions. Technologies such as surveillance cameras, biometric systems, mobile phone trackers, and interconnected databases are not deployed to preserve public order, but rather to identify, categorize, and manage social actors.

One of the most emblematic cases of techno-authoritarian governance is the Social Credit System developed by the People's Republic of China.[1] This model monitors citizens' behavior in urban, economic, and digital domains[2] and assigns scores based on predefined criteria.[3] Although the system has not been implemented nationwide and remains largely confined to

[1] Drew Donnelly; Horizons; "China Social Credit System Explained – What is it & How Does it Work?"; Feb. 11, 2024; Link, Archive
Zeyi Yangarchive; MIT Tech. Rev.; "China just announced a new social credit law; Here's what it means"; Nov. 22, 2022; Link, Archive

[2] Ms. Smith; CSO; "Skynet in China: Real-life 'Person of Interest' spying in real time"; Sep 26, 2017; Link, Archive
Raymond Zhong; NY Times; "China Snares Tourists' Phones in Surveillance Dragnet by Adding Secret App"; Jul. 2, 2019; Link, Archive

[3] Paul Mozur; NY Times; "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras"; Jul. 8, 2018; Link, Archive

local pilot projects,[4] its conceptual foundation, the fusion of technological surveillance with social consequences, has inspired governments such as the Islamic Republic of Iran.[5] While technical and social complexities in China have led to a focus on legal violations rather than universal behavioral control,[6] the Iranian model pursues a more ideological and security driven trajectory.

Beyond the general patterns of authoritarian governance focused on technological control of public space, the Islamic Republic of Iran has additional motivations to develop such systems. In addition to conventional security concerns aimed at managing civil unrest, the regime follows an ideological and religious doctrine in which a specific model of mandatory dressing code, namely hijab, is interpreted not merely as a dress code for women but as a symbol of loyalty to the state's religious authoritarian order.

In the Islamic Republic, hijab is not simply a cultural norm or a religious obligation; it has become a central tool for managing citizens' bodies and identities. Unlike some Muslim-majority countries where adherence to hijab is treated as a personal religious choice, in Iran, violating mandatory hijab laws is considered a state offense punishable under security and legal frameworks. As a result, a wide array of mechanisms has been designed to identify and penalize individuals who violate this rule, from morality police patrols to urban and digital

---

[4] Vincent Brussee; MERICS; "China's social credit score – untangling myth from reality"; Feb 11, 2022; Link, Archive
Jessica Reilly, Muyao Lyu, Megan Robertson; The Diplomat; "China's Social Credit System: Speculation vs. Reality"; Mar. 30, 2021; Link, Archive

[5] Paul Mozur, Aaron Krolik; NY Times; "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers"; Dec. 17, 2019; Link, Archive
Jeremy Daum; The Jamestown Foundation, China Brief; "Far From a Panopticon, Social Credit Focuses on Legal Violations"; Volume: 21, Issue: 19, Oct. 8, 2021; Link, Archive

[6] Nectar Gan; The China Morning Post; "The complex reality of China's social credit system: hi-tech dystopian plot or low-key incentive scheme?"; Feb. 7, 2019; Link, Archive
BBC; "In Your Face: China's all-seeing state"; Dec. 10, 2017; Link, Archive
Lily Kuo; The Guardian; "China bans 23m from buying travel tickets as part of 'social credit' system"; Mar. 1, 2019; Link, Archive

surveillance technologies. The state employs hijab as an entry point to build broader infrastructures of identity management and social control, infrastructures that can easily extend to other forms of civil disobedience.

Within this framework, public urban space, from streets and subways to parks and shopping centers, is no longer a neutral environment for movement but a terrain of state enforcement. The citizen is no longer an anonymous individual in a crowd but a traceable and identifiable subject whose behavior must be monitored.[7] The state enforced hijab, which superficially presents as a religious or moral obligation, has effectively become a platform for deploying identity recognition systems, digital verification mechanisms, and general purpose surveillance technologies. Initially introduced under the pretext of combating immodesty, these tools rapidly evolve into mechanisms that target other socially defiant groups, including protesters, civil activists, women, and minorities.

The wave of social uprisings in recent years from January 2018 and November 2019 to September 2022 marked a turning point in the Islamic Republic's control strategies.[8] During this period, the regime gradually shifted away from traditional, physically enforced methods such as the morality police patrols and began adopting more technologically driven and institutionalized surveillance models.[9] This shift was driven by two key factors: first, the declining legitimacy and operational capacity of street patrols, especially following the death of Mahsa Amini in custody and the ensuing public debates around the use of CCTV footage; and second, the increasing availability of technical infrastructure for citizen identification, including facial recognition systems, SIM card tracking, national ID databases, and license plate surveillance.

---

[7] Ali Khamenei, The Supreme Leader of the Islamic Republic of Iran; "Ramadan Meeting with State Officials"; Apr 4, 2023; Google Translated Link, Archive

[8] Erwin van Veen, Hamidreza Azizi; Clingendael, The Netherlands Institute of International Relations; "Protests in Iran in comparative perspective"; Mar. 8, 2023; Link, Archive, Download

[9] Amnesty International; "What happened to Mahsa/Zhina Amini?"; Sep. 15, 2023; Link, Archive

A Strategic Shift in the Governance of Compulsory Dress Codes: From Cultural Indoctrination to Digital Surveillance

The Islamic Republic of Iran has undergone a marked transformation in its approach to regulating citizens' clothing, shifting from cultural and religious propaganda to a securitized, data-driven surveillance model. Three key resolutions passed by the Supreme Council of the Cultural Revolution; Resolution 413 (1998),[10] Resolution 566 (2005),[11] and Resolution 820 (2019),[12] illustrate this trajectory. These documents show a transition from soft cultural promotion of hijab toward the implementation of informational, operational, and technological enforcement mechanisms. Notably, Resolution 820 for the first time emphasized the use of modern technologies, statistical monitoring, and security reporting, while transferring policy authority from the Ministry of Culture and Islamic Guidance to the Ministry of Interior. This shift signals a paradigmatic change from persuasion to coercive enforcement.[13]

The killing of Mahsa Amini in September 2022, while in custody of the so-called Morality Police, undermined the legitimacy of field patrols and elevated the hijab to the symbol of a national civil resistance movement.[14] In response, rather than scaling back enforcement, authorities in the Islamic Republic doubled down on technological enforcement and the invisibilization of street control. This included the activation of platforms such as Mobile registry, biometric national ID cards, judicial and banking databases, municipal CCTV networks,

[10] SCCR; "Principles, Foundations, and Executive Methods for Promoting the Culture of Chastity"; Feb 3, 1998; Download

[11] SCCR; "Strategies for Promoting the Culture of Chastity"; Jul 26, 2005; Download

[12] SCCR; "Supplementary Executive Measures for Promoting the Culture of Chastity and Hijab'; Sep 3, 2019; Download

[13] Khari Johnson; Wired; "Iran Says Face Recognition Will ID Women Breaking Hijab Laws"; Jan. 10, 2023; Link, Archive

[14] Tirana Hassan; Human Rights Watch; "Iran Events of 2023"; Link, Archive

and mobile applications like Nazer for public crowd-sourced reporting. Under the guise of the Hijab and Chastity Law, these digital instruments have now become formalized tools of identification, monitoring, and repression.

Throughout this period, senior Iranian officials have publicly affirmed the use of digital surveillance to enforce dress codes:

- The Head of the Headquarters for the Promotion of Virtue and Prevention of Vice, stated that municipal CCTV cameras, linked to digital identity systems, are used to send SMS warnings to improperly veiled women.
- The then commander of Islamic Republic of Iran's police (FARAJA), confirmed the use of urban surveillance systems to counter "social irregularities."
- The Chairman of the Judiciary and Legal Committee of the 11th Parliament (2020–2024), declared: "Those who violate norms in public should be identified through facial recognition, not physical confrontation. Once identified, they will be notified and penalized through the suspension of their civil rights."
- The commander of Islamic Republic of Iran's police (FARAJA) Ahmadreza Radan, has repeatedly emphasized that digital surveillance will form the core of police enforcement programs.
- Former Interior Minister Ahmad Vahidi and the Supreme Court Chief Mohammad Jafar Montazeri also confirmed that the law must be implemented using "smart technologies" and "digital tools."

These policy directions were eventually codified in the Hijab and Chastity Law, which legally authorizes tools such as facial recognition, integration with civil registration databases, and public digital reporting systems. The law grants formal powers to the police and judiciary to surveil and penalize citizens through technology.

Hijab Law: Legalizing Digital Surveillance in Public Spaces

A major turning point in the Islamic Republic's surveillance strategy was the passage of the "Law for Supporting the Family by Promoting the Culture of Chastity and Hijab" commonly referred to as the Hijab Law, in October 2023.[15] Framed as a legal mechanism to enforce compulsory veiling in public spaces, the law institutionalizes the role of digital surveillance within Iran's policing framework. It represents the logical continuation of three earlier decrees issued by the Supreme Council of the Cultural Revolution, which outlined the transition from "cultural promotion" to "intelligent control" in the regulation of women's dress.

Multiple provisions of the law lay out the structural foundation for identifying and managing citizens' identities in urban spaces. Article 14 obliges the Ministry of Interior to develop "regional social profiles," enabling localized cultural engineering. Article 23 tasks the Ministry of ICT with accelerating the development of the National Information Network (NIN), under the supervision of the Supreme Council of Cyberspace. Article 25 assigns intelligence duties to the Ministry of Intelligence and the IRGC Intelligence Organization, mandating them to use digital tools to track and prosecute individuals involved in "removing the hijab," "nudity," or sending images to foreign media outlets.

The law's most direct application of surveillance technologies appears in Article 29, which obligates the Islamic Republic's police (FARAJA) to identify and penalize improperly veiled individuals using "fixed and mobile cameras," "artificial intelligence," "citizen reports," and "identity verification systems." This provision represents the clearest institutional convergence of surveillance technology and state enforcement mechanisms.

[15] "Law for Supporting the Family by Promoting the Culture of Chastity and Hijab"; Oct 2023; Download

To compensate for technological gaps, Article 31 designates the Basij as a human auxiliary force for judicial officers. Sub-articles of Article 33 extend surveillance practices into the realm of employment and social services, making adherence to hijab regulations a prerequisite for hiring, promotion, or obtaining work permits.

Finally, Article 64 of the law formalizes the institutional infrastructure for digital surveillance: all government bodies, banks, private companies, and even individuals are mandated to provide access to their CCTV footage and to enable police access to citizens' identity information, including national ID numbers, mobile data, and geolocation. In this sense, the Hijab Law functions not merely as a cultural or moral policy but as a legal blueprint for the systematic expansion of digital governance in the Islamic Republic.

Facial Recognition Deployment in Public Spaces: Policy, Technology, and Field Realities

The Islamic Republic of Iran, through both official legislation and extralegal mechanisms, is actively pursuing the design and implementation of a technological system aimed at identifying and verifying the identity of citizens in public spaces, primarily to enforce the mandatory hijab policy. But how is this ambitious project progressing in practice? Have facial recognition systems and digital tracking technologies been widely and operationally deployed across the country as claimed? Or are they still facing significant limitations in infrastructure, technical capabilities, and algorithmic development?

Field evidence suggests that, rather than implementing a centralized national system, the Islamic Republic's security forces have opted for fragmented, localized, and hybrid solutions. This model relies on the scattered capacities of individual institutions and cities. In specific locations such as metro stations or shopping centers, monitoring and identification systems have been installed, but these systems lack national integration. In many cases, key components of the project are not domestically developed but imported, particularly in the area of surveillance hardware such as urban cameras, license plate recognition systems, and data storage devices. At this stage, Iran's security infrastructure resembles what can be described as a "pre-data" phase.[16] In this model, similar to the Chinese approach, images, audio, and geolocation data are collected and stored, yet full integration between analytic systems and national identity databases has not been established.

[16] The "pre-data" phase refers to a stage in which information-gathering infrastructures, such as surveillance cameras, microphones, or tracking devices, have been deployed, but the collected data has not yet been processed analytically, classified, or integrated into AI powered systems. This phase constitutes a necessary precursor to the development of analytical engines in digital surveillance and decision-making architectures.
Sandra Wachter, Brent Mittelstadt; Columbia Business Law Review; "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI."; vol. 2019, no. 2, Oct. 5, 2018; Link, Archive

Claims of Facial Recognition Implementation and the Reality on the Ground

Official media coverage and statements by senior officials of the Islamic Republic of Iran in recent years have projected the image of an advanced surveillance system that leverages AI-powered cameras, linked to national identity databases, to identify individuals in public spaces and automatically issue warnings or impose penalties. Within this narrative, facial recognition algorithms are presented as the primary mechanism, especially for enforcing mandatory dress codes targeting women.[17]

However, field assessments and visual evidence suggest that this portrayal reflects a propagandistic and exaggerated projection more than a technical reality. There is little indication that such facial recognition systems have been implemented nationwide; at best, they may have been deployed in limited pilot projects confined to high-traffic areas such as recreational centers or commercial districts.[18]

Although the previous section highlighted the Islamic Republic's policy orientation and rhetorical commitment to deploying facial recognition technologies for direct, automated surveillance, independent investigations and verifiable data do not support the claim that such capabilities are being implemented widely or in real-time across Iranian cities. These claims remain more speculative and aspirational than operational, often reflecting public anxieties and dystopian forecasting rather than existing technical capacity.[19]

That said, past experience indicates that the Islamic Republic is capable of executing long-term projects that initially seemed implausible. A case in point is the NIN, which began in the 2000s

[17] Sanam Mahoozi; Thomson Reuters Foundation; "Mahsa Amini death: facial recognition to hunt hijab rebels in Iran"; Sep. 21, 2022; Link, Archive

[18] Melody Kazemi, Azin Mohajerin; Filter Watch; "Surveillance and Secrecy: Examining Iran's Claims on the Use of Facial Recognition for Social Control"; Mar 28, 2023; Link

[19] Factnameh; "Evaluating the Exaggerated Claims About AI in Iran's Hijab Enforcement Plan"; Apr 16, 2024; Link

as a loosely defined policy aspiration and gradually evolved into a functional infrastructure for traffic segregation between domestic and global internet. Similarly, while there is currently no functional national facial recognition network, other tools such as the Nazer system, vehicle plate tracking, and hybrid geolocation technologies based on BTS triangulation and IMSI-Catcher devices are actively being tested and expanded.[20]

In summary, what Iranian authorities promote under the labels of artificial intelligence and facial recognition is not a coherent, nationwide, and operational surveillance infrastructure, but rather a fragmented and opaque collection of limited, mostly experimental projects. These systems lack transparency, reliability, and a unified domestic algorithmic framework. Nonetheless, the regime's investment in passing new legislation, importing critical technologies, and building executional infrastructure suggests that surveillance and identity detection in public spaces, though currently limited, are progressing incrementally toward a long-term strategy that combines physical enforcement with digital control.

Importing Surveillance Equipment from China with Facial Recognition Capabilities

In the absence of a robust domestic infrastructure for facial recognition at a national level, security forces of the Islamic Republic have focused on importing equipment that could eventually be integrated with such algorithms. Leading these imports are visual surveillance

[20] Access Now; "Weapons of control, shields of impunity: Internet shutdowns in 2022"; Feb. 28, 2023; Link, Archive, Download

technologies from the People's Republic of China, currently the largest exporter of surveillance infrastructure to authoritarian governments worldwide.[21]

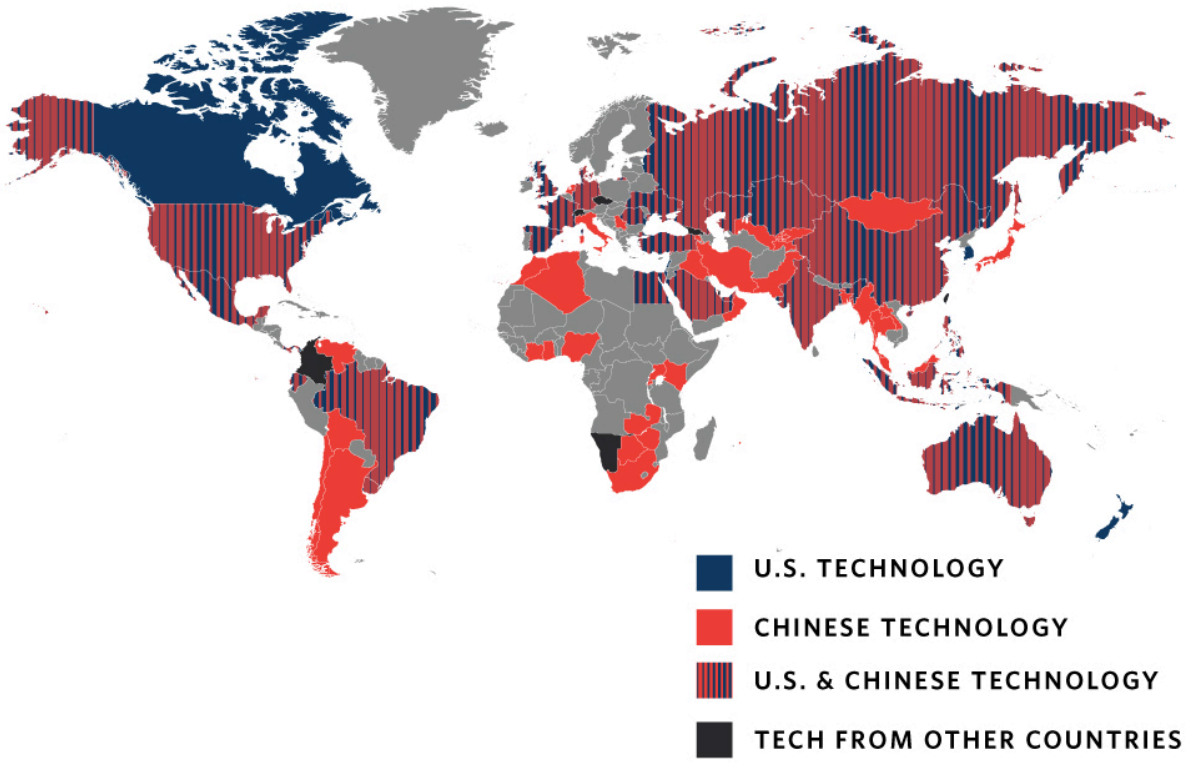
Even the most advanced smart cameras are primarily designed to identify faces or individuals not to interpret nuanced social behavior. Determining whether a specific act (such as a woman's manner of dress) constitutes a legal violation remains contingent upon human judgment or rigid rule based visual classification systems. In Iran, as in China, this presents a significant obstacle to the full automation of behavioral surveillance.

Despite these algorithmic limitations, the Islamic Republic continues to build out its technical infrastructure. Many of the Chinese companies supplying these technologies are sanctioned by the United States or the European Union. Nevertheless, Iranian security agencies and municipal authorities proceed with importation, installation, and operational deployment through commercial intermediaries or unofficial procurement channels. These partnerships not only enhance the technical capacity for domestic repression but also reflect Iran's strategic alignment with the Chinese model of digital authoritarianism where image based systems are integrated with identity databases as core tools of social control.

[21] Steven Feldstein; Carnegie Endowment for International Peace; "The Global Expansion of AI Surveillance"; Sep. 17, 2019; Link, Archive, Download, AI Global Surveillance (AIGS) Index

MAP 1

AI Surveillance Technology Origin



Despite these algorithmic limitations, the Islamic Republic continues to pursue infrastructure development. Many of the Chinese firms supplying these technologies appear on US or EU sanctions lists, yet Iranian security agencies and municipal authorities have continued to import, install, and operate these systems through commercial intermediaries or unofficial procurement channels.[22] These collaborations not only strengthen the technical apparatus of domestic repression but also reflect a strategic alignment with the Chinese model of digital

[22] Tate Ryan-Mosley; MIT Tech. Rev.; "This huge Chinese company is selling video surveillance systems to Iran"; Dec. 15, 2021; Link Archive

governance,[23] one in which image based surveillance systems are fused with national identity databases to form a central mechanism of social control.[24]

Chinese firms and their multiple, parallel representatives in Iran, such as Tiandy Technologies, Zhejiang Uniview, Hangzhou Hikvision, Zhejiang Dahua, and others, have played an active role in providing surveillance infrastructure to Iranian military and intelligence institutions. Several of these companies have also been subjected to international sanctions by the United States and the European Union.

Beyond the import of visual surveillance hardware, the Islamic Republic has cultivated strategic partnerships with major Chinese telecommunications corporations such as Huawei and ZTE in the domain of communications and monitoring infrastructure. These partnerships include the transfer of technologies that enable wide-scale surveillance of telephone, internet, and mobile communications.[25] For instance, in 2010, ZTE signed a €98.6 million contract with the Telecommunication Company of Iran (TCI) to supply advanced monitoring systems capable of intercepting both voice and internet traffic.[26] Although this collaboration triggered international backlash at the time, similar engagements with Huawei have persisted. The company stands accused of selling surveillance technologies to Iran and is believed to have played a key role in the development of the Islamic Republic's digital communications control infrastructure.[27]

Simultaneously, security institutions of the Islamic Republic have drawn inspiration from China's surveillance architecture, particularly large scale projects like Skynet and the technologies

---

[23] Tehran Times; "Senior MP: Iran-China cooperation plan is a win-win game"; Apr. 12, 2021; Link, Archive

[24] SCSP, Foreign Policy Panel; "Defending Digital Freedom and the Competition for the Future of the Global Order"; Dec. 2022; ; Download

[25] Iran Watch; "Investigative Report on the U.S. National Security Issues Posed by the Chinese Telecommunications Companies Huawei and ZTE"; Oct. 8, 2012; Link, Archive

[26] Light Reading; "ZTE Defends Iran Position"; Mar. 28, 2012; Link, Archive

[27] Charles Custer; Tech in Asia; "How Huawei Helped Iran Spy on Citizens and Why Brand China is Poison"; Dec. 6, 2012; Link, Archive

developed by Chinese firms such as Megvii and CloudWalk. China's Skynet initiative, designed to monitor public spaces, integrates millions of cameras with facial recognition algorithms to enable real-time tracking of individuals. It is considered one of the world's most advanced digital governance systems.[28] Megvii, through its Face++ platform, has developed highly accurate facial recognition algorithms capable of real-time image analysis and cross-referencing with national databases.[29] Meanwhile, CloudWalk has come under criticism for exporting facial recognition technologies to countries at high risk of human rights violations. The company has played a central role in China's surveillance export strategy, particularly in the development of facial behavior analysis and large-scale facial image databases.[30]

The appeal of such technologies to the Islamic Republic is evident especially for identifying "unveiled women" or participants in protest gatherings. Both Megvii and CloudWalk are listed under U.S. Treasury Department sanctions.

Ultimately, even in the absence of immediate access to advanced or integrated facial recognition algorithms, possession of such hardware constitutes the first operational layer of facial recognition systems. More precisely, Iran has entered the pre-data phase: a stage in which raw data (images, locations, audio, and ...) are collected and stored, though not yet systematically linked to analytical engines or decision-making frameworks. Nevertheless, this foundational infrastructure could soon pave the way for deploying domestic or imported

---

[28] Chen Shuibo, Li Zhen; People's Daily; "What Does Skynet Monitor?"; Nov. 20, 2017; Link, Archive
David Sehyeon Baek; "Skynet Project in China - The Rise of Ubiquitous Surveillance"; Oct. 31, 2024, Link, Archive
Thomas J Ackermann; "What is China's SKYNET (yes: it is what you think it is)"; May 10, 2019; Link, Archive

[29] Masha Borak; SCMP; "Why one of China's largest facial recognition companies faces a US ban"; Sep. 20, 2019; Link, Archive
Bernard Marr; Forbes; "The Amazing Ways Chinese Face Recognition Company Megvii (Face++) Uses AI And Machine Vision"; May 24, 2019; Link, Archive

[30] Bulelani Jili; EPIC; "The Rise of Chinese Surveillance Technology in Africa"; May 31, 2022; Link, Archive
Amy Hawkins; Foreign Policy; "Beijing's Big Brother Tech Needs African Faces"; Jul. 24, 2018; Link, Archive

algorithms, marking a new chapter in Iran's vision of digital governance through image-based surveillance.

Domestic Development of Facial Recognition: Projects, Actors, and Field Deployment

In the absence of broad access to advanced algorithms and under conditions of technology sanctions, the Islamic Republic has pursued the domestic development of facial recognition systems through a network of private companies, research institutions, and state-affiliated entities. While these initiatives are often framed as "knowledge-based" or "applied research" projects, they operate in close alignment with security and judicial bodies. Their primary focus lies in developing machine learning algorithms to analyze facial features, match images to identity databases, and monitor public behavior in urban spaces.

Among the more prominent companies in this domain is Yaftar, known for its previous collaboration with the Filtering Committee on smart filtering initiatives.[31] Field reports further indicate that projects related to image analysis, behavioral monitoring, and facial identity recognition have been commissioned by entities such as the Passive Defense Organization, the Ministry of Intelligence, and FATA (the cyber police), and delegated to private firms or university-affiliated research teams.[32]

Although these domestic projects remain in their early stages, they benefit from institutional funding and legal backing. They are often implemented in high-security environments and

[31] Open Sanction; "Yaftar Pajoohan Pishtaz Rayanesh"; Link

[32] CIRA; "Iranian Companies Provide Facial Recognition Services to Government and Security Services"; May 22, 2023; Link, Archive

limited urban zones, such as public transportation systems, shopping centers, and busy thoroughfares. These initiatives allow the Islamic Republic to operate semi-automated identity recognition systems even in the absence of imported advanced technologies.

The experimental implementation of facial recognition algorithms in Iran has primarily occurred in semi enclosed and controlled environments. Several domestic news outlets have reported the use of AI powered facial recognition systems in commercial centers, metro stations, and major urban intersections. However, field evidence suggests that most of these systems have not reached full operational capacity and remain confined to localized pilot programs. The absence of centralized data analysis infrastructure, the lack of stable indigenous algorithms, and persistent challenges in linking these systems to national identity databases have all hindered the development of a nationwide implementation.

Identity Infrastructure and Street Surveillance: Linking Data, Cameras, and National Databases

While facial recognition algorithms have not yet been widely deployed in Iran's public spaces, the country's urban surveillance infrastructure and national databases function as the backbone of its identity tracking system. In the Islamic Republic's surveillance architecture, institutions such as municipalities, the Ministry of Roads and Urban Development, banks, and the police (FARAJA) have built an extensive visual monitoring network through urban, roadside, and banking cameras. Though originally established to manage traffic and banking security, this infrastructure has increasingly become a key instrument for identifying citizens in public spaces.

A critical component of this infrastructure is the nationwide network of urban, roadway, and banking surveillance cameras, which has been expanded in recent years to cover high-traffic public areas. Initially deployed for traffic control and recording driving violations, this network is now repurposed for state security objectives.

One of the central systems in this network is SAPTAM (National Integrated Visual Surveillance System), which aggregates footage from cameras placed in streets, shopping centers, and government buildings, and feeds the data directly to FARAJA. According to Article 64 of the "Hijab and Chastity Law," all public institutions, commercial establishments, and banks are legally required to share their surveillance footage with the police. SAPTAM, or the Public Spaces Visual Surveillance Platform, was developed in cooperation with the Police for Public Places Oversight and the National Licensing Portal. Its stated purpose is to standardize, authorize, and monitor CCTV systems in commercial venues and public spaces.

SAPTAM functions as a regulatory authority that assesses and approves the quality of surveillance systems (CCTV) in commercial establishments. These certifications are issued based on laboratory standards, and SAPTAM inspectors supervise the process of camera installation and placement. Once these cameras are deployed, in the event of an incident or crime in a commercial or public space, the Police for Public Places (FARAJA) can access the recorded footage for investigation. Businesses are linked to the police oversight system via the National Licensing Portal and can review the technical specifications of approved surveillance equipment for their sector through the SAPTAM interface. Upon approval, SAPTAM may install a designated number of cameras, depending on operational needs, within exchange bureaus or shops. The footage from these cameras is stored on a cloud based platform provided by SAPTAM, enabling law enforcement to access visual data from private spaces when required.

The data backbone of surveillance projects in the Islamic Republic is supported by a constellation of national databases that contain biometric and civil identity information. These include the Smart National ID Card system (HODA), the Civil Registry Organization, judicial authentication platforms such as SANA, driver's license and passport databases, and banking institutions, all of which serve as potential sources for cross-referencing image data with personal identity profiles.

Hybrid Systems and Field Deployment: Data Networks Linked to Digital Identity

Over the past few years, the Islamic Republic's urban surveillance strategy has evolved from exclusively human led and on the ground monitoring to a hybrid model, integrating both technology and human agents for identity discovery and social control. Traditional human based methods such as morality patrols, Basij field reporting, or direct police observation remain in use, but they face serious limitations in terms of scalability, especially in the context of widespread civil disobedience. The regime cannot maintain physical presence in all urban spaces or respond to incidents in real time. To address this, a new model has emerged: human agents initiate the monitoring process; digital systems record and analyze the data; and punitive messages or alerts are sent to individuals automatically without the need for direct police intervention.

This shift does not diminish the role of human actors but rather redefines their function: from direct enforcers to initiators of a data processing chain. Such a hybrid approach enables the Islamic Republic to leverage the linkage between various databases and surveillance tools including facial images and geolocation data to identify, warn, and penalize citizens. In this

section, we examine the core components of this model, its supporting systems, and concrete examples of its field level implementation.

The goal of this infrastructure is to build a unified mechanism for identity discovery in public spaces. In this system, identity is derived from a combination of visual data (urban CCTV), identity credentials (such as national ID cards or SIM cards), and institutional linkages (such as connections to police or judiciary platforms). Even in the absence of functional AI powered facial recognition, the integration of these elements enables the identification of individuals through license plates, phone numbers, or home addresses. As highlighted in international reports, these systems increasingly function as either substitutes or complements to facial recognition in field operations.[33]

Examples of such integrations can be seen in systems like SAPTAM, which cross-reference public reports or surveillance footage with identity data to refer individuals to interrogation or legal processing platforms. Other components of this evolving network include SHAHKAR (for linking SIM cards to national ID numbers) and HAMTA (for tracking mobile phone devices). Together, these systems form an identity centric data surveillance infrastructure that allows for identity discovery even in the absence of advanced algorithmic tools.

This data network, in conjunction with the Islamic Republic's hardware imports and domestic algorithmic efforts, constitutes the third pillar of its national identity surveillance architecture. If AI algorithms represent the "eyes" of this system, and Chinese hardware the "body," then these identity-linked databases serve as its "brain and memory." Without this backbone, the connection between image and identity would remain impossible; with it, identity discovery becomes operational—even without sophisticated AI engines.

[33] Freedom House; "Freedom Net 2024"; Jun 2024; Link, Archive

Role of the “21st of Tir” Headquarters and Field Operations by the IRGC-Basij

In response to public protests and the growing challenge to compulsory hijab enforcement, the Islamic Republic has established more coordinated field enforcement structures. One of the most notable is the Tir 21 Headquarters (Gharargah-e 21 Tir), officially affiliated with the Headquarters for the Promotion of Virtue and Prevention of Vice. Working in coordination with the IRGC and Basij, this unit is tasked with “mobilizing volunteers to confront improper hijab.” By issuing directives and conducting training sessions, it has organized thousands of Basij members across Iranian cities to identify women deemed “improperly veiled,” and has equipped them with semi-official judicial authorization cards to participate in the enforcement of the Hijab Law. A parliamentary research report explicitly confirms the presence of “Basij officers” alongside police forces. This role has been codified in Article 31 of the Hijab and Chastity Law.

The NAZER App: Crowdsourced Surveillance

A key tool for converting citizen reports into actionable data is the NAZER app, developed by Iran’s Law Enforcement Command (FARAJA). This application allows users to directly send photos, videos, or geolocation data of “improperly veiled” or “norm-violating” individuals to the police. These reports are then processed by FARAJA’s system and may result in SMS warnings or fines. According to reports, NAZER is also integrated with national identity and vehicle registration systems, enabling law enforcement to identify individuals based on license plates or mobile numbers.[34]

[34] Azin Mohajerin, Amir Rashidi; FilterWatch; “Nazer App: How Iran is Using Technology to Suppress Women’s Rights”; Jan 5, 2024; Link

Facial Recognition as a Complement to Data-Based Surveillance

Alongside facial recognition algorithms and imported surveillance hardware, the Islamic Republic has increasingly focused on linking identity data with visual and telecom surveillance infrastructure. Contrary to popular belief, identifying citizens in public does not necessarily require complex facial recognition systems. Rather, integrating national data platforms from smart ID cards and SIM registration systems to SHAHKAR and HAMTA enables identification even in the absence of advanced AI.[35]

For example, during the hijab enforcement campaign in 2025 in cities such as Mashhad, Tehran, Shiraz, and Isfahan, individuals were not identified via facial scans, but through vehicle plate numbers, ownership records, mobile data, and civil registry databases. This model shows that when urban camera systems are connected to national databases, they function as effective supplements to facial recognition.

Systems like SHAHKAR, HAMTA, and smart ID linked SIM registration, along with traffic enforcement cameras, form a surveillance backbone that can identify individuals without using facial algorithms. Notably, Article 64 of the Hijab and Chastity Law mandates all public agencies and service providers to grant the police access to surveillance footage, national IDs, location data, phone numbers, and other personal information. This policy affirms that even in the absence of AI based facial recognition, dispersed identity linked data is sufficient for surveillance operations.

In this view, facial recognition is not the starting point of surveillance in Iran, it is the final layer of an already functional identity racking system built on pre-existing national, financial,

[35] Filter Watch; Solmaz Eikder; "A Battlefield Named Isfahan: Targeted Use of IMSI-Catchers and Surveillance Cameras to the Enforce Chastity and Hijab Law"; Apr 17, 2025; Link

communication, and video datasets. The Islamic Republic has already operationalized semi automated identification in public spaces by combining digital surveillance with data integration, even if its claims of artificial intelligence use remain exaggerated.

Devices such as IMSI-catchers are merely entry points in this broader architecture. By simulating cellular towers, they capture the IMSI and mobile numbers of nearby users. However, these identifiers alone are insufficient for attribution.[36] For raw telecom metadata to become actionable identity profiles, the state relies on intermediary platforms that match phone numbers or device IDs with official identity, family, judicial, or financial records.

Middleware systems such as HAMTA, SHAHKAR, SIAM, HODA, SANA, and Eshraf serve as analytical layers. When connected to field tools like cameras or IMSI-catchers, these platforms allow security agencies to rapidly determine an individual's identity, location, legal history, or family background.[37]

Following initial rollouts in Isfahan, scattered reports have emerged from cities such as Rasht (Gilan Province), where new cameras were reportedly installed and SMS alerts sent to drivers. In Shiraz and Tehran, local activists have observed similar enforcement tactics, particularly in commercial zones or high-traffic areas where officers observe, photograph, extract license plate or mobile information, and issue warnings or initiate legal action. These patterns suggest that the Islamic Republic, rather than building a single national system, is developing localized surveillance hubs linked to centralized data platforms.

[36] EFF; "Cell-Site Silulators, IMSI Catchers"; Link

[37] Access Now; Weapon of Control, Shields of Impunity"; Feb 2023; Download

Assessment of Capabilities and Future Use in Protest Crackdowns

Ultimately, the Islamic Republic's layered and hybrid model of public surveillance marks a transition from traditional monitoring to semi digital population control. But are these systems mature enough for sustained, nationwide deployment?

The evidence suggests that the current model remains in a pre-mature phase: fragmented infrastructure, lack of full software integration, and technical and legal limitations still impede China-style real-time surveillance. Tools like IMSI-catchers, basic facial recognition, or mobile data monitoring are deployed tactically for targeting specific women or dissidents rather than as part of a centralized, scalable strategy.

Nonetheless, the regime's long-term direction is unmistakable. As seen in the rollout of the National Information Network and the institutionalization of hijab enforcement, short-term inefficiency has not deterred long-term investment. Gradual integration of domestic APIs, Chinese imports, and regulatory support for data linkage all point toward an evolving attempt to shift from pilot projects to full scale operational systems.

Appendix

Glossary