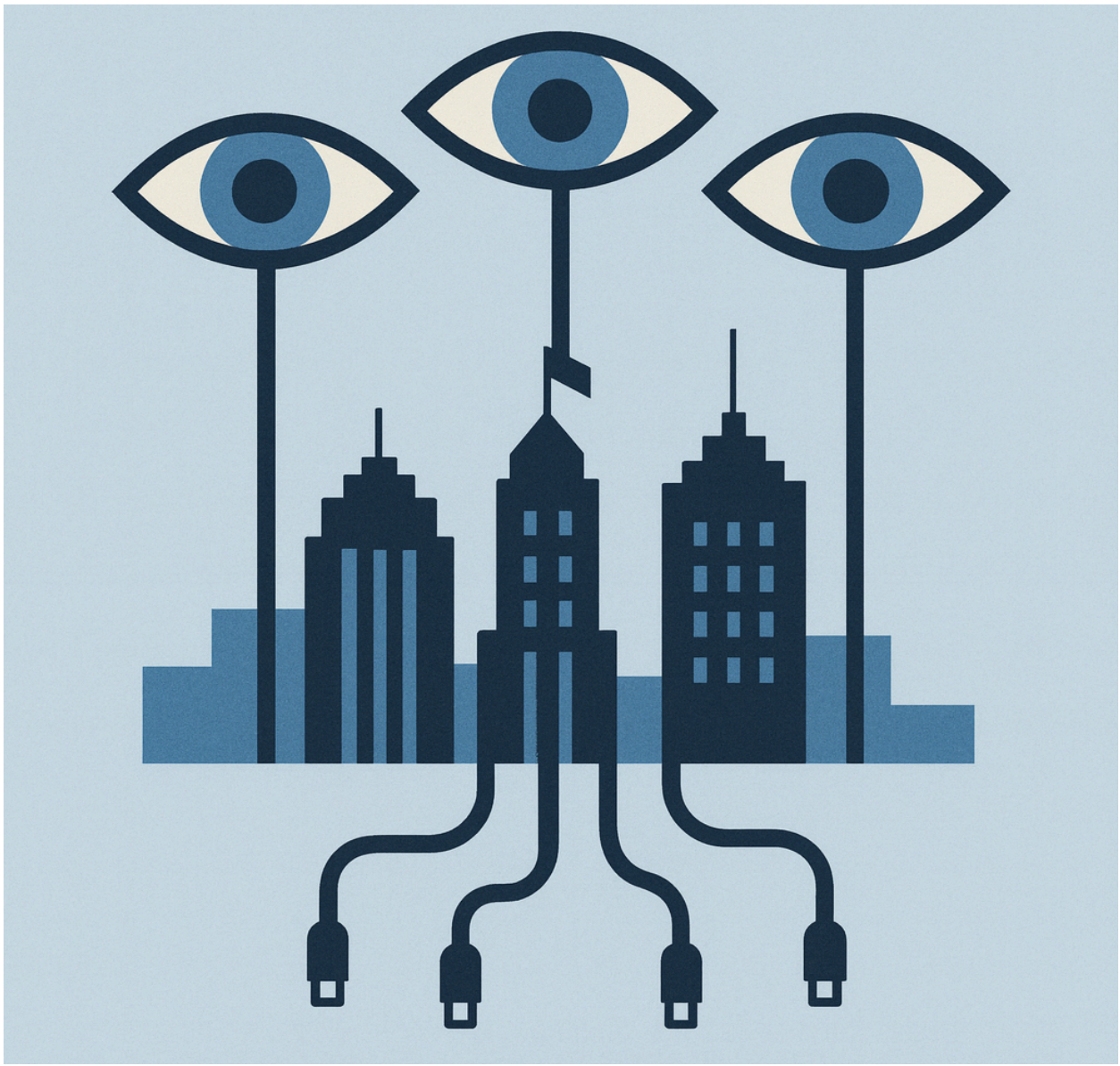
Policymaking and Institutional Mapping of Surveillance and Interception on Citizens under the Islamic Republic of Iran

Part 1: Surveillance Governance and Infrastructures for Interception and Data Access



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 1: Surveillance Governance and Infrastructures for Interception and Data Access

---

This report examines the formal institutional and technical architecture through which state surveillance is structured in the Islamic Republic of Iran. It analyzes how legal mandates, regulatory bodies, telecommunications infrastructure, and centralized data systems enable interception, lawful access, and large-scale data aggregation. The report shows how surveillance is embedded in official policy, licensing regimes, and national internet infrastructure, forming a durable framework for monitoring communications and enforcing digital control.

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 1: Surveillance Governance and Infrastructures for Interception and Data Access

This report examines the policymaking framework and institutional architecture underpinning surveillance and interception in the Islamic Republic of Iran, with a focus on governance mechanisms, legal foundations, and state-controlled infrastructures for data access. It maps how surveillance and interception are embedded within upstream laws, regulatory frameworks, and internet governance bodies, where oversight and data access are treated as core state functions rather than exceptional security measures.

Part 1 analyzes the role of centralized institutions and policy documents shaping Iran's digital governance, including the National Information Network, lawful interception frameworks, identity verification regimes, and tiered access policies. It demonstrates how these instruments collectively enable systematic monitoring of citizens' online and offline activities through both infrastructure-level systems and formally civilian service platforms. By examining how administrative and identity-based systems are integrated into centralized data and judicial frameworks, the report shows how everyday civic interactions are transformed into data streams subject to state oversight.

Through institutional mapping and policy analysis, this section establishes the foundational governance logic that enables large-scale surveillance and interception in Iran, setting the stage for subsequent parts of the report that examine covert mechanisms, street-level surveillance, and the international proliferation of these technologies.

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

Table of Contents

List 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

The Status of Surveillance and Interception in IR Iran's Internet Governance Framework

The government of the Islamic Republic of Iran has expanded its capabilities for surveillance and interception of citizens through the use of modern technologies. CCTV networks, facial recognition systems, applications designed to capture or log private user messages, and systems assessing citizens' lifestyle patterns and behavioral profiles collectively provide the Islamic Republic's security agencies with the means for broad and precise monitoring of the population.

One of the central components of these surveillance and interception structures is the National Information Network (NIN),[1] commonly referred to by the public as the "national internet." The NIN is a state-controlled digital infrastructure designed to function as a domestic intranet, enabling authorities to maintain national-level connectivity even if access to the global internet is restricted or cut off. Restrictions on freedom of expression through filtering and censorship, and the obstruction of free information flows through disruptions, platform blocking, or full nationwide and regional shutdowns, constitute the most significant human rights violations associated with this infrastructure.

However, even more significant is the expansion of the NIN's surveillance and interception capabilities across multiple technical layers, each developed with distinct objectives by different governmental bodies. Some of these systems are designed for Mass Surveillance,

[1] ASL19; Citizen Lab; "Iran's National Information Network"; Nov. 9, 2012; Link, Archive
Center for Human Rights in Iran; "Guards at the Gate; The Expanding State Control Over the Internet in Iran"; Jan. 2018; Download
Article19; "Iran: Tightening the Net"; Sep. 2020; Link, Download Persian Version

while others enable targeted spying, tracking, and communication interception. These systems are examined in the sections that follow.

Surveillance and Interception in the Protection Bill

In recent years, the Islamic Republic's parliament advanced the "Regulatory Framework for Digital Services Bill," widely known to the public as the "Protection Bill."[2] After facing significant public opposition and criticism from civil society, the bill was pushed forward through a complex and semi-clandestine procedure allowing it to bypass full parliamentary scrutiny (Article 85 of the Islamic Republic Constitution).[3] Among critical experts, the Protection Bill has been understood as a legal instrument designed to restrict the internet in Iran. Yet a close examination of how the bill emerged and was debated in parliament shows that surveillance and interception have always been among the state's core objectives in this legislative project.

During the nationwide protests of January 2018, the Supreme Council of National Security (SCNS), an entity under the control of the Supreme Leader and composed of senior military and intelligence officials, blocked access to Telegram,[4] claiming the platform played a role in the

[2] "Bill for the Regulation of Domestic Messaging Platforms"; Nov 18, 2018; Download
"Bill on the Protection of Users' Rights in Cyberspace and the Regulation of Social Messaging Platforms"; 2020; Download
"Bill on the Protection of Users' Rights and the Regulation of Basic Application Services"; 2020; Download
"Bill on the Protection of Users' Rights and the Regulation of Basic Application Services"; Jul 17, 2021; Download
"Bill on the Regulatory Framework for Digital Services"; Dec 26, 2021; Download
"Bill on the Regulatory Framework for Digital Services", Jan 29, 2022; Download

[3] RFE/RL, Radio Farda; "Reporters Without Borders: The Protection Bill Is Modeled After 'Chinese-Style Censorship'"; Jul 28, 2021; Link, Archive

[4] BBC Persian; "Telegram 'Temporarily Blocked After Refusing to Cooperate with the Iranian Government'"; Oct 20, 2015; Link, Archive

unrest.[5] In negotiations with Telegram's executives, the Islamic Republic's demands were explicit: access for surveillance, interception, and censorship.[6]

It was this loss of control over communications and media flows, once they moved beyond state-dominated infrastructure, that catalyzed the first draft of the Protection Bill. The bill required foreign platforms to relocate servers containing the data of Iranian users inside the country. The government's main legal pretext for this requirement was the notion of "data residency." Yet, as the Telegram case demonstrates, the Islamic Republic's underlying objective has consistently been the ability to monitor, intercept, and censor Iranian users' communications.

Internet Oversight and Lawful Interception in Iran's "Cyberspace" Governance

The Islamic Republic's demand for extensive access to users' digital activities is not new. In 2001, the Supreme Council of the Cultural Revolution (SCCR), a cultural policy-making body under the authority of the Supreme Leader, approved the "Regulations and Guidelines for Computer Information Networks," one of the earliest building blocks of internet governance in Iran.[7] Under this regulation, the Internet Service Providers were required to submit user activity data to the Ministry of Information and Communications Technology (ICT), which could then transfer it to the Ministry of Intelligence (MOIS) upon request and with judicial authorization.

[5] Washington Post; "Iran just showed it has no intention of improving ties with the West"; Dec. 15, 2020, Link
[6] Pavel Durov post on X (formerly Twitter); Oct. 20, 2015; Link, Archive
[7] SCCR; "Regulations and Guidelines for Computer Information Networks"; Dec 3, 2001; Link, Archive

However, disclosures from the email servers of the judiciary's Filtering Committee show that, in many cases, such data and requests were sent directly from prosecutors to internet companies (see the Part II). This regulation provided an important legal basis for the Islamic Republic's Lawful Intercept system, or what is internally referred to as "information oversight," a system that, from a technical standpoint, represents a significant departure from international privacy standards (see the Section 5).

Ali Khamenei, the Supreme Leader, also established and directly controls the Supreme Council of Cyberspace (SCC), the principal body responsible for internet policy-making. Among its central documents is "Determining the Requirements of the National Information Network (NIN),"[8] which outlines the initial definitions and general principles for six core domains: Communications Infrastructure, Independence, Governance, Services, Security, and the Economic Model. The "Security" domain is the centerpiece of the document, with many of its operational details classified and unpublished.[9] Phrases such as "the ability to monitor, oversee, and enforce governing policies," "a unified and reliable identity management system," and "comprehensive content filtering" reveal an agenda to build mechanisms that, in subsequent years, have enabled security agencies and the IRGC to monitor and surveil ordinary citizens (see image below).

A notable parallel exists between the timing of China's creation of high-level digital governance institutions and developments in Iran. The Cyberspace Administration of China (CAC) was established in 2011,[10] and only months later, in March 2012, the Supreme Leader of the Islamic

[8] SCC; "Definition of the Requirements of the NIN", Dec 20, 2016; Download

[9] In Section Five, "Security", the subsection on "Protection and Management of Interactions within the NIN" outlines various aspects of user activity surveillance, interception, and content filtering (referred to in official terminology as "Content Purification").

[10] Stanford University, Digichina; Jamie P. Horsley; "Behind the Facade of China's Cyber Super-Regulator"; Aug 8, 2022; Link, Archive

Republic established the National Center for Cyberspace (NCC).[11] Both bodies were designed to centralize state control over digital infrastructure, expand regulatory authority, and consolidate policy-making on internet governance. Crucially, in both countries, governments favor the term "Cyberspace" rather than "Internet," framing the digital sphere not as an open global network but as a governable realm subject to state regulation, control, and sovereignty.

[11] "[The Supreme Leader's] Decree on the Establishment and Appointment of the Members of the SCC"; Mar 7, 2012; Link, Archive

۷. تحقق طرح‌های تداوم عملکرد و بازیابی در حوادث؛

۸. پالایش و سالم‌سازی جامع بر مبنای فرهنگ اسلامی- ایرانی؛

۹. حفاظت از اطلاعات طبقه‌بندی‌شده؛

۱۰. حفاظت در برابر اشراف و نفوذ بیگانگان و مقابله با سوءاستفاده آنان از زیرساخت فضای مجازی کشور؛

۱۱. تأمین اشراف اطلاعاتی و رصد، امکان شنود قانونی و نظارت جامع و برخط بر این عملیات؛

۱۲. صیانت از حریم خصوصی، حقوق عمومی و آزادی مسئولانه؛

۱۳. تأمین امنیت عمومی و پشتیبانی از مشارکت‌های اجتماعی کاهنده جرائم و ارتقاء بخش سالم‌سازی و امنیت؛

۱۴. پایداری و بازگشت‌پذیری[۳۳] (زیرساخت‌ها، خدمات و مدیریت).

۴- [غیرقابل انتشار]

۵- "نیازمندی"های[۳۴] سالم‌سازی و امنیت به‌ویژه مدیریت مخاطرات شبکه ملی اطلاعات به‌صورت یک فرآیند مستمر در تمام چرخه طراحی، اجرا، نگهداری، به‌روزرسانی، تغییرات و توسعه این شبکه تأمین شود؛

۶- نیازمندی‌های نظام یکپارچه امنیت و نظام یکپارچه سالم‌سازی در شبکه ملی اطلاعات و زیرنظام‌های هریک، در لایه‌ها، ابعاد و مناطق مختلف شبکه تأمین شود؛

۷- در استقرار، تقویت و به‌روزرسانی نظام‌های سالم‌سازی و امنیت در چارچوب اسناد بالادستی، با تأکید بر تقویت نظام‌های حقوقی، قضایی، انتظامی و امنیتی و شکل‌گیری زیرنظام‌های تعیین‌شده در الزامات قانونی، تسریع[۳۵] شود؛

۸- میان حوزه‌های مختلف مدیریت سالم‌سازی و مدیریت امنیت هماهنگی‌شده و تمامی لایه‌های شبکه ملی اطلاعات شامل و نه محدود به زیرساخت‌ها، خدمات زیرساختی و پایه کاربردی، از آن‌ها پشتیبانی نمایند (با تأکید بر اعمال سیاست‌های سالم‌سازی و امنیت مربوط به تعاملات درونی تا حد امکان[۳۶] در نزدیک‌ترین نقاط به مناطق دسترسی و همچنین استقرار مراکز اشتراک‌گذاری اطلاعات، تحلیل و دانش لازم)؛

۹- [غیرقابل انتشار]

۱۰- [غیرقابل انتشار]

۱۱-تأکید بر ویژگی‌های ذیل در ارائه خدمات توسط شبکه ملی اطلاعات:

Reliable Digital Identity Framework for the "Cyberspace"

Authentication, along with Authorization and Accounting (AAA), forms the backbone of any security framework for accessing digital resources and services. However, when these functions are centralized through unified and government-controlled Single Sign On (SSO) gateways, they become powerful tools for surveillance and interception of citizens. In such architectures, authentication lies at the very heart of every state surveillance system.

In September 2019, the SCC adopted a resolution titled "Reliable Digital Identity Framework for the National Cyberspace", stating that its goal was to "create the necessary infrastructure for secure and trustworthy interactions on the internet."[12] The resolution mandates that all technical, economic, cultural, social, political, and administrative interactions rely on verified digital identifiers.

According to this resolution, all entities on the NIN and its affiliated networks must possess a verified identity, and service providers are required to block any interaction lacking one. Article 3 mandates that all user interactions with the NIN or internal systems such as the Smart Government Portal must pass through the authentication channel. This article specifies that the identifier must be unique to each person, and every interaction on the NIN must be traceable to that unique individual. Article 4 assigns the Ministry of ICT the responsibility of developing the infrastructure for issuing identifiers. Other executive agencies operating any services on the NIN are to use this system, under the supervision of the SCC, to build out the mechanisms for application-level identifiers.

[12] SCC; ""Reliable Digital Identity Framework for the National Cyberspace"; Sep 2019; Download

Article 4 of this resolution included a three-year transition period for developing a unified portal (SSO) for identity providers. Despite the passage of this time, the Reliable Digital Identity Framework has yet to be fully implemented. Once completed, it will provide the Islamic Republic with a comprehensive infrastructure for managing user identities on the internet. While the stated aim of this plan is to "ensure the complete identification of users and their interactions on the internet," its actual consequence is to "facilitate tracking, content control, and the exercise of governing authority."

The 7th Five-year Development Plan of the Islamic Republic of Iran

The 7th Five-Year Development Plan of the Islamic Republic of Iran, ratified in the parliament in 2024 as the country's national roadmap, places particular emphasis on expanding digital infrastructure, e-government, and the smart delivery of public services.[13] This plan plays a key role in accelerating the rollout of authentication systems across Iran. In the absence of transparent legislation, independent oversight, and respect for citizens' rights, there is a high risk that such systems will evolve into tools for privacy violations and social control. Although these infrastructures are still under development, the most prominent system that drew public attention during the plan's adoption was the so-called "System for Monitoring and Measuring People's Lifestyle."

In the following section, we examine the mechanisms and actors behind the Internet Oversight systems in greater detail. Each system typically involves a commissioning entity, either an official state institution or a semi-official body, and an implementing or developing party, which

[13] "The Seventh Five-Year Development Plan of the Islamic Republic of Iran (2024–2028)"; Jul 8, 2024; Link, Archive

may belong to the government, to companies backed by state-affiliated investors, or even to the private sector.

State-Controlled Surveillance and Interception Systems Targeting Citizens in the Islamic Republic of Iran

The integration of authentication systems into public service infrastructure can offer legitimate benefits in many contexts, such as enhancing transparency, reducing fraud, and streamlining digital processes. However, in the Islamic Republic of Iran, where civil liberties are routinely suppressed, these systems raise serious concerns about their deployment as tools of surveillance and interception on citizens. Under state control, they enable the monitoring and collection of extensive data on individuals' online and offline activities. Although officially framed as mechanisms for building trust in the digital environment, in practice they are often used to identify political dissidents, restrict freedom of expression, and impose social control. The potential fusion of these identity-based infrastructures with behavioral analytics and machine learning poses an even greater risk of privacy violations against citizens of the Islamic Republic.

In January 2024, the Supreme Commission for Regulation,[14] an entity under the NCC and the highest regulatory authority for internet governance in Iran, ratified the "Executive Directive for Enhancing User Privacy Protection and the Collection, Processing, and Storage of User Data on Cyberspace Platforms."[15] This directive obligates all domestic digital service providers to clearly inform users about both mandatory and optional data access, encrypt user data, and provide the ability to delete one's account.

[14] SCC; "Description of Duties, Authorities, and Composition of the Members of the High Commission for the Regulation of the National Cyberspace"; 27 Aug 27, 2022; Download

[15] SCC; "Executive Directive for Enhancing User Privacy Protection and the Collection, Processing, and Storage of User Data on Cyberspace Platforms"; Jan 2024, Link, Download

> *"If a user requests to delete their personal data, such as by removing their user account, the request shall be processed immediately. However, in compliance with applicable legal regulations, including Articles 667 to 670 of the Criminal Procedure Code (Computer Crimes Act), the deleted data must be stored in a backup database that is isolated and kept offline. Once the relevant legal or judicial timeframes have expired, this data shall be permanently destroyed."*

In effect, user account data is not fully erased upon deletion requests but is instead archived on isolated, offline servers pending the expiration of legal retention periods.

Under this legal framework, service providers are required to retain traffic metadata for at least six months.[16] This includes information such as the origin, route, date, time, duration, and volume of communication, as well as the type of service used. Additionally, they must store details about users of access services, including service type, technical configurations, session duration, identity, geographic or postal address, IP contract, phone number, and other personal identifiers.

The executive directive requires all platforms to integrate their authentication systems with the centralized infrastructure developed under the Reliable Digital Identity Framework by the National Organization for Civil Registration of Iran (NOCR). All authentication requests must be routed through a unified mechanism that verifies user identities against the national registry maintained by the Ministry of Interior. This directive claims the goal is to "minimize the collection of identity data by platforms and systems," yet it effectively mandates centralized identity checks for every online interaction.

[16] "Criminal Procedure Code", Article 677, 678, Amendment Adopted in 2013 (Including the Computer Crimes Law); Jun 22, 2015; Link

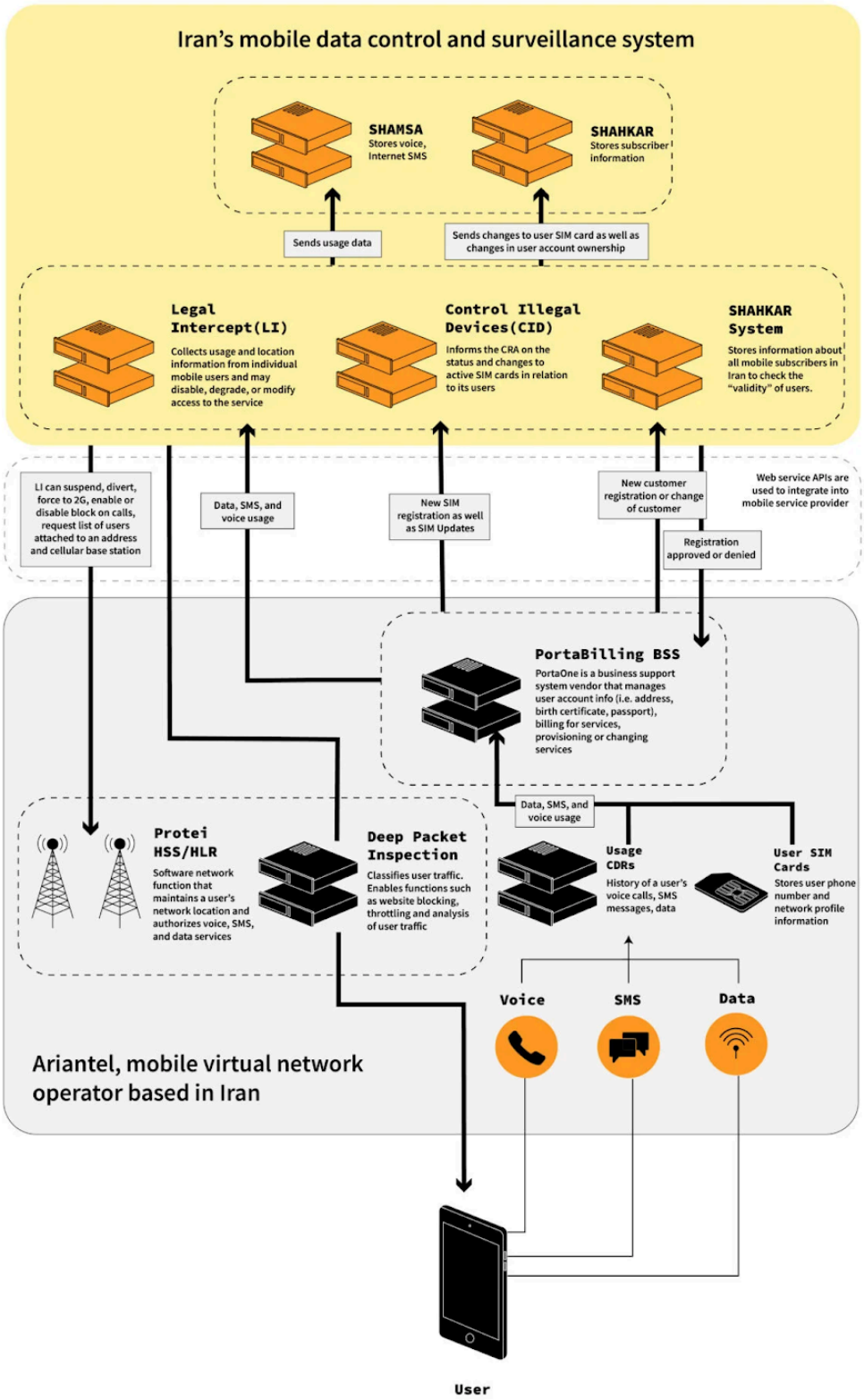
However, leaked documents from 2023 reveal that the SHAMSA data storage system is being used as the backend infrastructure for Islamic Republic of Iran's Lawful Intercept system (see diagram below).[17] This system deviates significantly from global standards for lawful interception, particularly those developed by the 3GPP working groups[18] and ETSI standards committees.[19] These international standards define technical interfaces and legal protocols for issuing warrants, intercepting communications, and delivering content to authorized legal entities. In contrast, the Lawful Intercept system in the Islamic Republic does not comply with any of these frameworks. Technical analysis and comparative reviews of internal documents show that it lacks legal safeguards, facilitates full user data handover upon activation, and is deeply embedded within telecom operators' business systems to retrieve content and manipulate user access.

[17] Gary Miller, Noura Aljizawi, Ksenia Ermoshina, Marcus Michaelsen, Zoe Panday, Genny Plumptre, Adam Senft, and Ron Deibert; The Citizen Lab; "You Move, They Follow; Uncovering Iran's Mobile Legal Intercept System"; Jan. 16, 2023; Link, Archive

[18] 3GPP; "Lawful Interception in mobile networks", Aug. 08, 2022; Link, Archive

[19] ETSI; "Lawful Intercept"; Link, Archive

Communciations Registration Authority (CRA) Legal Intercept System



Covert and Infrastructure-Level Surveillance, Interception, and Control Systems

This category consists of systems that are inherently designed for surveillance, interception, tracking, and intelligence gathering, and whose existence and operation largely remain outside the direct awareness of citizens. These systems operate at the infrastructure level of networks, telecommunications, traffic management, communication identity verification, and data aggregation, enabling continuous and large-scale access to citizens' communication and behavioral data without requiring any direct interaction with users. Systems such as SHAHKAR, SIAM, HAMTA, ESHRAF, SHAMSA, and lifestyle monitoring platforms function not as public service tools but as core components of the Islamic Republic's digital control architecture. From a technical perspective, their design enables systematic interception, tracking, data aggregation, and the enforcement of access restrictions in a centralized manner. In practice, these systems form the backbone of the state's surveillance and security infrastructure.

ESHRAF; "Oversight System for Cyberspace"

One of the most consequential resolutions shaping the vision of the NIN and the future of internet governance in the Islamic Republic of Iran is the "Macro Plan and Architecture of the NIN,"[20] ratified by the SCC in 2020. As the roadmap for the development of the internet in Iran, the document outlines the overarching framework, strategic goals, and technical, legal, and administrative requirements for managing and expanding the NIN. The plan identifies thirty objectives for the network; notably, the twenty-eighth objective is marked as "unpublishable."

[20] SCC; "Macro Plan and Architecture of the NIN"; Jan 2021; Download

جمهوری اسلامی ایران
شورایعالی فضای مجازی

۲-۲-۱-۲۲- تحقق کامل گذرگاه‌های ایمن مرزی؛

۲-۲-۱-۲۳- رشد بومی‌سازی تجهیزات شبکه به میزان ده درصد سالیانه بر اساس اولویت‌های تعیین شده توسط مرکز ملی فضای مجازی؛

۲-۲-۱-۲۴- بومی‌سازی سامانه‌های امنیتی مورد نیاز شبکه ملی اطلاعات به میزان صد درصد؛

۲-۲-۱-۲۵- اجرای کامل نظام پیشگیری و مقابله با حوادث فضای مجازی و نظام هویت معتبر در فضای مجازی مصوب شورای عالی فضای مجازی؛

۲-۲-۱-۲۶- تأمین ادله الکترونیکی در خدمات شبکه ملی اطلاعات در چارچوب قوانین کشور و مصوبات شورای عالی فضای مجازی؛

۲-۲-۱-۲۷- اجرای الزامات صیانت از حریم خصوصی و حقوق عامه در سطح خدمات شبکه ملی اطلاعات در چارچوب طرح مصوب شورای عالی فضای مجازی و قوانین کشور؛

۲-۲-۱-۲۸- (غیرقابل انتشار)؛

۲-۲-۱-۲۹- ارتقاء سالم‌سازی خدمات شبکه ملی اطلاعات به میزان بیست درصد در سال؛

۲-۲-۱-۳۰- ارتقاء سطح آمادگی امنیتی و دفاعی شبکه ملی.

۲-۲-۲- اهداف عملیاتی خدمات کاربردی

۲-۲-۲-۱- رسیدن به شاخص تمرکز مطلوب[۹] در سکوهای بومی خدمات؛

However, following a cyberattack on the email servers of the Attorney General's Office (Cyberspace Division),[21] a trove of internal documents was leaked, revealing unprecedented details about the operations and developmental plans of Iran's censorship and filtering apparatus specifically, the "Committee to Determine Instances of Criminal Content" (commonly known as the Filtering Committee). This committee is the central body responsible for internet censorship in the Islamic Republic of Iran.

Among the leaked materials was a draft bylaw titled "Bylaw for the Operation of the Oversight System for Cyberspace, Ministry of ICT." The draft explicitly states that "The Oversight System

[21] IranWire; "Anonymous hack of Iran's Filtering Committee servers", Nov 5, 2022; Link, Archive.

for Cyberspace pertains to Clause 28 of the Macro Plan and Architecture of the NIN, ratified by the SCC," the objective that had previously been marked as "unpublishable" in the original release of the NIN roadmap.

آیین نامه بهره برداری از سامانه اشراف وزارت ارتباطات

بخش اول) تعاریف و اختصارات

ماده ۱- تعاریف و اختصارات بکاررفته شده در این دستورالعمل به شرح ذیل است:

- سامانه : سامانه اشراف بر فضای مجازی موضوع بند ۲-۲-۱-۲۸ سند طرح کلان و معماری شبکه ملی اطلاعات مصوب شورای عالی فضای مجازی

- قانون : قانون آیین دادرسی کیفری

- داده ترافیک: هرگونه داده‌ای که سامانه‌های رایانه‌ای و مخابراتی در زنجیره ارتباطات تولید می‌کنند تا امکان ردیابی آن ها از مبدأ تا مقصد وجود داشته باشد. این داده‌ها شامل اطلاعاتی از قبیل مبدأ، مقصد، مسیر، تاریخ، زمان، مدت ، حجم و نوع ارتباط و خدمات می‌باشد

- اطلاعات کاربر: هرگونه اطلاعاتی راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورد استفاده، مدت زمان آن ، اطلاعات هویتی کاربر ، نشانی جغرافیایی یا پستی، IP ، شماره تلفن و سایر مشخصات فردی وی.

- کنترل ارتباطات: دسترسی به داده‌های در حال انتقال یا ذخیره شده ارتباطات خصوصی نظیر محتوای ایمیل، پیامک، گفتگوی خصوصی در شبکه‌های اجتماعی و پیام‌رسان و ارتباطات مخابراتی.

- متقاضی : مقامات قضایی، ضابطان دادگستری (فرماندهان، افسران و درجه داران نیروی انتظامی که کارت ضابط دریافت نموده‌اند) که برای ایفای وظایف و اجرای مأموریت‌های خود در خصوص شناسایی، مجرمین، کشف یا مقابله با جرایم c

The draft states that all "traffic data, such as the origin, destination, and timestamp of communications," as well as "user information," may be stored and disclosed to an "applicant" upon the issuance of a judicial order, in cases where there is "a strong suspicion of criminal activity." These documents suggest that the intended functionality of the Oversight System for Cyberspace closely resembles that of the Islamic Republic's lawful interception infrastructure. This marks the first time a document has surfaced that explicitly details part of this interception system's operations under the label "Oversight System for Cyberspace."

Although Clause 28 of the NIN's strategic doc, defining the Oversight System, remains unpublished, the leaked draft bylaw nonetheless reveals key operational details that shed light on the scope of this "intelligence oversight." For instance, the draft identifies the categories of eligible users of the Oversight System as follows:

> *"Judicial authorities, judicial officers (commanders, officers, and non-commissioned officers of the police force who hold judicial officer credentials) … personnel of the Ministry of Intelligence engaged in uncovering large-scale economic corruption, and IRGC personnel involved in missions defined in the IRGC's statute, as well as the Law of the MOIS, are recognized as judicial officers."*

This language not only formalizes access for the MOIS and the IRGC-IO to user data but also embeds these security bodies within the judicial process, granting them institutionalized access to sensitive digital information under the guise of legal authority.

The IRGC's statute[22] refers to "actions aimed at overthrowing the Islamic Republic," a charge classified as a national security offense under Iranian law. This framing underscores the centrality of the Oversight System within the Islamic Republic's security and intelligence infrastructure. What is particularly striking, however, is the Ministry of ICT's authority over all data exchanges occurring within the country. According to the draft bylaw:

[22] Articles 2 to 5 of the Statute of the IRGC (Archive)
Article 2: Lawful combat against individuals and groups seeking sabotage, the overthrow of the system of the Islamic Republic, or actions directed against the Islamic Revolution of Iran.
Article 3: Lawful combat against individuals who, through the use of coercive force, seek to negate the authority of the laws of the Islamic Republic.
Article 4: Taking action, in the same manner as other law enforcement forces, to disarm individuals who carry or store weapons and ammunition without legal authorization.
Article 5: Cooperation with law enforcement forces, when necessary, to establish order and security and to uphold the rule of law in the country.
Note: With regard to the missions specified in the above articles, the Islamic Revolutionary Guard Corps acts as an agent of the judiciary.

> *"In case-by-case requests for user traffic data or information, the applicant shall submit their request to the judicial authority handling the case, including justification, supporting evidence, and base information such as source or destination IP, date, time, type of service, and the destination website address. Upon approval by the judicial authority, the data disclosure order shall be registered through the system pursuant to Article 670 of the Criminal Procedure Code, and the system will automatically retrieve and deliver the requested data to the applicant."*

While no further technical documentation about the Oversight System or its implementation within the NIN has been released, existing disclosures from other systems, including SIAM, HAMTA, and SHAHKAR, clearly indicate that the Ministry of ICT is actively building infrastructure that enables full-spectrum interception of communications and mass surveillance of user traffic. This aligns with mandates ratified nearly two decades ago by the SCCR, which laid the groundwork for embedding censorship and surveillance into Iran's digital governance model.

SHAHKAR; Users Authentication Network

SHAHKAR is used to authenticate users in communication and Internet services. This system, by matching people's national ID numbers with their mobile phone numbers, confirms the identity of users and prevents anonymous use of digital services. SHAHKAR also mandates that service providers check whether the mobile number belongs to the owner of the national ID.

Internal documents revealed that the CRA is establishing direct access via APIs to mobile operators' backend systems (billing, service activation, and provisioning) for SHAHKAR. This enables the CRA to block registrations, enforce identity verification in real time, and maintain a

centralized registry of mobile users as a core component of Islamic republic of Iran's broader lawful intercept architecture.

SHAHKAR collects and stores identity data including national ID, phone number, and registration details. This raises significant privacy risks if data security is weak or misuse occurs. Users are often unaware of how their identity data is stored, used, or shared in SHAHKAR.

SIAM; Integrated System for Telecommunication Inquiries

SIAM is one of Islamic Republic of Iran's most potent centralized systems of surveillance and Interception, demonstrating the government's deep control over citizens' digital communications. Operated under the CRA, Iran's principal telecommunications regulator, SIAM was developed as early as 2013. However, its internal architecture and surveillance functions were publicly revealed in 2022 through leaked technical documentation.[23]

According to the technical specification documents, SIAM includes at least 40 distinct functionalities for monitoring, interception, tracking, and suppressing citizens.[24] Among its capabilities is the Force2GNumber function, used to downgrade users from 3G/LTE to 2G networks, making data interception easier. The system enables precise geolocation through SIM and IMEI tracking, retrieves contact and message metadata, and provides real-time access to user data via APIs that connect directly to operator back-end infrastructure, service logs, and billing systems.

---

[23] Sam Biddle, Murtaza Hussain; The Intercept; "Hacked Documents: How Iran Can Track and Control Protesters' Phones"; Oct. 28, 2022; Link, Archive

[24] "Iran's SIAM Manual in Persian for Tracking and Controlling Mobile Phones", Page 35-44, Link, Archive

اداره‌کل امنیت سیستم‌های ارتباطی

سامانه یکپارچه استعلامات مخابراتی (سیام)

محل درج لوگوی اپراتور

۴-۵- استعلام ریز ارتباطات ترکیبی (GetIPDR)

تابع ریز ارتباط ترکیبی، یک یا ترکیبی از پارامترهای شماره‌دار ورودی را ارسال و همچنین بازه تاریخ و زمان مشخص نموده و باید جدولی از ریز ارتباطات IP موجود در دورهٔ مشخص شده را دریافت کند:

نام متد		پارامترهای ورودی			پارامترهای خروجی	
فارسی	انگلیسی	شماره	فارسی	انگلیسی	فارسی	انگلیسی
استعلام ریز ارتباطات ترکیبی	GetIPDR	۱	شماره تلفن	TelNum	رشته پاسخ	QryResult
		۲	آدرس IP	IPAddr	هر رکورد از این رشته به ترتیب با مقادیر زیر پر می‌شود: ۱. شماره تلفن/ سیم خصوصی/ غیره ۲. آدرس IP ۳. شناسه مشترک ۴. بستر ارتباطی (ADSL، WiFi، Wireless، ...) ۵. تاریخ و ساعت شروع ارتباط (Session) ۶. تاریخ و ساعت پایان ارتباط (Session) ۷. Ip مبدا ۸. Ip مقصد ۹. Port مبدا ۱۰. Port مقصد ۱۱. حجم UpLoad ۱۲. حجم Download ۱۳. MacAddress ۱۴. Protocol ارتباطی (Layer3) ۱۵. Protocol ارتباطی (Layer4) ۱۶. آدرس سایت مقصد ۱۷. موقعیت جغرافیائی مشترک (N&E)	
		۳	شناسه مشترک	CId		
			از تاریخ	FDate		
			تا تاریخ	TDate		
			نام کاربری	Uname		
			رمز عبور	AutStr		
			توجه: فیلدهای تاریخ مطابق یا فرمت ذکر شده در بند ۲-۸ پر می‌شوند. ساعت ارسال شده در پاسخ تاثیر گذار بوده و باید توسط اپراتور از فیلدهای تاریخ استخراج گردند.			

SIAM also has the ability to throttle internet speeds, block connectivity, and enforce involuntary service transitions. It collects and stores extensive logs of users' communications, including calls, SMS, and, in some cases, the content of online interactions, all within centralized cloud systems controlled by state entities. The architecture and operational model of SIAM not only

violate internationally recognized privacy norms but also pose a high risk of abuse, particularly against politically targeted individuals.

The use of mobile network infrastructure for real-time location tracking of specific individuals is not new.[25] Iranian media has previously reported on research and operational deployments by law enforcement agencies in this domain. Additional evidence surfaced in the wake of recent cyberattacks on government servers. In one leaked document, the head of the security division within the legislative branch informed the Islamic Republic parliament speaker Mohammad Bagher Ghalibaf that, following the outbreak of the 2022 protests, a list of mobile phone numbers belonging to members of parliament and parliamentary staff was compiled and handed over to intelligence and security agencies for location tracking.[26]

This letter underscores that the real-time geolocation of MPs was technically feasible and operationally implemented. Given the spontaneous and decentralized nature of the protests, often forming suddenly in unannounced times and locations, such monitoring systems are essential tools for state surveillance, enabling authorities to track and potentially suppress political dissent even within official institutions.

[25] IranWire; "How Do Security Agencies in Iran Track Mobile Phones?"; Feb 6. 2021; Link, Archive

[26] "Measures Taken by the Parliamentary Protection Unit Regarding the Unrest: Letter from Hossein Erfanian, Head of the Judiciary Protection Center, to Mohammad Bagher Ghalibaf, Speaker of the Islamic Republic Parliament"; Sep 26, 2022", Page One: Link (Archive) and Page Two: Link (Archive)

محرمانه

جناب آقای دکتر قالیباف

رئیس محترم مجلس شورای اسلامی

موضوع: اقدامات مرکز حراست قوه مقننه در خصوص اغتشاشات

با سلام و صلوات بر حضرت محمد و آل محمد(ص) و احترام، اقدامات مرکز حراست قوه مقننه در خصوص تحرکات و اغتشاشات اخیر با موضوعیت فوت خانم مهسا امینی به شرح ذیل تقدیم می گردد:

- ارسال پیامک برای کلیه نمایندگان مجلس در راستای جلوگیری از تخلیه تلفنی توسط شبکه های معاند
- ارسال پیامک به نمایندگان در خصوص هوشیاری پیرامون عدم موضع گیری در مورد خانم مهسا امینی و اغتشاشات اخیر
- احصاء شماره تلفن کلیه نمایندگان و کارکنان مجلس و ارسال آن برای نهادهای امنیتی و اطلاعاتی جهت رصد احتمال حضور آنها در تجمعات و همکاری با اغتشاش گران
- توجیه و رصد کارکنان مجلس در جهت عدم موضع گیری نسبت به فوت خانم مهسا امینی و اتفاقات اخیر کشور
- اعلام هوشیاریاش و توجیه مرکز فناوری اطلاعات مجلس در خصوص احتمال حملات سایبری که پس از وقوع این حملات بدلیل اتخاذ تدابیر پیش دستانه موفقیتی برای آنان حاصل نگردید.
- توجیه حضوری و تلفنی تعدادی از نمایندگان حاشیه ساز در خصوص اغتشاشات نظیر آقایان پزشکیان، پاک فطرت، رشیدی کوچی، خضریان و ... که این اقدام موجب تعدیل قابل توجه مواضع نمایندگان و در نهایت نیز منجر به انتشار بیانیه از سوی آقای پزشکیان گردید.
- هماهنگی با یگان انتظامی شهید مدرس در جهت جلوگیری از تجمعات اعتراضی مقابل مجلس
- ارائه گزارش جلسه محرمانه علل فوت خانم مهسا امینی در کمیسیون شورایی مجلس برای سازمان اطلاعات سپاه و حراست کل کشور
- توجیه خبرنگاران خانه ملت و پارلمانی در خصوص حفظ چارچوب و خطوط قرمز نظام در تهیه و انتشار اخبار مرتبط با فوت خانم امینی
- احصاء توییت های منتشره از سوی نمایندگان در خصوص مواضع آنها در مورد فوت خانم امینی و ارسال آن به مراجع فوق الاشاره
- فعال سازی منابع خبری در خصوص جمع آوری نقطه نظرات کارکنان و نمایندگان در خصوص

System for Monitoring and Measuring People's Lifestyle

The 7th Five-Year Development Plan of the Islamic Republic of Iran, ratified in 2024 as the national roadmap for the years ahead, places significant emphasis on expanding digital infrastructure, implementing e-government, and automating public service delivery. This framework plays a pivotal role in accelerating the rollout of national digital identity systems and other centralized control tools. In the absence of transparent legislation, independent oversight, or respect for civil liberties, these emerging systems risk becoming instruments of surveillance and social control rather than tools for public service delivery. As of now, most remain in early conceptual or pilot stages.

One of the most controversial proposals during the plan's passage was the System for Monitoring and Measuring People's Lifestyle.[27] Its stated purpose is to collect, monitor, and analyze behavioral, cultural, and lifestyle patterns of citizens on a large scale. Implementation has been assigned to the Ministry of Culture and Islamic Guidance, in coordination with the Statistical Center of Iran, with launch expected in 2025.[28] In the original draft bill, the system was titled: "System for Monitoring, Observing, and Continuous Measurement of Public Culture Indicators for Assessing Religiosity, Spirituality, Ethics, and Lifestyle of the People." This language was later softened in the final version submitted to parliament, which renamed it the "System for Monitoring, Observing, and Continuous Measurement of Public Culture and Lifestyle Indicators."

According to this plan, the Ministry of Culture and Islamic Guidance is mandated to build a centralized platform for measuring the values, behaviors, and cultural indicators of Iranian

[27] BBC Persian; "What Is the 'System for Monitoring and Measuring People's Lifestyle' and How Does It Work?"; Aug 5, 2023; Link, Archive

[28] FilterWatch; "The 'Lifestyle Assessment System': A New Tool for Spying on the Public"; Oct 30, 2023; Link, Archive

society through an “Islamic-Iranian” framework. All government bodies and institutions possessing relevant data are legally required to provide continuous, real-time access to their databases. While the operational mechanisms remain unclear, the envisioned system is expected to aggregate a wide range of behavioral and consumption data, including online purchases, service usage, participation in social or cultural events, and even dietary habits. Integrating such granular information into a centralized repository would enable deep behavioral profiling of the population and presents a serious threat to the right to privacy.

همبستگی و اعتماد به نفس ملی، ارتقای هویت ملی و روحیه مقاومت، کار و تلاش در جامعه اقدامات زیر انجام می‌شود:

الف- وزارت فرهنگ و ارشاد اسلامی و سازمان اداری و استخدامی کشور مکلفند با هماهنگی دبیرخانه شورای‌عالی انقلاب فرهنگی و کسب نظر از مرکز مدیریت حوزه‌های علمیه و سایر دستگاههای فرهنگی ذی‌ربط به‌منظور بازسازی انقلابی ساختار فرهنگی کشور با رویکرد اصلاح ذهنیت، فرهنگ و نرم‌افزار حاکم بر جامعه و با هدف افزایش کارایی و اجتناب از همپوشانی و تداخل مأموریت و وظایف و با رویکرد استقرار الگوی حکمرانی هوشمند، شبکه‌ای، تعاملی، مردم‌پایه، ارزشی و انقلابی تا پایان سال دوم برنامه نسبت به تهیه طرح اصلاح رویکردها، رویه‌ها، روشها و مأموریت، ساختار، وظایف و تشکیلات دستگاههای فرهنگی که به‌نحوی از انحا از بودجه‌های عمومی به‌طور مستقیم و یا غیرمستقیم استفاده می‌کنند، اقدام نموده و به‌تصویب مراجع ذی‌صلاح برسانند.

ب- به‌منظور احصای دقیق و برخط داده‌های آماری مورد نیاز جهت تسهیل پردازش، تحلیل دقیق و ایجاد بستر مناسب برای آینده‌پژوهی روندهای سبک زندگی جامعه ایرانی، شناخت تحولات فرهنگی- ارتباطی و همچنین انتشار آنها، وزارت فرهنگ و ارشاد اسلامی مکلف است با همکاری سازمان صدا و سیمای جمهوری اسلامی ایران و مرکز آمار ایران و راهبری و نظارت مرکز رصد و برنامه‌ریزی و ارزیابی دبیرخانه شورای‌عالی انقلاب فرهنگی و با رعایت اصل بیست و پنجم (۲۵) قانون اساسی و قانون مدیریت داده‌ها و اطلاعات ملی نسبت به راه‌اندازی سامانه رصد، پایش و سنجش مستمر شاخصهای فرهنگ عمومی، سبک زندگی مردم، مرجعیت رسانه‌ای و وضعیت ارتباطات کشور اقدام نماید. دستگاههای اجرائی و دارندگان پایگاههای داده موضوع این بند، بجز دستگاههایی که مستقیماً زیر نظر مقام معظم رهبری هستند مکلفند نسبت به ارائه مستمر و جامع داده‌ها به این سامانه به‌صورت برخط اقدام کنند. وزارت فرهنگ و ارشاد اسلامی مکلف است ضمن برقراری دسترسی برخط مجلس به سامانه فوق، گزارش تغییرات شاخصهای فرهنگ عمومی را سالانه به کمیسیون فرهنگی مجلس ارسال نماید.

Formal and Visible Surveillance and Identity Verification Systems in Everyday Civic Interactions

This category includes systems that, in their official definition and public presentation, serve civil, administrative, and service-oriented functions, and which citizens are required to use for routine interactions with public institutions. Systems such as SAMAVA, SANA, EMTA, and HODA have functional equivalents in many other governments and are generally intended to facilitate public service delivery, identity verification, fraud reduction, and the digitalization of administrative processes. However, in the Islamic Republic of Iran, these systems operate within a framework that systematically repurposes them as instruments of surveillance, interception, and intelligence gathering. Their integration with centralized identity infrastructures, mandatory routing of interactions through unified gateways, and interoperability with security and judicial systems allow data generated through ordinary civic processes to be readily accessed and exploited for monitoring, tracking, and control. As a result, what is formally presented as digital public service infrastructure effectively becomes part of the broader chain of state surveillance and information oversight.

SAMAVA; National Authentication and Inquiries Gateway

SAMAVA was developed by the Information Technology Organization (ITO), a division under the Ministry of ICT. It functions as an identity provider within the Reliable Digital Identity Framework.[29] According to official sources, SAMAVA is intended to integrate authentication

[29] IRNA; "Reliable Identity Verification in the Virtual Space for All Users"; May 15, 2021; Archive

processes and deliver identity services to both governmental and non-governmental entities, including platforms and internet service providers.

Official documents describe SAMAVA as a foundational digital trust infrastructure operating within a national authentication gateway model. Rather than storing sensitive identity data in a centralized database, SAMAVA acts as a secure orchestrator that queries authoritative sources such as the NOCR or the Communications Regulatory Authority (CRA) for real-time verification. This architecture, framed as "privacy by design," allows government services to confirm users' identities through yes/no token responses without direct access to underlying databases. While this model reduces cyberattack risk and enhances interoperability across government entities, it also creates a strategic dependency: any failure in connected systems, such as the NOCR database, could disrupt access to all digital government services.

While SAMAVA is presented as a facilitator of e-government services, it also raises concerns about its potential use as a tool for social control and the restriction of civil liberties.

HODA; Iranian Digital Identity Authentication System

The HODA system (Iranian Digital Identity)[30] was launched by the National Organization for Civil Registration (NOCR) to digitize and replace physical identity verification processes, such as presenting photocopies of birth certificates or national ID cards.[31] This platform allows government agencies and authorized institutions to verify an individual's identity electronically via secure API-based queries.

[30] Tabnak; "What Is the HODA System and How Can One Register for It?"; Aug 18, 2024, Archive

[31] IRNA; "The HODA System Replaces the Submission of Copies of Birth Certificates and National ID Cards"; Jul 31, 2024; Archive

While HODA is framed as a modernization initiative within Iran's e-government agenda, its centralized structure and accumulation of highly sensitive identity data have raised concerns among privacy advocates. Iranian state media has referred to HODA as the government's flagship or "mega project" for national authentication, a designation that underscores both its scale and its potential implications for surveillance, data mining, and real-time citizen monitoring.[32]

SANA; Online Judicial Authentication System

SANA has been developed by the Judiciary's Statistics and Information Technology Center, under the Judiciary E-Services Division.[33] It is an official judicial identity verification platform intended to authenticate users for judicial services, online case access, and other court-related digital interactions.

Internal documentation indicates that SANA requires users to authenticate using their national ID number, mobile number, and in some cases verification of personal details (name, address) against the national civil registry or court records. Official sources emphasize that individuals who fail to authenticate through SANA may be barred from accessing judicial e-services, including court summons and case-related notifications, which are now exclusively delivered through the platform.

SANA collects and stores personal identifiers used during registration, and records of authentication attempts. This raises concern over transparency, especially regarding how long

[32] Tasnim; "A Transformation in Electronic Identity Verification with the 'HODA System'"; Sep 25, 2024; Archive
[33] Tabnak; "Registration in the THANA System"; Sep 8, 2024; Archive

data is retained, who has access, and how it is shared with judicial or security institutions. Many users are unaware of these practices or lack meaningful options to control or delete their data under existing legal structures.

HAMTA; Smart System of Communication Devices Registry

HAMTA (commonly referred to as Iran's national device registration platform)[34] is a regulatory system established to control the importation and usage of mobile devices in Iran. By registering and tracking device IMEI numbers, HAMTA aims to prevent unauthorized imports and ensures that mobile phones are only activated on national networks if they have been officially imported.[35] This gives the Islamic Republic's customs authority and the MIMT granular oversight over device distribution and usage.

Under HAMTA, users are required to register the device identity and link it to a verified user when a new IMEI is detected on the network. If this process is not completed within 30 days of initial connection, the phone's data services are cut off. Registration fees vary depending on the device brand and model. In 2023, this system was used to block the activation of all iPhone 14 and newer models in Iran. This restriction, while framed as an import control measure, also limits user choice and sets the stage for deeper state intervention in mobile access.

Given recent government investments in developing "national smartphones" and "domestic operating systems," the regulatory infrastructure behind HAMTA could evolve into a powerful

[34] Gary Miller, Noura Aljizawi, Ksenia Ermoshina, Marcus Michaelsen, Zoe Panday, Genny Plumptre, Adam Senft, and Ron Deibert; The Citizen Lab; "You Move, They Follow; Uncovering Iran's Mobile Legal Intercept System"; Jan. 16, 2023; Link

[35] Digikala; "Guide to Mobile Phone Registration"; Oct 21, 2024; Archive

tool for restricting access to specific devices, controlling hardware ecosystems, and extending surveillance through enforced device conformity. Such developments pose serious risks to user privacy and digital autonomy.

EMTA; E-commerce Customer Authentication System

The EMTA system was launched by the E-commerce Development Center of the Ministry of Industry, Mine, and Trade (MIMT) to authenticate and verify sellers in Iran's digital commerce ecosystem.[36] EMTA cross-checks declare user information, such as identity and business credentials, against government databases in real time to validate the legitimacy of e-commerce actors.

While officially intended to reduce fraud and build trust in online markets, EMTA also functions as a state-controlled data collection hub that enables regulatory bodies to monitor individuals' commercial activities. The architecture of EMTA reveals a dual mandate: it serves both as a service platform designed to facilitate e-commerce (an incentive for businesses) and as a regulatory instrument used by the state to exert control over the digital marketplace (a source of pressure). This built-in duality has fueled ongoing controversy and resistance regarding its implementation.

The official narrative from the E-Commerce Development Center emphasizes user convenience, security, and support for businesses. However, the system's most prominent and mandatory use cases have emerged in response to economic crises, such as price inflation in the car market. The involvement of the Prosecutor's Office in mandating EMTA's use in certain sectors

[36] AsanSabt; "What Is the EMTA System?"; Archive

of the economy underscores that its role extends beyond enabling online commerce. It is also a tool of law enforcement and economic regulation.

The system collects detailed records of traded goods and services (SKU-level data), transaction histories, and identity-linked interactions. Given its integration into the government's digital governance infrastructure, even state media outlets have criticized EMTA for its opaque identity verification process and potential overreach.[37]

SAKHA; Islamic Republic Police Platform

The SAKHA system is the centralized electronic services platform operated by the Islamic Republic Law Enforcement Forces (FARAJA or Iranian Police), functioning as a core component of the Islamic Republic's e-government infrastructure.[38] It provides a wide range of non-presential services, including conscription and military service management, passport issuance and renewal, residence address verification, vehicle registration and license plate transfers, traffic violation inquiries and appeals, and selected exit permit procedures.

Officially, SAKHA is framed as a service facilitation platform designed to streamline administrative processes and reduce in-person visits. In practice, mandatory registration and identity verification for access to essential services have positioned the system as a central hub for aggregating sensitive citizen data. Authentication is based on national ID numbers linked to mobile phone numbers registered with the National Organization for Civil Registration, effectively creating a centralized and non-repudiable digital identity.

[37] Tasnim; "What Are the Benefits of Using EMTA for Businesses?"; Oct 6, 2020; Archive
[38] Tabnak; "What Is the SAKHA System? A Visual Guide to Registration in SAKHA"; Dec 10, 2024; Archive

SAKHA consolidates multiple categories of sensitive data within a single platform, including identity records, verified residential addresses, military service status, passport and exit bond information, and law enforcement and travel histories.[39] This cross-domain aggregation enables systemic linkage between civil, administrative, and security-related datasets, allowing law enforcement authorities to condition access to civil services on compliance with data verification requirements.

From a surveillance perspective, SAKHA functions beyond a conventional service portal and operates as an instrument of digital administrative control. Restrictions such as blocking vehicle registration, delaying service delivery, or enforcing travel limitations can be applied algorithmically, without direct physical intervention. The concentration of such comprehensive datasets under the direct control of FARAJA, in the absence of a comprehensive personal data protection law, raises substantial concerns regarding privacy violations, secondary data use, and the normalization of centralized administrative surveillance.

MIKHAK; Integrated Consular Services Management Platform

The MIKHAK system is the centralized consular services platform operated by the Ministry of Foreign Affairs of the Islamic Republic of Iran, designed to provide digital access to consular services for Iranian citizens residing abroad.[40] The platform covers a wide range of functions, including identity record registration and updates, passport-related services, consular powers

[39] Tabnak; "How Address Verification Works in the SAKHA System"; Oct 6, 2024; Archive
[40] Digikala; "MIKHAK System Guide: From Login and Registration to Appointment Scheduling"; Sep 21, 2025; Archive

of attorney, document authentication, civil registry matters, and selected nationality and residency-related services. Comparable digital consular systems exist in many countries, and MIKHAK is officially framed within this standard service-delivery model.

In practice, however, MIKHAK has become a central hub for the aggregation of identity and consular data on Iranian citizens abroad. Access to services requires the submission of detailed identity, residency, and contact information, with authentication mechanisms designed to link consular records to domestic identity databases. This architecture enables the consolidation of overseas consular data with internal government datasets, effectively producing a traceable digital profile of citizens living outside the country.

From a surveillance perspective, MIKHAK functions beyond a purely service-oriented platform and operates as a tool of administrative and consular monitoring. By conditioning access to essential consular services on data registration and verification, the system allows authorities to manage, delay, or suspend services algorithmically. The concentration of sensitive data on the Iranian diaspora within a centralized platform, combined with limited transparency regarding data-sharing practices with other state institutions, raises significant concerns about secondary data use, consular tracking, and the potential application of administrative or security pressure on citizens abroad.

This section demonstrates that the architecture of surveillance and interception in the Islamic Republic of Iran is not limited to covert security tools but is built upon a combination of hidden infrastructure-level systems and formal, service-oriented platforms. Within this structure, systems designed for civil or administrative purposes are integrated into centralized identity and judicial frameworks, transforming everyday interactions into instruments of monitoring and control. At the same time, covert systems enable large-scale interception, tracking, and data aggregation. The result is a model in which routine civic activities are systematically converted into data streams subject to state oversight and enforcement.

Appendix

Glossary