FILTERWATCH YEARBOOK

THE STATE OF DIGITAL RIGHTS IN IRAN

1399

MARCH 2020 – MARCH 2021

FILTER WATCH

KAVEH AZARHOOSH, MELODY KAZEMI, JAMES MARCHANT
JUNE 2021

CONTENTS

PREFACE

WELCOME to the second edition of the Filterwatch Yearbook, covering the Iranian calendar year 1399 – extending from 20 March 2020 until 20 March 2021.

It perhaps comes as little surprise to say that in Iran, as in the rest of the world, this year was dominated by the spread of the COVID-19 pandemic, which had already taken 1,433 lives at the time of the Nowruz holidays. By the end of the year, a confirmed 61,742 lives had been lost to the pandemic (although the real death toll could be significantly higher, according to a member of Iran's Supreme Medical Council)[1], and the country had been battered by a series of halting, stop-and-start lockdowns that struggled to suppress its spread.

As well as driving the closure of public spaces, the pandemic in Iran has also had the effect of ushering in a period of intense closure of the online public realm. Over this period, state authorities have radically expanded restrictions imposed on free expression online, in the name of combatting "disinformation" and "fake news". In reality, journalists

[1] Dan De Luce and Leila Gharagozlou, *NBC News*, 28/10/2020, "Iran's Covid death toll may be four times the government's official tally, says top doctor", available at: **https://nbcnews.to/3eGedQi**

and citizens have been targeted for expressing legitimate concerns about the state's handling of the pandemic, while figures such as Supreme Leader Ali Khamenei have continued to spout conspiracy theories about the United States' deployment of "a special version" of COVID-19 against Iran.[2]

At the same time, Iran's digital infrastructure has been put to the ultimate test, and has been found wanting. The mandatory uptake of distance learning and working across Iran highlighted the gaps and inequalities that still persist doggedly across the country's marginalised, rural (and generally ethnic minority-inhabited) border provinces. The effects of these inequalities were particularly felt by vulnerable children in these communities, who missed out on access to crucial learning resources.

This was also the last full calendar year of Rouhani's presidency. Although his government is isolated, and faced a hostile, conservative-dominated Parliament from February 2020, a number of new resolutions and policies have nonetheless emerged from the Supreme Council for Cyberspace. All of these new policies have confirmed Iran's commitment to its vision of a hyper-localised and tightly controlled internet, in which sophisticated information control mechanisms such as its "layered filtering" regime create a divided and hierarchical population of internet users.

This report details how Iranian authorities have ruthlessly exploited the pandemic to exert control over online space in Iran, while taking major strides towards the realisation of their long-term National Information Network project. Although the Rouhani era is nearly at an end, his administration's main achievement in the field of ICT – the near-total completion of the NIN's technical and policy infrastructure – will lay the groundwork for future administrations to exert ever greater control over Iranian internet users' online speech, and ever more access to their most sensitive personal data.

After a challenging year, Iranians deserve a brighter vision for what their online public spaces could be – spaces that allow for the free exchange of ideas, for social and political mobilisation, and for the expression of identity without fear of surveillance or retribution. Disappointingly, it looks as if none of the candidates for the upcoming presidential elections in June will be capable of offering such a vision. Regardless of the outcome of the upcoming election, Filterwatch will continue to monitor and assess the evolution of internet policy in Iran, and its impacts upon digital rights in the years ahead.

If you have any questions about any of the subjects covered in this report, please don't hesitate to contact us at: ask@filter.watch.

All the best,

THE FILTERWATCH TEAM

[2] *France 24*, 22/03/2020, "Iran's Khamanei refuses US help to fight coronavirus, citing conspiracy theory", available at: **https://bit.ly/3oesWVD**

1 / INTERNET GOVERNANCE

IRAN'S model of internet governance remained fundamentally stable between March 2020 and March 2021, with only minor changes in the composition of Iran's top Internet policy-making bodies, and no meaningful shifts in the way that the internet is governed. The Supreme Council of Cyberspace (SCC) remains Iran's highest level internet policy-making body, and determines the overarching, long-term objectives for the Internet in Iran. The Committee to Determine Instances of Criminal Conduct (CDICC) is a Judiciary-hosted committee that decides which sites and apps should be filtered nationally. After the parliamentary elections of February 2020, the legislature's representatives on the SCC and the CDICC were replaced, but these were the only changes in these bodies over this period.

At the CDICC, after a delay of several months it was eventually announced on 17 November 2020 that the conservative-backed MPs Seyed Javad Hosseini Kia (from the Industries and Mine Committee) and Mahdi Bagheri (from the Judicial and Legal Affairs Committee) would be appointed to the 12-member body.[3] Although conservatives have taken a more aggressive approach to filtering websites and apps, the lessening influence of the CDICC in recent years means that these appointments are unlikely to drive any immediate shifts in filtering policies.

Meanwhile over at the SCC, Morteza Aghatehrani (the new Chair of the Cultural Affairs Committee) and Mohammad Bagher Ghalibaf (the new Parliamentary Speaker) took up their posts on the SCC. Both were conservative-backed candidates in the February 2020 elections. Nonetheless, their appointment did not result in any meaningful shifts in the balance of power on the SCC – the resolutions subsequently passed by the body were in line with the overarching internet localisation policies that have been in place for the duration of Rouhani's administration.

Over the course of this year, Iranian authorities failed to develop any legislation or implement any meaningful policies to improve the situation of fundamental human rights in Iran's online spaces. On the contrary, policy-makers have developed several bills and SCC resolutions to further restrict Iranians' rights online, typically under the guides of "protecting users' rights". In this chapter, we will assess these resolutions and legislative developments in turn.

1.1 SUPREME COUNCIL OF CYBERSPACE RESOLUTIONS

The SCC resolutions passed in recent months offer the year's most meaningful policy developments, with all seeking

[3] Arash Parsapour, *Digiato*, 17/11/2020, "What is the record of the new representatives in the filtering working group?" [Persian], available at: **https://bit.ly/3tMzOWF**

to further Iran's long-term objective to deliver a localised, censored and surveilled internet in the form of the National Information Network (NIN).

National Information Network Macro Plan and Architecture Resolution

In October 2020 Iran's Supreme Council for Cyberspace (SCC) published the text of its "National Information Network Macro Plan and Architecture" resolution.[4] The resolution itself was passed in September. Comprising five articles, the resolution focuses on the following topics:

Article 1: Policies Governing the NIN;

- The policy objectives governing the NIN include: self-reliance, opportunity building, deterrence and resistance from threats, streamlined governance, cooperation between relevant organizations, green expansion and health orientation, among other objectives.

Article 2: Operational and Strategic Goals on the Horizon for 2025;

- This article features targets set on 2 February 2020, which are focused on further expanding and promoting the use of domestic services to further advance the localisation of Iran's internet. These are set under a number of strategic and operational targets some of which include:
    - 80% fixed bandwidth coverage with the average speed of 25MB/s and 100% mobile internet coverage with the average speed of 10MB/s
    - Localising 100% of security systems required for the NIN
    - At least 20% market share for smart phones using domestic operating systems made by domestic manufacturers
    - Establishing 'core domestic services' with priority given to messaging apps and search engines by 2025
    - Formation of at least three cloud service providers capable of meeting infrastructural, storage, and processing and platform needs for all 'core domestic services' and acquiring 80% of the market share for the country's cloud service needs
    - Other operational targets have also been set in relation to 'healthy content and service security', as well as a number of other operational targets relating to content and services

Article 3: Architecture of the NIN;

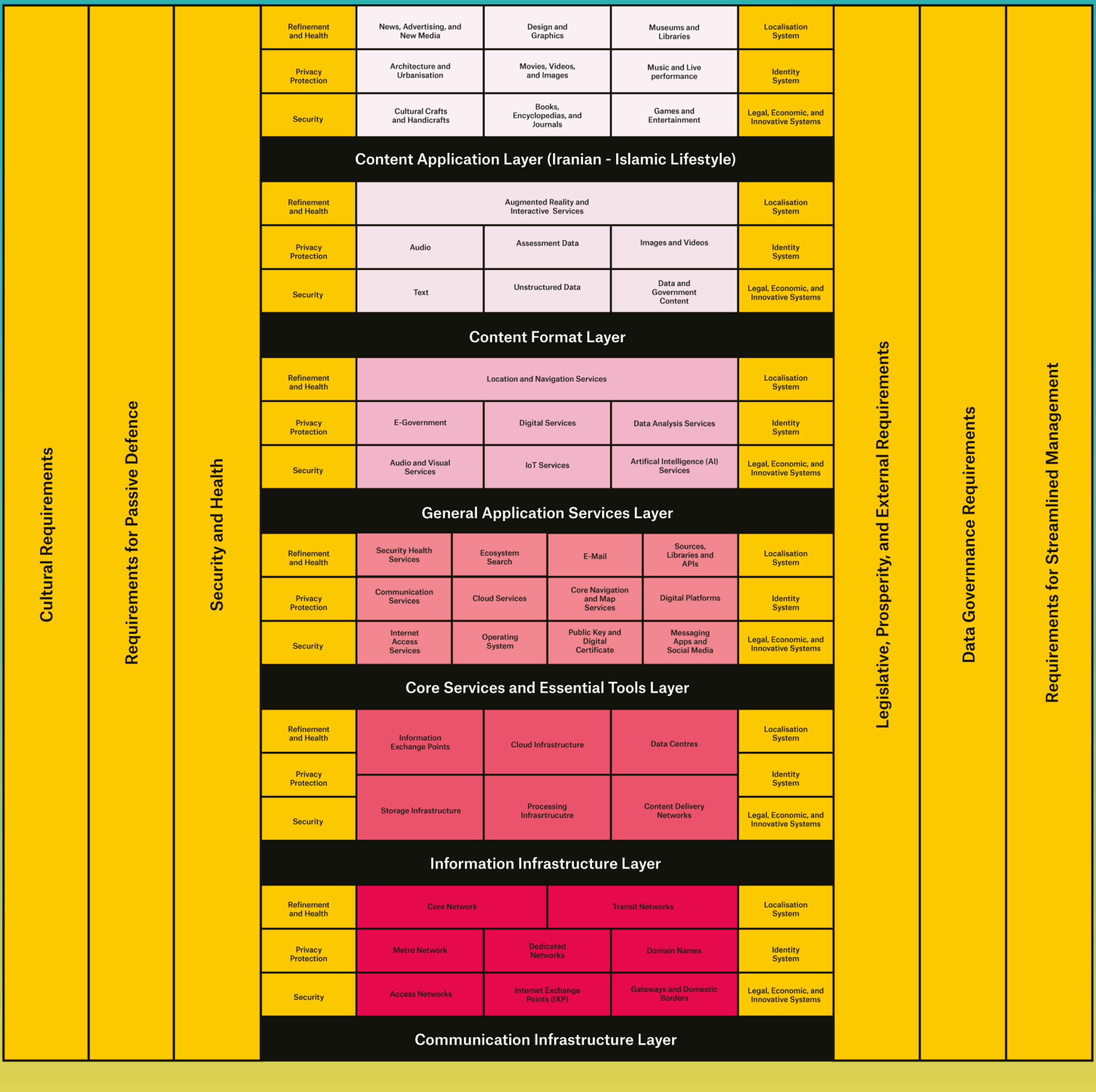
- This article sets out the technical architecture of the NIN, along with a series of illustrative diagrams. A translation of the main illustration is available below.

[4] Melody Kazemi, *Filterwatch*, 16/11/2020, "Policy Monitor – October 2020", available at: **https://filter.watch/en/2020/11/16/policy-monitor-october-2020/**

NATIONAL INFORMATION NETWORK

THIS visual has been taken and adapted from a version published under Article 3 of the Supreme Council of Cyberspace's "National Information Network Macro Plan and Architecture Resolution". It sets out the technical architecture of the NIN along with a series of illustrative diagrams.

Although the chart is not organised in an entirely clearly structured way, it is helpful for demonstrating the sheer scope of the NIN project, spanning major infrastructural expansion, legislative and regulatory reform, as well as the introduction of a wide range of user-facing services and applications. The overall impact of all of these layers of the NIN is to grant authorities greater control – whether over the "internet backbone" itself, or over user content and data hosted on domestic servers.



Cultural Requirements

Requirements for Passive Defence

Security and Health

Refinement and Health | News, Advertising, and New Media | Design and Graphics | Museums and Libraries | Localisation System

Privacy Protection | Architecture and Urbanisation | Movies, Videos, and Images | Music and Live performance | Identity System

Security | Cultural Crafts and Handicrafts | Books, Encyclopedias, and Journals | Games and Entertainment | Legal, Economic, and Innovative Systems

Content Application Layer (Iranian - Islamic Lifestyle)

Refinement and Health | Augmented Reality and Interactive Services | Localisation System

Privacy Protection | Audio | Assessment Data | Images and Videos | Identity System

Security | Text | Unstructured Data | Data and Government Content | Legal, Economic, and Innovative Systems

Content Format Layer

Refinement and Health | Location and Navigation Services | Localisation System

Privacy Protection | E-Government | Digital Services | Data Analysis Services | Identity System

Security | Audio and Visual Services | IoT Services | Artifical Intelligence (AI) Services | Legal, Economic, and Innovative Systems

General Application Services Layer

Refinement and Health | Security Health Services | Ecosystem Search | E-Mail | Sources, Libraries and APIs | Localisation System

Privacy Protection | Communication Services | Cloud Services | Core Navigation and Map Services | Digital Platforms | Identity System

Security | Internet Access Services | Operating System | Public Key and Digital Certificate | Messaging Apps and Social Media | Legal, Economic, and Innovative Systems

Core Services and Essential Tools Layer

Refinement and Health | Information Exchange Points | Cloud Infrastructure | Data Centres | Localisation System

Privacy Protection | Identity System

Security | Storage Infrastructure | Processing Infrasrtrucutre | Content Delivery Networks | Legal, Economic, and Innovative Systems

Information Infrastructure Layer

Refinement and Health | Core Network | Transit Networks | Localisation System

Privacy Protection | Metro Network | Dedicated Networks | Domain Names | Identity System

Security | Access Networks | Internet Exchange Points (IXP) | Gateways and Domestic Borders | Legal, Economic, and Innovative Systems

Communication Infrastructure Layer

Legislative, Prosperity, and External Requirements

Data Governance Requirements

Requirements for Streamlined Management

Article 4:Components of the NIN

- The resolution divides the components of the NIN into infrastructure and services. The NCC and the ICT Ministry are to review the conceptual model, technical architecture model, and the components of the NIN in light of technical developments within two years, in accordance with the resolution.

Article 5: Macro Actions and Institutional Mapping

- This article provides a breakdown of the state organisation(s) responsible for implementing the operational targets set for the NIN.

Taken together, the content of this resolution demonstrates that the state's vision for the National Information Network remains consistent. The document outlines a comprehensive plan for the radical localisation of Iran's digital infrastructure and services. It also shows that multiple government ministries and other institutions are working in a coordinated fashion to implement this plan.

Document on Preventing and Combating the Dissemination of Misinformation and Fake News and Content Resolution

In February 2021 the SCC released the text of another alarming resolution titled the "Document on Preventing and Combating the Dissemination of Misinformation and Fake News and Content".[5] The resolution represents Iran's first attempt at creating a legal framework to deal with mis- and disinformation online.

The resolution calls for the Judiciary to introduce a bill to combat "false news" within three months. The bill is to be developed in collaboration with the National Centre for Cyberspace (NCC), the Ministry of Culture and Islamic Guidance (MCIG), and the ICT Ministry and is required to include appropriate sentencing, as well as setting out the obligations and responsibilities for owners of news outlets and online platforms.

The MCIG has been given several responsibilities, including "identifying and verifying" publication outlets at national and provincial levels, and forming an "information database" to support collaboration with outlets, with priority to be given to "popular" outlets. These measures are also required to take place within three months.

The resolution also established that the MCIG is responsible for creating a mechanism for the "comprehensive monitoring and verification" of news, and for the creation of a "reference platform" to raise awareness about "false news and information". The MCIG

[5] Majazi.ir, 13/02/2021, "Communication of the resolution of the country's Supreme Council of Cyberspace regarding the requirements for preventing and combating the dissemination of information, news and false news located in cyberspace" [Persian], available at: **https://bit.ly/3nQholb**

is also required to collaborate with the Foreign Ministry in order to create an "information collection mechanism" for establishing points of contact with foreign messaging apps about the publication of false information.

The resolution has ambitions to engage with foreign platforms with regards to "false information". Foreign platforms therefore must be aware of the potential human rights implications of complying with such measures.

The Foreign Ministry has its own set of obligations, being mandated to use "diplomatic and legal opportunities" to take action against "authorities responsible for disseminating false information against national interests and national security".

Incentives to pass legislation to combat the dissemination of disinformation have intensified in recent years, especially in the wake of the COVID-19 pandemic. However, given Iran's far-reaching restrictions on press freedom and freedom of expression online, Filterwatch remains extremely concerned that the new resolution and any forthcoming legislation will be used to silence government critics – especially in the run-up to Iran's presidential elections in June. Additionally, these new measures could further encourage self-censorship on the part of individuals and the press, if users perceive that their online speech could expose them to prosecution.

Policies and Requirements for Supporting Competition and Combating Monopolies in Cyberspace Platforms Resolution

The resolution "Policies and Requirements for Supporting Competition and Combating Monopolies in Cyberspace Platforms", issued in September 2020, is another crucial resolution seeking to construct legal frameworks governing private sector operations within the NIN. The resolution claims that it is designed to "encourage competition and prevent the formation of monopolies in cyberspace through transparency".[6]

One of the more dangerous and worrying sections of the resolution is contained in Article 7, titled "Requirements from platform service providers towards the government". Under this article, platforms are required to "present their requested data to the Competition Council to facilitate their research and investigation procedures. This is in line with the realisation of Article 60 of the General Policies of Article 44 of the Constitution."[7]

Article 7 does not define the limits or extent of authorities' access to

[6] Arash Parsapour, 12/08/2020, "Details of the anti-monopoly resolution on online platforms has been released" [Persian], available at: **https://bit.ly/3od414O**

[7] Ministry of Cooperatives, Labour and Social Welfare, 28/01/2008, "Law for the Enforcement of General Policy, Article 44" [Persian], available at: **https://www.mcls.gov.ir/fa/law/260**

platforms' data, which could result in government authorities being permitted access to vast quantities of personal data held by platforms operating in Iran. No guidance has been published about how this information should be accessed, nor about any requirements to protect the transfer of this data, nor to anonymise personally identifiable data. One lawyer also criticised the resolution for creating a 'difficult environment' for the growth of online platforms, particularly for startups.[8]

This resolution has the potential to further extend state access and control over the private technology sector, as well as further restricting the availability of international platforms in Iran.

Instructions for Management of Bots and Robots in Cyberspace Resolution

The SCC resolution published a resolution in September 2020 titled "Instructions for Management of Bots and Robots in Cyberspace".[9] This resolution seeks to regulate the activities of bots online. The resolution defines bots under five categories:

1. Information production and dissemination bots
   - These bots aim to develop "social influence", including bots that send "mass text messages, or mass messages on social media, or push notifications".
2. Information and content collection bots,
   - These include 'crawlers' such as search engine bots, whose aims are to "create databases from online content"
3. Non-content service bots
   - These include chatbots, survey bots, and the like. These bots often operate in messaging apps or other mobile applications.
4. Bots involved in financial and commercial services
5. Disruptive bots
   - These are bots that are designed to "threaten cybersecurity"

According to the instructions provided by this resolution, multiple ministries (including the ICT Ministry, Ministry of Culture and Islamic Guidance, and the Ministry for Industry, Mines and Trade) will be allocated responsibility for regulating different categories of bots. The resolution establishes that these ministries must provide their respective implementation plans and timelines within one month.

[8] *Khabar Online*, 27/09/2020, "Legal scholar: There are many flaws in the Supreme Council of Cyberspace's document" [Persian], available at: **https://bit.ly/3h3d72v**

[9] Supreme Council of Cyberspace, "Instructions for Management of Bots and Robots in Cyberspace Resolution", available at: **https://bit.ly/3xOv4b3**

1.2 LEGISLATIVE DEVELOPMENTS

Conservatives and hardliners secured a decisive victory in the parliamentary elections held in February 2020, seizing control of the legislature.

This year, two bills moved through the Iranian parliament that threaten to further undermine the rights of Iranian Internet users: the "Protection of User's Rights Online and Managing Social Messaging Apps Bill" and the "Criminalising Online Gambling Bill".

"Protection of User's Rights Online and Managing Social Messaging Apps Bill"

One of the legislative priorities of this new parliament seems to be an amended version of the "Managing Social Messaging Apps Bill", which has been brought back onto the Parliamentary Cultural Committee's Agenda. It is the only one of the six ICT-related bills unveiled in 2018 to have advanced to this stage: the other five (detailed in our special report *Bills, Bills, Bills: Upcoming Policy Challenges in Iran, and How We Can Resist Them*) remain in limbo. According to reports, on 24 August the "Managing Social Messaging Apps" bill was placed on the current agenda of the Parliamentary Cultural Committee.[10] The bill – which was first introduced in 2018 by a cross-factional parliamentary grouping known as the "Cyber Faction" – underwent a review at the Parliamentary Research Centre (PRC), and returned to the Majles for approval by the Cultural Committee in late 2019.[11] This approval process was not completed before the end of the last parliamentary term. The text of the new draft of the bill, which is now known as the **"Protection of User's Rights Online and Managing Social Messaging Apps Bill"** has been published by the PRC.[12]

According to the bill's proposals, the administration of all messaging apps will be managed by an "Oversight Board". This board will be chaired by the Head of the National Centre for Cyberspace, "a relevant deputy" or other representatives from several government ministries, Islamic Republic of Iran Broadcasting (IRIB), an MP from the Parliamentary Cultural Commission, and representatives from the Intelligence Organisation of the Islamic Revolutionary Guard Corps (IRGC), as well as the National Police.

One of the most controversial and dangerous articles of the bill gives the Armed Forces control over internet gateways, without any restrictions. The bill also introduces a number of new legal articles, one of which criminalises the

[10] Behnaz Tohidi, *Peivast*, 24/09/2020, "Parliament again attempts to hand over Internet portals to the Armed Forces" [Persian], available at: **https://peivast.com/p/84192**

[11] Melody Kazemi, *Filterwatch*, 01/04/2020, "Iran's "Managing Social Messaging Apps" Bill Returns to Parliament", available at: **https://bit.ly/3fdq4Va**

[12] Majlis.ir, 14/07/2020, "Protection of User's Rights Online and Managing Social Messaging Apps Bill", available at: **https://rc.majlis.ir/fa/legal_draft/show/1600586**

unauthorised production, publication or distribution of VPNs and circumvention tools.

Despite the bill's name, there are no substantive new articles dedicated to data protections or privacy protections for users. Instead, the bill allocates the responsibility of "protecting users' private data" to messaging apps, hosting services, and ISPs. Any data protection measures set out in this bill appear to be limited to the use of messaging apps.

If the bill is approved by the Commission, it will subsequently be subjected to a vote in the Majles and then sent for approval by the Guardian Council before it becomes law.

"Criminalising Online Gambling Bill"

Another significant bill introduced in Iran's parliament this year is designed to confront the growth of online gambling in Iran. According to Reza Taghipour, Tehran MP and member of the Parliamentary Mines and Industry Committee, on 26 December MPs submitted a bill "criminalising online gambling" to the Parliamentary Judicial Committee for review.[13] The bill is designed to amend a number of articles relating to gambling within Iran's Islamic Penal Code (Articles 705-711), under which gambling through 'any means' is banned.

According to Taghipour, the changes adjust the penalties for online gambling, introduce punishments for repeat offenders, and clarify the definition of 'online gambling'. A few days before Taghipour's announcement, Hassan Norouzi, the Deputy Head of Parliamentary Judicial Committee said that repeat gambling and betting offences could be considered "corruption on earth" – a crime which is punishable by death under the Islamic Penal Code.[14] This proposed legislation – should it be passed – is a grossly disproportionate response to the activities of online gambling websites, and threatens the rights of Iranian internet users.

1.3 INSTITUTIONAL CONFLICTS

Although the past year has generally seen a great deal of continuity in policymaking, it has also seen a resurgence of some of the internal conflicts that have persisted throughout Rouhani's eight-year administration. During this period, Rouhani's government has persistently clashed with the IRIB, parliamentary hardliners and the Judiciary.

Although these policymaking actors are broadly aligned in their long-term vision for the NIN, they are also engaged in smaller scale disagreements that

[13] Mina Safdari, *ICTna*, 26/12/2020, "Parliamentary plan to deal with online gambling", [Persian], available at: **https://www.ictna.ir/id/119482**

[14] Mina Safdari, *ICTna*, 23/12/2020, "Internet gamblers were sentenced to death", [Persian], available at: **https://www.ictna.ir/id/119411/**

could see a number of divergent short-term policy outcomes depending on the shape of the ICT Ministry after the 2021 presidential election.

Jahromi Clashes With Parliament On Rural Internet Access

These tensions came to a head on 22 December 2020, when ICT Minister Mohammad-Javad Azari Jahromi was called to a public session of the Majles to answer questions raised by the MP for Sistan and Baluchestan Province, Habibullah Dehmardeh.[15] The Parliament's increased focus on connectivity has been triggered in part by the consequences of the COVID-19 pandemic, and a rapid surge in the public's dependency upon internet connectivity for education and business.

Dehmardeh questioned Jahromi on the lack of fiber optic infrastructure in border provinces including Sistan and Baluchestan, which according to Dehmardeh, had resulted in connectivity issues in cities across the province. He added that these disruptions had particularly affected students seeking to access online learning. In response, Jahromi vowed that "connecting villages with a population of over 20,000 to the internet will be a priority for the ICT Ministry". Following Jahromi's response, the MP declared that he was 'satisfied' with Jahromi's answer.

Following the public session, Jahromi travelled to Sistan and Baluchestan and announced that an additional 1,000km of fiber-optic cables would be installed in the province, and that the ICT Ministry had set a target of "connecting 1,200 villages to the NIN".[16]

During President Rouhani's administration, the expansion of internet services to rural areas and villages has been a key component of the NIN project. However, despite claims of increased expansion and connectivity, rural areas continue to suffer from a lack of connectivity. Sistan and Baluchestan has historically had the lowest internet penetration rates in the country.[17]

Jahromi Faces Court Summons Over Policy Clashes

Later in the year, Jahromi found himself in a very public conflict with the Judiciary too. On 20 January a number of Iranian news outlets reported that ICT Minister Azari Jahromi had been summoned to the Culture and Media Court by the Attorney General for questioning in relation to a number of claims made against him, one of which, accordingly to reports related to non-compliance

[15] IRNA, 22/12/2020, "Habibollah Dehmardeh was convinced of Azari Jahromi's answers", [Persian], available at: **https://bit.ly/2PWvVpa**

[16] Iranian ICT Ministry, 27/12/2020, "A target of connecting 1,200 villages to the NIN in [Sistan and Baluchestan], COVID demand is an opportunity for us", [Persian] available at: **https://bit.ly/3b6RxpY**

[17] Melody Kazemi, *Filterwatch*, "Policy Monitor – May 2020", 19/06/2020, available at: **https://filter.watch/en/2020/06/19/policy-monitor-may-2020/**

with a filtering order for Instagram. This led to speculation that a new order had been issued for the filtering of the popular social media platform, which is one of the only major international platforms not currently filtered in Iran.

However, this speculation was quickly laid to rest when an ICT Ministry spokesperson Jamal Hadian tweeted pages from Jahromi's written defense statement.[18] According to the statement, Jahromi was indicted on the basis of a number of claims:

- Non-compliance with a May 2018 order to block Instagram;
- Complaints from 432 people from Ahvaz regarding the use of cyberspace in a terrorist attack in Ahvaz Province[19] (a claim which appears to have first been made in 2019)[20];
- Complaints about an interview with the ICT Minister regarding the Islamic Republic of Iran Broadcasting's (IRIB) control over 700 and 800 MHz frequency bands;
- Complaints about a tweet from Jahromi relating to bandwidth increases.

Hadian confirmed that Jahromi had returned to work following a conditional release while the case is being investigated.

Rouhani reacted with anger in his first public appearance after the incident, announcing his full backing for his ICT Minister.[21] He also hinted that Jahromi was summoned for not limiting international internet bandwidth in the country; a position that he defended. Although Judiciary officials later dismissed the claim that the summons was related to a decision over Internet bandwidth in Iran,[22] Hadian disputed the Judiciary's account.[23]

At the time many commentators attributed Jahromi's court summons to political maneuvering ahead of Iran's upcoming June presidential elections. The case has not progressed further since Azari Jahromi's release.

[18] @jamal_hadian, *Twitter*, Tweet [Persian], 20/01/2021 11:01, available at: **https://twitter.com/jamal_hadian/status/1351847338457882630**

[19] BBC News, 22/09/2018, "Iran military parade attacked by gunmen in Ahvaz", available at: **https://www.bbc.co.uk/news/world-middle-east-45611411**

[20] 8DeyNews, 20/03/2019, "Likely to hear a complaint against the ICT Minister in the next year" [Persian], available at: **https://bit.ly/3xOucDn**

[21] Radio Farda, 27/01/2021, "'Try Me:' Rohani Warns Judiciary Over Telecoms Minister's Prosecution", available at: **https://bit.ly/3hwc0st**

[22] Mehr News, 27/01/2021, "The summoning of Azeri Jahromi has nothing to do with the issue of bandwidth", [Persian], available at: **https://bit.ly/3f1BoDs**

[23] @jamal_hadian, *Twitter*, Tweet [Persian], 27/01/2021 17:15, available at: **https://twitter.com/jamal_hadian/status/1354478203436470276**

IRIB and ICT Ministry Clash Over Broadcasting Frequencies, Online Content Oversight

The ICT Ministry has not only come to blows with the parliament and the judiciary, but also Iran's state broadcaster Islamic Republic of Iran Broadcasting (IRIB). In an interview on 23 May the Secretary to the SCC, Abolhassan Firouzabadi commented[24] on the longstanding[25] tension between the ICT Ministry and the IRIB over the management of the 700MHz and 800MHz broadcasting frequency bands. Both institutions claim that they are the legitimate managers of these bands.

In recent months Azari Jahromi has revived the argument, asking the President to weigh in on the issue in favour of the ICT Ministry, in order to help meet increased network demands, especially in light of the COVID-19 pandemic. Azari Jahromi had also reportedly said that he would offer "free internet" for the domestic education app Shad if the ICT Ministry is given ownership of the frequency bands.

Firouzabadi said that the SCC has not yet been asked to deliberate on the questions. However, he said he could not see how the frequency could have relevance to the Shad app, as its traffic is "negligible" and was mostly used "at home" so did not require mobile internet (despite the fact that mobile internet penetration rates remain far in excess of landline penetration rates across the country). He also added that the control of the frequencies by the ICT Ministry could have impacts on "job creation and the digital economy". He added that a decision on the ownership of the frequencies would depend on the ICT Ministry's plans for using them. He added that "there are no time pressures" to make a decision, as "there are still global conversations on whether there is enough technological readiness for these frequencies".

The ICT Ministry lost the same battle to IRIB in a vote in parliament in February 2019, when it voted against the transferral of the management of the bands from IRIB to the ICT Ministry.[26] The matter has not yet been formally referred to the SCC for a decision.

Another conflict between IRIB and the ICT Ministry resurfaced after the parliamentary election results, this time over these institutions' oversight of online multimedia content. On 12 January the Parliamentary Budgetary Consolidation Commission passed a resolution allocating the management and oversight of online content to the Islamic Republic of Iran Broadcasting (IRIB).[27] The Commission allocated a

[24] Mehr News, 23/05/2020, "Economic aspects of the 700 and 800 frequencies for the ICT Ministry" [Persian], available at: **https://bit.ly/3tnMtUJ**

[25] James Marchant, 17/04/2019, "Filterwatch—February 2019", available at: **https://medium.com/filterwatch/filterwatch-february-2019-8597e47c7fbe**

[26] *Ibid*

[27] Peivast, 12/01/2021, "New parliamentary decision: transfer of management of online content to IRIB" [Persian], available at: **https://bit.ly/3b275LV**

20,000 billion IRR (an estimated 475 million USD) budget for online content creation split between the IRIB and the Islamic Development Organisation's Culture and Communications Organisation.

The resolution still needs to be debated in a public session in Parliament, and approved by the Guardian Council before it becomes law. This is not the first time that plans to hand over content-related management and oversight to the IRIB have been raised. The ICT Ministry criticised the resolution. ICT Minister Azari Jahromi previously described such a move as an "obstacle" to realising content and services for the National Information Network (NIN).[28]

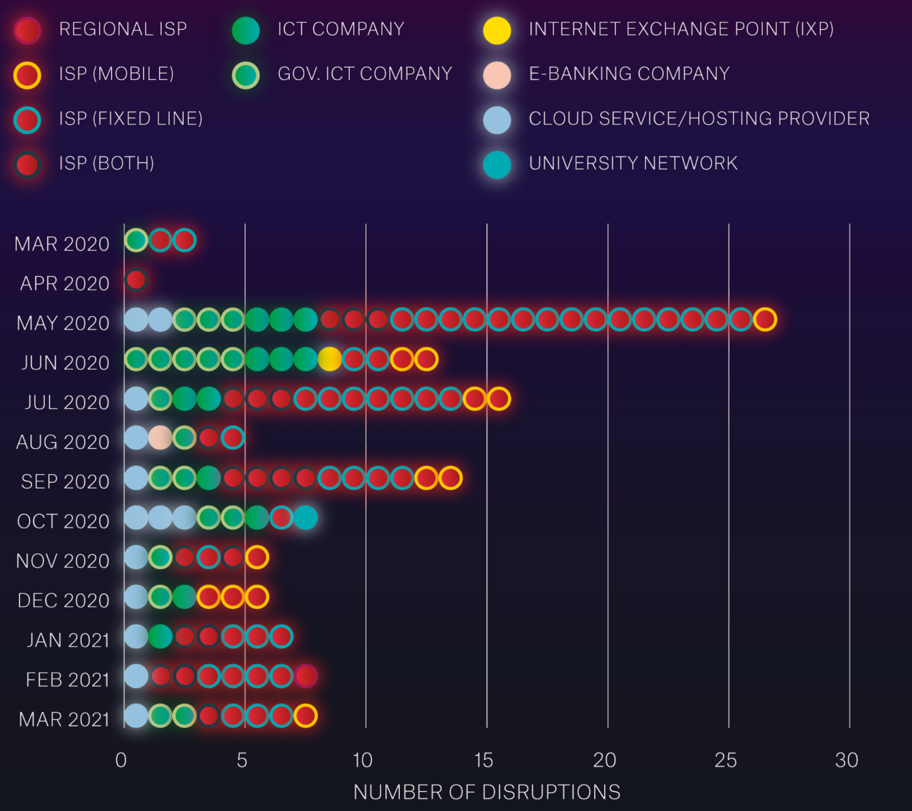
[28] Arash Parsapour, *Digiato*, 12/01/2021, "Control over cyberspace content; Will the parliament make IRIB's dream a reality?" [Persian], available at: **https://bit.ly/3eYNZaD**

NETWORK MONITOR 1399

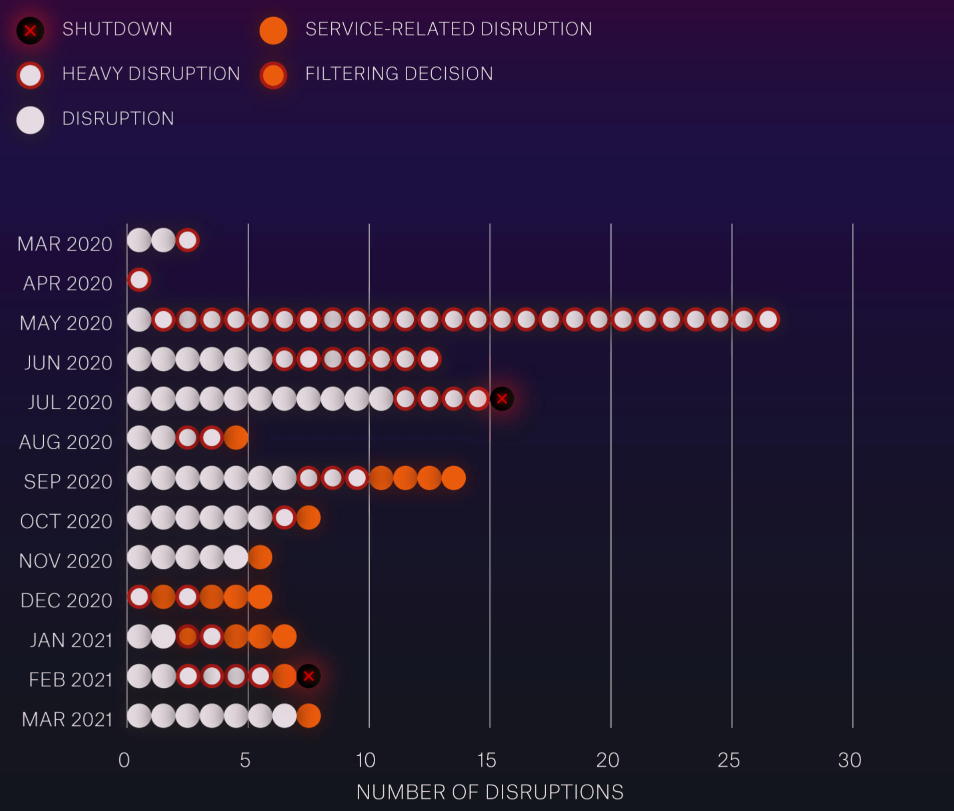
THIS visualisation summarises the findings of Filterwatch's monthly Network Monitor reports over the course of the Iranian calendar year 1399 (March 2020 – March 2021). The data for this visualisation was collected via the tools provided by Oracle Internet Intelligence (OIM) Map, and Internet Outage Detection and Analysis (IODA). This data is representative of observed disruptions during this period, however it is not exhaustive – other disruptions may have taken place, but were not observed.

The data shows that numerous disruptions were detected across the Iranian internet over the course of this year, including two brief shutdown events: in response to protests in the city of Behbahan in July 2020, and to unrest in Sistan and Baluchestan province in February 2021.

MONTHLY DISRUPTIONS BY AS TYPE



MONTHLY DISRUPTIONS BY DISRUPTION TYPE

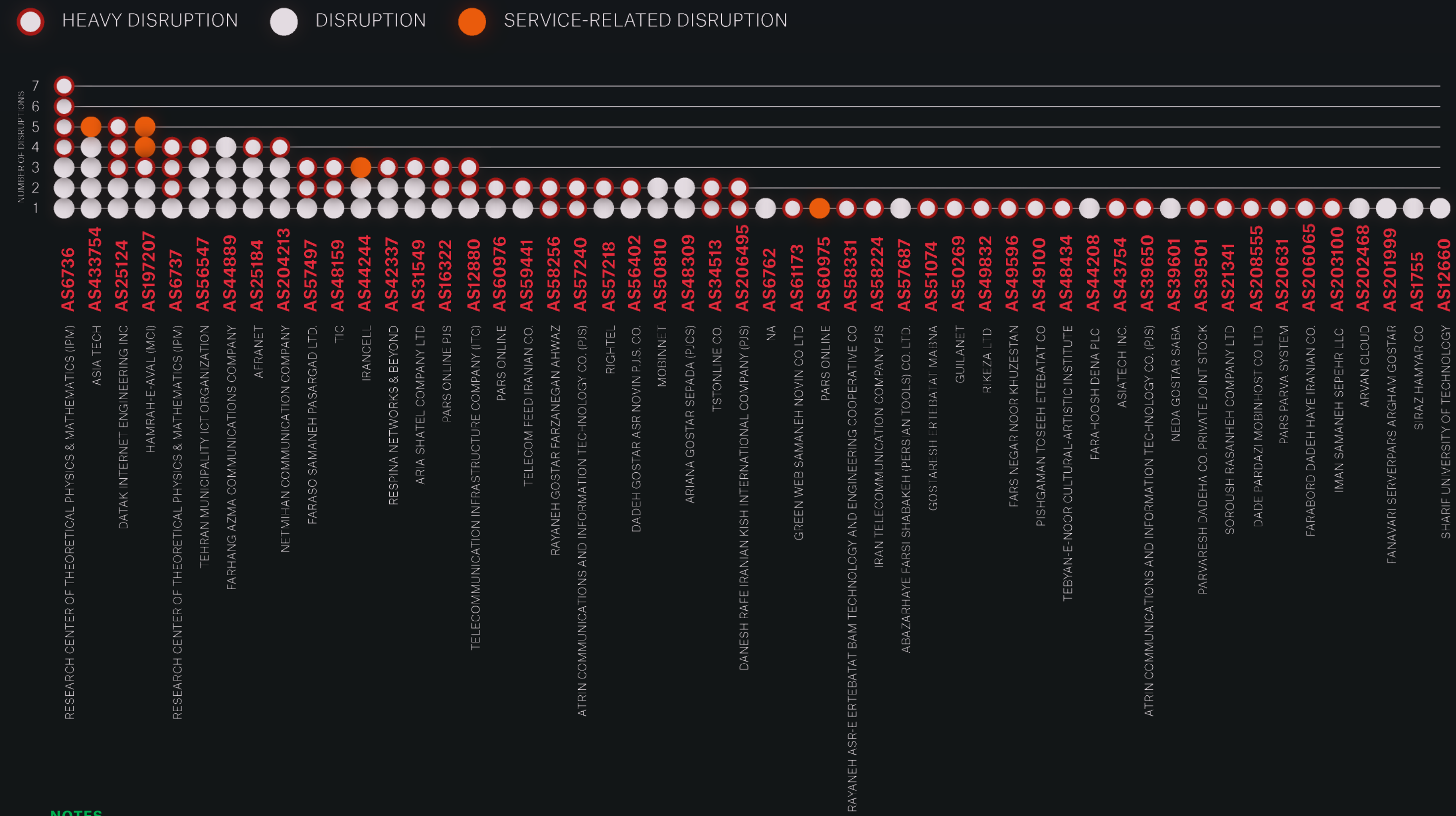


AT A GLANCE: ALL OBSERVED DISRUPTIONS

● NO DISRUPTIONS DETECTED
□ AT LEAST ONE DISRUPTION DETECTED

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
2020	MARCH	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	□	●	●	●	●	□	●	●	●	●	●	●
	APRIL	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	□	●	●	●	●	
	MAY	●	□	●	●	●	●	●	●	●	□	●	□	●	●	●	●	●	●	□	□	●	●	●	●	●	□	●	●	●	●	●
	JUNE	□	●	●	●	●	●	●	●	●	●	●	●	●	●	□	□	□	●	□	●	●	●	●	□	□	●	●	●	●	●	
	JULY	□	●	●	●	●	●	●	□	●	□	●	●	●	●	●	□	●	●	●	●	●	●	●	□	●	●	●	●	●	●	●
	AUGUST	●	□	●	●	●	□	●	□	●	●	●	□	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	SEPTEMBER	●	●	●	●	●	●	●	●	●	●	●	●	●	□	●	●	□	□	□	□	●	□	●	●	□	●	●	●	●	●	
	OCTOBER	●	●	●	●	□	●	●	□	□	●	●	●	□	□	●	●	●	●	●	●	●	●	●	●	●	□	●	●	●	●	●
	NOVEMBER	□	□	●	●	●	●	●	●	●	●	●	●	●	●	●	□	□	●	●	●	●	●	●	●	●	●	●	●	●	●	
	DECEMBER	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	□	●	□	□	□	●	●	●	●	●	●	●	●	●	●	□
2021	JANUARY	●	●	●	●	●	□	●	●	●	●	●	●	□	●	●	●	●	●	●	●	●	●	□	●	□	●	●	●	●	●	●
	FEBRUARY	□	●	●	●	●	●	□	●	□	●	●	●	●	●	●	●	●	●	●	●	●	●	●	□	●	●	●	●			
	MARCH	●	□	●	●	□	●	●	●	□	●	●	●	□	□	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

DISRUPTIONS BY AS NUMBER



NOTES

"Disruption" events are identified where OIM showed an anomalous fall in traceroutes of <50%
"Major Disruption" events are counted where OIM showed an anomalous fall in traceroutes of >50%. And <100%
"Shutdown" events are counted where OIM, IODA, or reliable alternative sources report sustained, complete service disruptions.
"Service-Related Disruption" events are counted when individual services experience temporary disruptions.
"Filtering Decision" events mark the permanent filtering of individual services.
"AS" means "autonomous system", and represents a single network or a group of networks that is controlled by a common network administrator

2 / INFORMATION CONTROLS

IRAN continues to employ one of the world's most sophisticated information controls regimes to restrict the free flow of information within the country. At the start of the Rouhani era, Iran operated a largely reactive model of filtering – blocking popular platforms and services as they emerged, and relying on content filtering techniques that could mostly be easily countered via VPNs. But over the past several years, the Rouhani administration and senior policy-making bodies such as the SCC have overseen the development of new tools to inhibit free expression online.

Content filtering remains, but an altogether more dangerous threat stems from Iran's increasing capacities to impose nationwide and regional internet shutdowns. With the expansion of the NIN, these shutdowns can be imposed at a lower cost, with domestic services remaining online. At the same time, this year saw the further implementation of plans to develop "layered filtering" infrastructure that could see different types of internet users granted different levels of access to the global internet. With the technological and regulatory structures underpinning "layered filtering" now broadly in place, we anticipate that these new information control measures are likely to be rolled out further in the year ahead.

2.1 CONTENT FILTERING

Given that most popular international apps and websites have already been blocked in Iran, fresh announcements about the filtering of foreign platforms by Iranian authorities have been few and far between in recent years. However, this year did see one more high-profile victim of Iran's programme of filtering: the messaging app Signal. On 25 January a number of outlets reported that Iranian users were experiencing difficulty accessing the Signal app, suggesting that the app had been blocked.[29] These disruptions were identified a few days after a series of other disruptions to the Signal website. Prior to Signal being filtered, the app was removed from Iranian app stores on 14 January as per an order from the CDICC.[30]

Signal was previously blocked in December 2017. Although it is unclear exactly who gave the order, ISNA reported that the Prosecutor-General's office was responsible.[31] The app was unblocked a short time later without any formal explanation. The filtering of Signal is unsurprising in light of Iran's overarching internet policy objectives to promote and encourage the use

[29] Arash Parsapour, *Digiato*, 25/01/2021, "Signal messenger is unavailable" [Persian], available at: **https://bit.ly/3bwqJA2**

[30] Arash Parsapour, *Digiato*, 15/01/2021, "Signal app removed from Iranian app stores" [Persian], available at: **https://bit.ly/3ul8oMP**

[31] ISNA, 27/01/2021, "Who Filters?" [Persian], available at: **https://bit.ly/3vkerm3**

of domestic apps over more secure international equivalents.

In 1399 we also witnessed Iranian authorities using domestic copyright laws to block websites. According to an announcement on 31 October from the Regulatory Organisation for Audio and Visual Media (SATRA), 15 websites and applications were 'blocked' following complaints received from the copyright right holder for the Iranian TV show 'Aghazadeh'.[32]

However, in the year 1399 there have not been further blocking of websites which proved to be the main tool of information control, but instead, we saw further instances of internet disruptions, the development of layered filtering, as well as the offline policing of online spaces.

2.2 INTERNET SHUTDOWNS AND DISRUPTIONS

Iran did not experience a national internet shutdown this year, however authorities did impose two regional shutdowns in response to localised protests in two of Iran's poorest and most marginalised provinces.

On July 16, in response to a protest in the southwestern city of Behbahan, security forces fired tear gas to disperse protesters.[33] The protest started at roughly 20:00 local time, and mobile internet access was cut off from around 20:45 in the neighborhoods where protests took place. During this shutdown mobile services had been completely cut off, unlike in November 2019 when domestic sites were accessible during the shutdown.

The second (and longer-lasting) incident took place in February. On 22 February Iran's Revolutionary Guard Corps (IRGC) forces clashed with fuel traders in the city of Saravan, near the Iran-Pakistan border. The incident sparked protests around Sistan and Baluchestan Province in the following days. In total, the government crackdown on protests resulted in the deaths of at least ten people according to Amnesty International,[34] and potentially up to 23 according to an OHCHR statement.[35]

According to local sources in Zahedan, at around 21:00 local time on February 24 a small group of protestors set fire to a poster of Supreme Leader Ali Khamenei in front of the IRGC Intelligence Organization's local office. This incident led to a further protest.

[32] SATRA, 31/10/2020, "15 media outlets infringing on the intellectual property of domestic drama series were blocked" [Persian[, available at: **https://bit.ly/3eVdH14**

[33] Parisa Hafezi, Reuters, 16/07/2020, "Iran security forces fire tear gas to disperse protesters", available at: **https://reut.rs/3hxwAsk**

[34] Amnesty International, 04/03/2021, "Iran: Internet Shutdowns Curb Protests And Conceal Human Rights Violations In Sistan And Baluchistan", available at: **https://www.amnesty.org/en/documents/mde13/3782/2021/en/**

[35] OHCHR, 05/02/2021, "Press briefing notes on Iran", available at: **https://bit.ly/3v0fyr2**

At around 21:30 local time mobile data was heavily disrupted, and by 21:40 all mobile operators had been disconnected from the internet in the cities of Zahedan, Khash, Saravan, Zabol, Darak, and Chabahar. A province-wide shutdown of all local and international internet services – via mobile and landline connections – persisted until 27 February.

2.3 LAYERED FILTERING

For several years now, we have been hearing whispers of Iran moving toward a "layered filtering" model of information control. Under this model, users are granted different levels of privilege to access online content depending on their employment status, age, social status, education level, or other attributes. Over the course of this year, Iranian policy-makers have taken further steps towards realising such a system, developing a scheme for the regulation of "legal VPNs".

On 13 April 2020, SCC Secretary Abolhassan Firouzabadi announced that regulatory guidance for legal VPNs had been finalised by the CDICC.[36] He noted that the ICT Ministry would be made responsible for deciding who will have access to legal VPNs. Although the text of this regulatory guidance has not yet been published, the little information which was later relayed to the public on the progress of the scheme raised further concerns that these legal VPNs are in fact the infrastructure needed for implementation of a layered filtering regime in Iran.

On 5 April 2021 Sajjad Bonabi, a board member of Telecommunication Infrastructure Company, announced that certain user groups "such as university professors, students, doctors and journalists" would soon be granted permission to access YouTube.[37] These comments led to speculation that such groups would be able to register for highly monitored government-issued VPNs, which could facilitate access to otherwise filtered platforms. Such a system threatens to further extend authorities' power to regulate Iranian internet users' access to online content, and to monitor their online activities.

2.4 ARRESTS, DETENTIONS AND EXECUTIONS

Iran continued to target journalists and human rights advocates on the basis of their online activities this year. The most high-profile case was that of the dissident journalist Ruhollah Zam, who previously managed the

[36] ITIran, 13/04/2020, "The ICT Ministry is responsible for assigning legal VPNs to eligible individuals" [Persian], available at: **https://bit.ly/3sz1fsz**

[37] Arash Parsapour, *Digiato*, 05/04/2021, "Removal of filtering of some sites begins for a section of the community" [Persian], available at: **https://bit.ly/3uscnrA**

Telegram channel Amad News. Zam was abducted and brought back to Iran from exile in October 2019. He was sentenced to death on 30 June 2020, and subsequently executed on 12 December.[38]

Zam's execution was condemned by international human rights organisations[39] and UN human rights experts,[40] and has been pointed to as an example of Iran's ongoing war against journalists and freedom of expression online.

Iran has not only targeted its political opponents in the past year, but worryingly, Iranian authorities have moved to arrest a number of Iranians working in the technology sector after accusing them of permitting undesirable content on their platforms. Mohammad Javad Shakuri Moghadam, CEO of the Iranian video sharing platform Aparat was sentenced to twelve years' imprisonment, including ten years for 'encouraging corruption', one year for 'propaganda against the system', and one year for 'publishing vulgar content'.[41] This charge came after a video was uploaded to Aparat in which an adult asked a number of children if they "knew how they had been born".

This case brings into question the responsibilities of platforms and hosting services in respect of user-generated content. Iran's laws currently do not offer clarity on the issue of intermediary liability, although Iran's Computer Crimes Law does hold Internet Service Providers (ISPs) responsible for users accessing illegal content. Meanwhile, Iran's Audiovisual Media Regulatory Authority (SATRA) issued a statement criticising the verdict, supporting Shakuri Moghadam, and arguing for the principle that intermediary platforms should be protected from prosecution relating to user-generated content, so long as they have substantive content moderation policies in place.[42]

According to a statement from Aparat, the company will appeal the sentence. In any case, this case offers a clear example of Iranian authorities' desire to outsource some of its information control strategies to domestic tech companies, by intimidating them into enforcing stringent content moderation policies.

On 26 December the NCC's Office for Cultural, Social and Content Affairs published a report on the 'Status of Mobile Applications and Stores' and called for expansion of Halal content domestically.

[38] Amnesty International, 12/12/2020, "Iran: Execution of journalist Rouhollah Zam a 'deadly blow' to freedom of expression", available at: **https://bit.ly/3fFwNHr**

[39] *Ibid*

[40] OHCHR, 14/12/2020, "Iran: UN experts condemn execution of Ruhollah Zam", available at: **https://bit.ly/2QQdjaT**

[41] Arash Parsapour, *Digiato*, 26/10/2020, "Why was the CEO of Aparat sentenced to 10 years in prison?" [Persian], available at: **https://bit.ly/3xQvuOc**

[42] IMNA, 26/10/2020, "SATRA's comment about the conviction of Aparat's site administrator" [Persian], available at: **https://bit.ly/2R2bGXF**

3/ STATE SURVEILLANCE

IRAN'S Cyber Police (FATA) continues to play a leading role in the implementation of online surveillance in Iran. In late 2018, we have seen high-ranking FATA officials boasting about "society-based surveillance" in which "every citizen is a police officer", relying on thousands of volunteers to help them monitor online spaces.[43] Since then, our FATAwatch project has documented many hundreds of arrests for charges stretching from online fraud, to vague accusations of "spreading rumours", and to loosely-defined morality charges.

Over the course of this year, FATA's online surveillance practices were closely entwined with Iran's reaction to the COVID-19 pandemic, with FATA leading the state's charge against "disinformation" online. In practice, FATA's crackdown has extended to target journalists and other internet users who offer legitimate criticisms of Iran's handling of the pandemic.

Elsewhere, FATA's surveillance and law enforcement practices continued in much the same vein, with regular social media users monitored and targeted in the even that their online activities cross the state's established 'red lines' on cultural issues. As ever, these surveillance and control measures are deeply gendered, with Iranian women frequently being pursued for not wearing the hijab in images or videos, or for other supposed "moral" violations.

3.1 THE COVID-19 PANDEMIC AND IRAN'S CRACKDOWN ON "DISINFORMATION"

In the early months of the pandemic, when panic and uncertainty were widespread, FATA acted quickly and brutally to suppress online speech about the disease and its progression. Between March and May, the rapid spread of COVID-19 in Iran did result in the emergence of online rumours about the disease, and the government's response. Rumours included discussions about possible local lockdowns in certain cities, reports on shortages of medical equipment, and the low readiness of Iranian hospitals, among many other issues. The spread of such conversations was met with a tough response from the country's security forces and judiciary; in April individuals were identified and arrested for 'spreading rumours' about COVID-19 in the cities of Mahabad, Hormozgan, Mazandaran, Fars, Western Azerbaijan, Kerman, Kohgiluyeh and Boyer Ahmad, and Tehran.[44] It is unclear how many

[43] Kaveh Azarhoosh, 19/01/2019, "Iran's Cyber Police — 'Society-Based Policing' and the Rise of Peer Surveillance", available at: **https://bit.ly/3uZDYkg**

[44] Cyberpolice.ir, multiple dates, **https://tinyurl.com/yxl29tbx** (Mahabad), **https://tinyurl.com/y933825a** (Hormozgan), **https://tinyurl.com/y625smer** (Mazandaran), **https://tinyurl.com/y4phxp4t** (Fars), **https://tinyurl.com/y3gopquc** (Western Azerbaijan), **https://tinyurl.com/y38we537** (Kerman), **https://tinyurl.com/y4vn8ess** (Kohgiluyeh & Boyer Ahmad).

of those arrested were subsequently charged.

According to an announcement by the FATA Chief for Fars Province, Colonel Heshmat Soleimani, at least 24 people were arrested in the province for 'spreading rumours' about COVID-19.[45] The Head of FATA Police also commented that 118 people were arrested for spreading rumours online.[46] According to a senior spokesperson for Iran's Armed Forces, both the Basij and Police had arrested up to 3,600 people by April 29 for spreading "false information or rumours" online.[47]

The scale of these arrests is alarming, especially in light of the fact that FATA operates with no transparency, and a history of suppressing legitimate online expression. There is a severe risk that any state-backed actions to counter "disinformation" online could provide cover for the suppression of legitimate criticisms of the government's handling of the crisis. Iran's response to journalists' criticisms proved that these concerns were justified: on 23 April Masoud Heydari, the Managing Director of the Iranian Labour News Agency (ILNA), and Hamid Haghjoo, the administrator of ILNA's Telegram channel were arrested for publishing a cartoon that briefly appeared on the news agency's Telegram channel.[48] The cartoon – which was deleted shortly after it was posted – mocked the unscientific remedies to COVID-19 promoted by religious individuals and public figures.[49]

The economics reporter Mohammad Mosaed was also interrogated by security forces in late February after he posted a series of tweets questioning the country's handling of the COVID-19 pandemic. It appears that during his interrogation, security forces took control of Mosaed's online accounts. In an interview with BBC Persian, Mosaed stated that he is banned from publishing any online content until his court appearance.[50]

3.2
FATA'S CONTINUED ROLE IN CULTURAL POLICING

This year, FATA continued its programme of policing online spaces to ensure their

[45] Aftab News, 06/04/2020, "Arrest of 24 people in Fars", available at: **https://bit.ly/3vSTxdt**

[46] Cyberpolice.ir, date unavailable, "Warning to rumour-mongers in cyberspace", available at: **https://tinyurl.com/y9snvwjq**

[47] Khabar Online, 29/04/2020, "Arrest of 3,600 online rumor spreaders" [Persian], available at: **https://bit.ly/3tzMfd0**

[48] Committee to Protect Journalists, 27/04/2020, "Iran arrests 2 journalists for allegedly sharing cartoon mocking government's COVID-19 response", available at: **https://cpj.org/2020/04/iran-arrests-2-journalists-for-allegedly-sharing-c.php**

[49] Iranwire Persian, 23/04/2020, "ILNA News Agency denies the publication of a cartoon on Islamic medicine" [Persian], available at: **https://iranwire.com/fa/jinac/37955**

[50] @bbcpersian, *Twitter*, Tweet [Persian], 22/02/2020, 19:47 UTC, available at: **https://twitter.com/bbcpersian/status/1231304603574116353**

compliance with state interpretations of religious morality. To this end, FATA engaged in widespread monitoring of social media users, persecuting a significant number of regular users and a handful of high-profile 'influencers' for their online attire. Such persecutions are deeply gendered, with women the subject of much of authorities' moral policing actions.

On 20 May, FATA Deputy for Social Affairs Colonel Pashaei stated that "over 320 people were arrested" in relation to their online activities. He reiterated that not wearing a hijab online constitutes "inappropriate behaviour" and will be considered a crime.[51]

The FATA Chief for Eastern Azerbaijan Province also reported the arrest of an individual who had attempted to "lure in and hire young, single women as models, through the Divar platform".[52] Elsewhere, the Prosecutor for the city of Amol stated that a woman had been arrested for posting "immoral" photos online.[53] Also in the same month, FATA agencies in the cities of Ilam[54] and Tehran[55] reported further arrests relating to social media content, including of a teenage girl who posted photos and videos of "illicit parties".

On 9 March 2021 the Instagram influencer Milad Hatam Abadi Farahani (otherwise known as Milad Hatami) was arrested by Turkish police and handed over to Iranian authorities at the Iranian -Turkish border.[56] According to Hadi Shirzad, the Head of International Police in Iran, an Interpol red notice was issued for Hatami's arrest for charges relating to "cybercrime, fraud and money laundering". Prior to his arrest Hatami lived in Istanbul with his wife and daughter.

Also in March, following the popularity of the "Iran, Tokyo" music video by the exiled Iranian pop singer, Sasan Yafteh (also known as Sasy) (formerly known as Sasy Mankan) released in March 2021 - featuring a cameo from the adult film star Alexis Texas - Iran's Judiciary announced that a number of people "involved in the production of the video" had been arrested, and warned that those who use the app Dubsmash to share the song further would be

[51] Payam-e Iran, 20/05/2020, "FATA Police Social Deputy: Hijab on Instagram is mandatory for Iranians" [Persian], available at: **https://bit.ly/2Q7vmce**

[52] Cyberpolice.ir, "Young women modelling illegally on the website Divar" [Persian], available at: **https://bit.ly/3hiJydt**

[53] Borna News, 17/05/2020, "Woman arrested on charges of publishing immoral images" [Persian], available at: **https://bit.ly/2Q96vos**

[54] Cyberpolice.ir, "Arrest of the leader of an immoral group on Telegram" [Persian], available at: **https://bit.ly/3tzevMU**

[55] Cyberpolice.ir, "Increasing followers at any price" [Persian], available at: **https://bit.ly/2Q5UzDS**

[56] R.F.I, "Gambling and betting site owner Milad Hatami in Turkey handed over to Iranian police", 10/03/2021,[Persian], Available at: **https://bit.ly/3fsvFYI**

prosecuted.[57] It was also added that should the video be released in full, Iran's Judiciary would use "international resources" to prosecute the singer. The video has since been released, and it is unclear whether the Judiciary has taken any steps against the singer.

[57] Masoud Azar, 11/03/2021, "From Tehran to Tokyo, from the Somyeh of the revolution to Sasy's Somayeh", BBC Persian, [Persian], available at: **https://bbc.in/3foKjjO**

4/DIGITAL INCLUSION

ALL around the world, the COVID-19 pandemic has forced people into unprecedented levels of dependence on the Internet, in order to allow them to continue working, and students to continue learning. But of course, not everyone has equal levels of access to the Internet, and digital divides have ended up having huge implications: both for people's livelihoods, and for the spread of the disease.

In Iran, the introduction of mandatory online distance learning software for schoolchildren highlighted a number of entrenched and persistent inequalities in access. In particular, the lack of connectivity in Iran's most deprived provinces became ever more visible during the pandemic, whereas those communities even further on the margins – such as Iran's large population of Afghan refugees – found themselves shut out from crucial pieces of digital infrastructure.

4.1 THE DIGITAL ACCESS GAP AND MARGINALISED COMMUNITIES

In response to the urgent need for online infrastructure for distance learning on 9 April the Ministry of Education announced the launch of the new domestic e-learning platform known as "Shad" (the Persian-language acronym of "Student Educational Network"), which is available to download via the platform's website.[58] Following the reiteration of the ban on the use of foreign messaging apps by public bodies, government organisations, schools and universities by the judiciary this February, the opportunity is being used to enforce and normalise the use of domestic analogues.[59]

However, Shad is already causing concern and challenges among users and digital rights activists – particularly given its implementation in an environment such as Iran, where enormous gaps in digital access remain between, and within provinces. Throughout this year Iranian media reported on a number of tragic suicides of minors in deprived regions of Iran, owing to the pressures imposed by a lack of adequate access to the Internet, or to electronic devices needed to access Shad.[60] The issue attracted such public concern that on 2 December it was reported that a new bill titled "Free Internet for Students, Teachers and Schools'" containing just one article and one sub-clause was introduced in

[58] Shad Homepage [Persian], available at: **shaddl.medu.ir**

[59] Melody Kazemi, *Filterwatch*, 20/03/2020, "Filterwatch Policy Monitor — February 2020", available at: **https://bit.ly/3tXkag6**

[60] Shahrara News, 12/10/2020, "'My son committed suicide because he did not have a mobile phone' - Mother of Bushehri 11-year-old boy explains her child's death" [Persian], available at: **https://bit.ly/3od4pAo**

the Majles to help address these gaps in access.[61]

The bill called for the use of the education app 'Shad' to be made free for the academic year 2020-2021, and for the state to provide 'one million free tablets' for students by the end of September 2020. However, Jahromi had claimed in September 2020 that 'an order will be issued to ISPs for the use of Shad to be made free'.[62] He also stated in December that the use of the app would be free, and that any issues with its use are related to 'technical difficulties'.[63] The slow progress of the bill has meant that the articles cannot be fulfilled in the time frame provided and it has been commented that the bill is unlikely to be passed by the Guardian Council as it does not make its source of funding clear. Some operators had also announced that they would not charge a fee for the use of Shad, despite some confusion earlier this year following the announcement of free internet packages for students and teachers by the ICT Ministry.[64]

Initially, there were also major concerns about the accessibility of the app to the Afghan migrant community in Iran. On 14 April the Association for the Protection of Refugee Women and Children (HAMI), an Iranian refugee protection NGO, raised concerns about the accessibility of the app by Afghan refugee children.[65] Their concerns stemmed from the fact that the app requires a national ID number to be entered in order to access it – something that refugee children often lack. According to HAMI, the Ministry of Education has now "resolved" the issue to allow foreign children to access the app.

These legitimate questions once again provided the Iranian ICT Ministry with the opportunity to frame NIN investments in terms of expanding access and sidelining the concerns around digital rights and the project. A report by the ICT MInistry on 17 May claimed that 1,578 additional villages had recently been connected to the NIN and 632 villages had been connected to mobile networks via operator Hamrah-e Avval (MCI), a subsidiary of the Telecommunication Company of Iran (TCI).[66]

According to this report 89% of villages with a population of over 20 families

[61] Peivast, 02/12/2020, "ICT Ministry must provide free internet for Shad" [Persian], available at: **https://peivast.com/p/90716**

[62] ISNA, 12/09/2020, "ICT Minister: Use of the Shad app will be free" [Persian], available at: **https://bit.ly/3we8Xcv**

[63] IRNA, 08/12/2020, "ICT Minister: The Shad network is free" [Persian], available at: **https://bit.ly/3fojLy8**

[64] Moshaver Group, "How to activate free Shad access for Irancell, Hamrah-e Aval and RighTel" [Persian], available at: **https://bit.ly/3wco8TC**

[65] @hamiorg, *Twitter*, Tweet [Persian], 14/04/2020, 10:28 UTC, available at: **https://twitter.com/hamiorg/status/1249992969530245120**

[66] Iranian ICT Ministry, 17/05/2020, "Connecting more than 1500 villages to the National Information Network" [Persian], available at: **https://bit.ly/3eWC6Db**

have been connected to the NIN, with the aim of reaching 100% by March 2021. Additionally 93% of villages now have mobile network coverage with an aim of “reaching 100% [coverage] for villages with over 20 families by the end of the year”.

5 / INFRASTRUCTURE & INFORMATION CONTROLS

THE expansion of Iran's National Information Network (NIN) is being marketed by the Iranian government as the underpinning for a massive expansion of internet access to so-far disconnected segments of Iran's population. As noted in the previous chapter, there is some truth to this, and rural connectivity continues to grow. But the NIN has been designed in such a way that there are costs to this expansion of access, to be paid through further limitations on user privacy, and the expansion of the state's abilities to cut Iran off from the global Internet.

Iran is leveraging its investments into domestic infrastructure to construct a new regime of information control based on localised data hosting – encouraging domestic businesses and content creators to host their data on local servers where it can be more easily surveilled and requisitioned.

5.1 PRIVATE COMPANIES & THE NATIONAL INFORMATION NETWORK

On 25 February Twitter users highlighted problematic clauses from the Public-Private Partnership Agreement between Arvan Cloud and the Iranian Information Technology Organisation (ITO).[67] Specifically, they noted how Article 4 raised questions about the role of the "Iran Cloud" project in localisation of Iran's internet.[68] Article 4 requires "legal interception" of all equipment and services, as well as the implementation of any "disconnections, connections, and restrictions" requested by the ITO.

These clauses are described as being based on "national and public security"-related measures. However, in the absence of legal limits, checks and balances, the absence of an independent Judiciary, and Iran's record of limiting online expression, broad and ambiguous concerns such as "national security" can be abused to infringe on Iranian's human rights. The Iranian private technology sector must do much more to protect the privacy and security of their users and acknowledge their human rights obligations to their users, by refraining from engaging in projects which contribute to the expansion of the NIN.

Other than Iran Cloud, this year also saw the implementation of other infrastructure projects designed to significantly expand Iran's domestic hosting capacities. According to the ICT Ministry, the largest data centre in Iran's north-west was unveiled in

[67] Iran FOIA [Persian], available at: **https://iranfoia.ir/web/guest/orgbaseddocs**

[68] Melody Kazemi, *Filterwatch*, 10/02/2021, "Policy Monitor – January 2021", available at: **https://filter.watch/en/2021/02/10/policy-monitor-january-2021/**

the city of Tabriz on 26 June.[69] The data centre was established by the Mobile Telecommunication Company of Iran (MCI), a subsidiary of the Telecommunication Company of Iran (TCI). The ICT Ministry claims that the data centre has capacity for "250 to 350 [server] racks, 1,500 physical servers and 16,000 virtual servers".

The expansion of domestic data hosting capacities is not just about improving the performance of domestic networks; it is also about developing the necessary infrastructure to support the growth of the NIN's own domestic apps and services, including domestic messaging apps. On 29 August the Deputy Director of the Telecommunications Infrastructure Company (TIC) Sajad Bonabi announced the launch of the first phase of the "Primary NIN Data Centre" in Bumahen, Tehran Province, with a planned capacity of 100 server racks.[70] According to Bonabi, the Primary Data Centre will first provide unspecified technical services free-of-charge to domestic messaging apps, and from its second phase will provide these services to domestic search engines and cloud-based services.

The Iranian cloud service provider Derak Cloud said in its "Annual Report on the State of the Internet in Iran 1399" that, based on its users' data, there had been a 10% increase in the use of domestic hosting services on the previous year.[71] Such statistics suggest steady progress is being achieved in Iran's drive towards expanded data localisation – potentially reducing some sanctions-related frictions for Iranian businesses, but also reducing friction for the state if it chooses to impose future internet shutdowns.

[69] Iranian ICT Ministry, 26/06/2020, "The largest data center in the west and northwest of the country will be opened" [Persian], **https://bit.ly/2Q5uqVL**

[70] Mehr News, 29/09/2020, "Providing free services to domestic media via the 'Mother Network' of the NIN" [Persian], available at: **https://bit.ly/33wmhwE**

[71] Derak Cloud, 08/05/2021, "Annual Report on the State of the Internet in Iran - 1399" [Persian], available at: **https://bit.ly/3fs0f3G**

6 / DATA SECURITY

OVER the course of this year, Iranian internet users were plagued by a number of additional data leaks and cyber attacks that highlighted the urgent need for the introduction of strong, privacy-protecting data protection legislation in the country's legislature. Until Iranian authorities introduce proper safeguards to protect Iranians' data, it seems inevitable that such leaks will continue to leave the public open to the risk of personal and financial harm.

In this chapter we offer a brief overview on some of these incidents, and their implications for the safety and security of Iranian internet users.

6.1 DATA lEAKS

According to a report by Comparitech on 30 March 2020, data from 42 million Iranian users from Telegram clones or "forks" (unofficial and unaffiliated versions of the app) including user IDs, telephone numbers, usernames, and hashes and secret keys.[72]

Compatitech added that a group known as "Hunting System" posted the data on Elasticsearch, which could be viewed without a password or authentication. It has been confirmed that the data was exposed for "around 11 days" before it was removed from Elasticsearch on 25 March. However, before it was removed unauthorised users had already accessed the data, and one user had posted the data on a hacking forum.

The filtering of Telegram has led to many Iranian users to move to insecure cloned versions of the app which do not have the same security measures, putting their data at risk. Those whose data has been leaked are now vulnerable to phishing and SIM swap attacks.

In January 2021 it was discovered that Iranian social media app Raychat's entire database had been exposed online.[73] According to Security Researcher Bob Diachenko, who discovered the breach, the data included "'names, emails, passwords, encrypted chats, and metadata" for over 276 million accounts. This included records of "multiple accounts created by the same users" and a number of "automated bot accounts, due to the nature of Raychat services".[74] This data was later destroyed by a bot attack. Raychat acknowledged the breach on Twitter and in a statement on their website on 1 February. Raychat apologised to users for causing "anxiety" but denied seeing

[72] Paul Bischoff, *Comparitech*, 30/03/2020, "42 million Iranian "Telegram" user IDs and phone numbers leaked online: report", available at: **https://www.comparitech.com/blog/information-security/iranian-telegram-accounts-leaked/**

[73] Lucas Ropek, *Gizmodo*, 2/03/2021, "Iranian Chat App Gets Its Data Wiped Out in a Cyberattack", available at: **https://bit.ly/3f2eugw**

[74] @MayhemDayOne, *Twitter*, Tweet, 31/01/2021, 16:20 UTC, available at: **https://bit.ly/3vjie2S**

evidence of a data leak.[75] Despite this claim, Raychat had already tweeted on 31 January asking users "not to click on a link contained in password change emails" should they receive one,[76] suggesting they were concerned about potential phishing attacks.

While Iran has experienced a significant boom in its startup and tech ecosystem in recent years, an ongoing failure to introduce effective security standards and practices means that users are more vulnerable on these platforms in comparison to some of their international counterparts. Companies have a fundamental responsibility to enforce meaningful privacy and security standards in their digital services, as well as to provide their users with transparent information about how their data is stored and used. This is particularly urgent in light of Iran's continued failure to introduce meaningful data protection legislation in line with international standards.

[75] "Raychat's statement on vulnerability: [we] will be transparent and accountable in responding to users and customers", *Raychat*, 1/02/2021, available at: **https://bit.ly/34cimVZ**

[76] @Raychat_io, *Twitter*, Tweet, 31/01/2021, 14:56 UTC, available at: **https://bit.ly/3vjfqTA**

CONCLUSION

The final year of Rouhani's administration in many aspects was overshadowed by the global pandemic. Iranians have experienced an incredibly challenging year, with the ever-present threat of COVID-19 compounded by an ongoing economic crisis, international sanctions, and the further closure of political and civic space.

In the realm of internet policy, it was a testing time for the country's digital infrastructure, which faced enormous new burdens as users' dependence on online services soared. In many ways the infrastructure appeared to be generally adequate to deal with these challenges; the near-decade of heavy investment in the National Information Network has enabled increased levels of connectivity to domestic sites and services. While serious concerns remain about the lack of meaningful access in marginalised rural and low-income communities, the relative stability of internet connectivity across much of Iran last year demonstrated that Iranian internet users are enjoying some benefits from the state's investments in digital infrastructure.

Of course, there is a darker side to this story, with improvements in internet infrastructure arising from the Rouhani administration's drive to implement the state's vision of a highly connected, but tightly controlled online realm. From outside, the Iranian internet seems more connected than ever before, but from within, this network feels more insular and oppressive than when connectivity was limited to a smaller section of society.

This closure of online space has been shaped by the policies and regulations developed in the past few years – whether to counter "disinformation", to regulate messaging apps, or to facilitate new mechanisms of "layered filtering". Yet the effects of this closure are most plainly visible in the radical expansion of online policing, and the skyrocketing number of arrests made by agencies like FATA. This ongoing crackdown is not only designed to limit political speech, but to aggressively police state conceptions of morality in online spaces.

The state of online freedoms in Iran is poor, but there is a very real prospect of the situation declining further. Iranians are rightly concerned about the implications of the election of a hardliner or conservative candidate in the upcoming presidential elections. Fears range from the prospect of further nationwide internet shutdowns, to an intensification of online censorship and surveillance, and even the permanent disconnection of Iran from the global Internet.

Whoever sits in the driving seat after the next election has been handed the infrastructural and policy foundations to further disconnect and isolate Iranians from the global Internet. Ultimately, the design and implementation of the National Information Network is perhaps the Rouhani administration's most significant legacy – one that could have dire consequences for human rights in Iran for many years to come.

A FILTERWATCH REPORT

RESEARCH:
Kaveh Azarhoosh
Melody Kazemi
James Marchant

DESIGN:
Surasti Puri

JUNE 2021

FILTER
WATCH