# Flygtningenævnets baggrundsmateriale

| | |
|---|---|
| **Bilagsnr.:** | **1189** |
| Land: | Iran |
| Kilde: | UK Home Office |
| Titel: | Country Policy and Information Note. Iran: Social media, surveillance and sur place activities. Version 2.0 |
| Udgivet: | april 2025 |
| Optaget på baggrundsmaterialet: | 30. juni 2025 |
| | |

Home Office

# Country Policy and Information Note

## Iran: Social media, surveillance and sur place activities

**Version 2.0**

**April 2025**

# Contents

# Executive summary

Iran's Constitution and legal framework restricts online freedom of expression. Penalties for breaching Iran's Computer Crimes Law range from fines and judicial orders to custodial sentences and the death penalty for crimes committed against public morality and chastity. Authorities employ various tactics of control over, and heavily monitor, the internet. There is no evidence to suggest that Iran operates a mass surveillance programme to monitor the online activity of all its citizens.

Iranian intelligence officials also monitor and target high profile Iranian dissidents abroad, including the UK and other Western countries, including online activities and repeated or high-profile participation in anti-regime demonstrations.

A person fearing persecution from the Iranian authorities on account of their online activities is likely to fall within the Refugee Convention on the grounds of actual or imputed political opinion, race, and/or religion.

Social media users in Iran whose posts are deemed critical of the state or against its self-declared high moral standards, or who comment on sensitive issues, may be subject to treatment, including harassment, arrest, ill-treatment, torture and criminal charges, that is sufficiently serious, by its nature or repetition, to amount to persecution. The risk posed will depend on the person's profile, ethnicity, religion, the level and nature of their online activity, and/or the size of audience of their online activity.

A person who participates 'sur place' in demonstrations which are deemed critical of the Iranian state may be subject to treatment on return to Iran that is sufficiently serious, by its nature or repetition, to amount to persecution. The risk posed will depend on a nuanced consideration of factors outlined in the Country Guidance case of BA. These include the nature of the sur place activity, the risk that the person has been, or will be, identified, and whether the profile or history of the person is likely to trigger further inquiry or action on return to Iran.

A person who is 'sur place' openly critical of the Iranian regime online may be subject to treatment on return to Iran that is sufficiently serious, by its nature or repetition, to amount to persecution. The risk posed will depend on a nuanced consideration of factors outlined in the Country Guidance case of XX. These include a person's position on a "social graph", whether they are likely to have been the subject of targeted online surveillance, and whether a person has, or is likely to, close their social media account(s) prior to any potential "pinch points", when basic searches on the person are likely to be carried out.

Where the person has a well-founded fear of persecution or serious harm from the state, they will not, in general, be able to obtain protection.

Where the person has a well-founded fear of persecution or serious harm from the state, they will not, in general, be able to internally relocate to escape that risk.

Where a claim is refused, it is unlikely to be certifiable as 'clearly unfounded' under section 94 of the Nationality, Immigration and Asylum Act 2002.

All cases must be considered on their individual facts, with the onus on the person to demonstrate they face persecution or serious harm.

Back to Contents

# Assessment

Section updated: 26 March 2025

## About the assessment

This section considers the evidence relevant to this note – that is the country information, refugee/human rights laws and policies, and applicable caselaw – and provides an assessment of whether, **in general**:

- a person faces a real risk of persecution/serious harm by the state because of the person's social media use and/or sur place activities
- internal relocation is possible to avoid persecution/serious harm
- a claim, if refused, is likely or not to be certified as 'clearly unfounded' under section 94 of the Nationality, Immigration and Asylum Act 2002.

Decision makers **must**, however, consider all claims on an individual basis, taking into account each case's specific facts.

Back to Contents

## 1. Material facts, credibility and other checks/referrals

### 1.1 Credibility

1.1.1 For information on assessing credibility, see the instruction on Assessing Credibility and Refugee Status.

1.1.2 Decision makers must also check if there has been a previous application for a UK visa or another form of leave. Asylum applications matched to visas should be investigated prior to the asylum interview (see the Asylum Instruction on Visa Matches, Asylum Claims from UK Visa Applicants).

1.1.3 Decision makers must also consider making an international biometric data-sharing check, when such a check has not already been undertaken (see Biometric data-sharing process (Migration 5 biometric data-sharing process)).

1.1.4 In cases where there are doubts surrounding a person's claimed place of origin, decision makers should also consider language analysis testing, where available (see the Asylum Instruction on Language Analysis).

**Official – sensitive: Not for disclosure – Start of section**

The information in this section has been removed as it is restricted for internal Home Office use.

**Official – sensitive: Not for disclosure – End of section**

Back to Contents

### 1.2 Exclusion

1.2.1 Decision makers must consider whether there are serious reasons to apply

one (or more) of the exclusion clauses. Each case must be considered on its individual facts.

1.2.2 If the person is excluded from the Refugee Convention, they will also be excluded from a grant of humanitarian protection (which has a wider range of exclusions than refugee status).

1.2.3 For guidance on exclusion and restricted leave, see the Asylum Instruction on Exclusion under Articles 1F and 33(2) of the Refugee Convention, Humanitarian Protection and the instruction on Restricted Leave.

**Official – sensitive: Not for disclosure – Start of section**

The information in this section has been removed as it is restricted for internal Home Office use.

**Official – sensitive: Not for disclosure – End of section**

Back to Contents

## 2. Convention reason(s)

2.1.1 Actual or imputed political opinion, race, and/or religion.

2.1.2 Establishing a convention reason is not sufficient to be recognised as a refugee. The question is whether the person has a well-founded fear of persecution on account of an actual or imputed Refugee Convention reason.

2.1.3 For further guidance on the 5 Refugee Convention grounds, see the Asylum Instruction, Assessing Credibility and Refugee Status.

Back to Contents

## 3. Risk

### 3.1 Risk from the state – within Iran

3.1.1 Social media users whose posts are deemed critical of the state or against its high moral standards, or who comment on sensitive issues, may be subject to treatment, including harassment, arrest, ill-treatment, torture and criminal charges, that is sufficiently serious, by its nature or repetition, to amount to persecution.

3.1.2 The Iranian authorities are able to monitor the online activities of persons to varying degrees, depending on the platforms used, and any additional precautions taken by individuals, such as the use of an alias or VPN (virtual private network). Decision makers must be satisfied that the person is able to demonstrate that their online/social media activity has brought them, or will bring them, to the adverse attention of the authorities. Whether a person is at real risk of persecution or serious harm from the state depends on, for example:

- the person's profile
- ethnic origin or religion
- the level and nature of their online activity, and/or

- the size of audience of their online activity

3.1.3 Decision makers should also take into account that the Iranian authorities are likely to intensify their efforts to suppress anti-regime online activities during periods of heightened political tension.

3.1.4 Each case must be considered on its facts with the onus on the person to show that they would be at real risk of serious harm or persecution on account of their actual or perceived political opinion, race or religion.

3.1.5 Iran's constitution and legal framework restricts freedom of expression and freedom online. Penalties for breaching the Computer Crimes Law range from fines and judicial orders, which close organisations and ban people from using electronic communications, to lengthy custodial sentences and the death penalty for crimes committed against public morality and chastity (see Domestic legal framework).

3.1.6 The Iranian authorities have employed various tactics of control over the internet. They have imposed internet shutdowns, filtered content, criminalised the use of circumvention tools, and used financial incentives to lure Iranians onto Iran's national intranet and away from the worldwide web. The Basij Cyber Council, the Cyber Police (FATA), the Cyber Army, the Iranian Revolutionary Guards Corps (IRGC) and its affiliated Centre to Investigate Organised Crimes (CIOC) are known to monitor and track alleged cyberthreats to national security or opposition to the government. This has led to the arrest of online activists who may face charges for vaguely-worded offences such as 'antirevolutionary behavior', 'corruption on earth', 'siding with global arrogance', 'waging war against God' and 'crimes against Islam'. In times of political uncertainty and during outbreaks of protests, Iran increases its monitoring, use of internet shutdowns, and imposes mobile restrictions (see Cyber surveillance in Iran).

3.1.7 President Pezeshkian, who came to power in July 2024, announced an easing of restrictions, starting with the unblocking of popular mobile phone applications. However, no timeframe for the reduction of censorship has been provided and the ability of the Iranian authorities to control online activity remains strong. President Pezeshkian has also said he plans to 'strengthen the governance' of Iran's cyberspace, and the government's prohibition of satellite internet in Iran indicates that it continues to exercise control and restrict the internet for Iranians (see Cyber surveillance in Iran).

3.1.8 Most Iranians, including Iran's top officials, use VPNs and other circumnavigation tools to access blocked websites and apps. A bill that was introduced in 2021 is designed to give the armed forces and security services near total control of the internet, to criminalise the use and distribution of VPNs, further restrict access to global providers, and requires people to register with an ID to access the internet. While the bill is yet to be officially enforced, sources report that unspecified aspects of the bill are already being implemented. Though the sale and purchase of VPNs was already criminalised, in February 2024, the Supreme Council of Cyberspace (SCC) also criminalised the use of VPNs without a license (see Domestic legal framework, Cyber surveillance in Iran, and Social media usage in Iran).

3.1.9 The online sphere is heavily monitored by the state, though there is no

evidence to suggest that Iran operates a mass surveillance programme to monitor the online activity of all its citizens. Persons who repeatedly post content critical of the government may attract adverse attention, especially if the content goes viral. The authorities or its affiliates target social media users using spear phishing campaigns or social engineering tactics (see paragraph 8.4.13 for definitions) to obtain sensitive information, and/or they use malware to infect software. Primary targets of such cyberattacks include NGOs, media organisations, academics, lawyers, political dissidents, activists, and minority groups such as Iranian Kurds, Baluchis and Azeris (see State monitoring of online activity and Use of malware).

3.1.10 The authorities have arrested and detained Iranians for their online activities, and they have used social media content as evidence for criminal charges on various grounds which include 'propaganda against the system', 'spreading lies' and 'insulting the Supreme Leader'. There is little available data available on the number of arrests made for online activities in recent years, however, according to one NGO, 1,315 people were arrested between January 2011 and the end of August 2023 for content they posted on social media (see Arrest, detention and convictions).

3.1.11 Those arrested between early 2023 and early 2025 include prominent activists, social and political figures, celebrities (including social media 'celebrities' and influencers), journalists, editors at independent news outlets, and citizen journalists associated with certain minority religious groups. Many arrests were made for online activities connected with the Woman, Life, Freedom movement (see paragraph 8.1.6 for more information). Charges rarely relate exclusively to virtual activities. Instead, it is reportedly more common for charges to be brought for combinations of different offences and profiles. Those convicted may face harsh sentences, torture and mistreatment in prison. However, it is also reportedly common for online activities to result in social media bans, threats, and intimidation short of imprisonment (see Arrest, detention and convictions).

3.1.12 See also the Country Policy and Information Note on Iran: Kurds and Kurdish political parties.

3.1.13 For further guidance on assessing risk, see the Asylum Instruction on Assessing Credibility and Refugee Status.

Back to Contents

## 3.2 Sur place activities – demonstrations

3.2.1 A person who participates 'sur place' in demonstrations which are deemed critical of the Iranian state may be subject to treatment on return to Iran, including harassment, arrest, ill-treatment, torture and criminal charges, that is sufficiently serious, by its nature or repetition, to amount to persecution.

3.2.2 Whether a person is likely to be at risk on return to Iran will depend on various factors outlined at paragraph 3.2.8, therefore decision makers must undertake a nuanced consideration of those factors for each case.

3.2.3 A person who participates in demonstrations infrequently, who plays no particular role in demonstrations, and whose participation is not highlighted in the media is not at real risk of identification. Such persons are therefore, in

general, unlikely to be subjected to treatment, including harassment, arrest, ill-treatment, torture and criminal charges, that is sufficiently serious, by its nature or repetition, to amount to persecution on return to Iran.

3.2.4 Decision makers should also take into account that the Iranian authorities are likely to intensify their monitoring efforts abroad during periods of heightened political tension in Iran.

3.2.5 Each case must be considered on its facts with the onus on the person to show that they would be at real risk of serious harm or persecution on account of their actual or perceived political opinion, race or religion.

3.2.6 Sources indicate that Iranian intelligence officials or its affiliates monitor and target high profile Iranian dissidents living outside the country, including in the UK. While statistical data is limited, the Metropolitan Police stated it had foiled 15 plots by the Iranian authorities to kidnap or kill UK-based individuals perceived to be enemies of the regime between the start of 2022 and February 2023. The Washington Institute documented 44 plots and attacks, and 14 surveillance events, against Iranian dissidents in the worldwide diaspora between 2023 and 2025 (see Targeting citizens abroad, Monitoring citizens abroad, Sur place activity).

3.2.7 In the Country Guidance case of BA (Demonstrators in Britain – risk on return) Iran CG [2011] UKUT 36 (IAC), heard on 5 and 6 October 2010 and promulgated on 10 February 2011, the Upper Tribunal (UT) held that:

‘Given the large numbers of those who demonstrate here and the publicity which demonstrators receive, for example on Facebook, combined with the inability of the Iranian Government to monitor all returnees who have been involved in demonstrations here, regard must be had to the level of involvement of the individual here as well as any political activity which the individual might have been involved in Iran before seeking asylum in Britain.

‘Iranians returning to Iran are screened on arrival. A returnee who meets the profile of an activist may be detained while searches of documentation are made. Students, particularly those who have known political profiles are likely to be questioned as well as those who have exited illegally.

‘There is not a real risk of persecution for those who have exited Iran illegally or are merely returning from Britain. The conclusions of the Tribunal in the country guidance case of SB (risk on return - illegal exit) Iran CG [2009] UKAIT 00053 are followed and endorsed.

‘There is no evidence of the use of facial recognition technology at the Imam Khomeini International airport, but there are a number of officials who may be able to recognize up to 200 faces at any one time. The procedures used by security at the airport are haphazard. It is therefore possible that those whom the regime might wish to question would not come to the attention of the regime on arrival. If, however, information is known about their activities abroad, they might well be picked up for questioning and/or transferred to a special court near the airport in Tehran after they have returned home.

‘It is important to consider the level of political involvement before considering the likelihood of the individual coming to the attention of the authorities and the priority that the Iranian regime would give to tracing him.

It is only after considering those factors that the issue of whether or not there is a real risk of his facing persecution on return can be assessed' (headnotes 1 to 3).

3.2.8 The UT in BA also held that:

'The following are relevant factors to be considered when assessing risk on return having regard to sur place activities:

'(i) Nature of sur place activity

- 'Theme of demonstrations – what do the demonstrators want (e.g. reform of the regime through to its violent overthrow); how will they be characterised by the regime?
- 'Role in demonstrations and political profile – can the person be described as a leader; mobiliser (e.g. addressing the crowd), organiser (e.g. leading the chanting); or simply a member of the crowd; if the latter is he active or passive (e.g. does he carry a banner); what is his motive, and is this relevant to the profile he will have in the eyes of the regime?
- 'Extent of participation – has the person attended one or two demonstrations or is he a regular participant?
- 'Publicity attracted – has a demonstration attracted media coverage in the United Kingdom or the home country; nature of that publicity (quality of images; outlets where stories appear etc)?

'(ii) Identification risk

- 'Surveillance of demonstrators – assuming the regime aims to identify demonstrators against it, how does it do so, through filming them, having agents who mingle in the crowd, reviewing images/recordings of demonstrations etc?
- 'Regime's capacity to identify individuals – does the regime have advanced technology (e.g. for facial recognition); does it allocate human resources to fit names to faces in the crowd?

'(iii) Factors triggering inquiry/action on return

- 'Profile – is the person known as a committed opponent or someone with a significant political profile; does he fall within a category which the regime regards as especially objectionable?
- 'Immigration history – how did the person leave the country (illegally; type of visa); where has the person been when abroad; is the timing and method of return more likely to lead to inquiry and/or being detained for more than a short period and ill-treated (overstayer; forced return)?

'(iv) Consequences of identification

- 'Is there differentiation between demonstrators depending on the level of their political profile adverse to the regime?

'(v) Identification risk on return

- ‘Matching identification to person – if a person is identified is that information systematically stored and used; are border posts geared to the task?’ (headnote 4).

3.2.9 The UT in BA also held that: ‘While it may well be that an appellant’s participation in demonstrations is opportunistic, the evidence suggests that this is not likely to be a major influence on the perception of the regime.’ (paragraph 65).

3.2.10 The UT in BA additionally held that: ‘… [F]or the infrequent demonstrator who plays no particular role in demonstrations and whose participation is not highlighted in the media there is not a real risk of identification and therefore not a real risk of consequent ill-treatment, on return.’ (paragraph 66).

3.2.11 In the Court of Appeal case of S v Secretary of State for the Home Department [2024] EWCA Civ 1482, heard on 27 November 2024 and promulgated on 6 December 2024, the Court of Appeal considered whether it was necessary for the Upper Tribunal (UT) to have considered whether the Appellant in S, whose political activities in the UK (demonstrations and Facebook posts) were accepted as opportunistic and not based on genuinely held beliefs, would disclose, or would have to disclose, any of his sur place activities given the likelihood of him being interviewed on return to Iran. It was argued on behalf of the Appellant in S that the UT ought to have considered the type of issues which Lord Dyson mentioned in the case of RT (Zimbabwe) v SSHD [2012] 1AC 152, (“RT”) (paragraph 57) before being properly able to reach a view as to the risk to the appellant on his return to Iran. In particular, it was argued on behalf of S that the UT ought to have considered what the Appellant might be asked by the authorities on his return to Iran and how well he would be able to lie to them. The Court of Appeal held that:

‘… [A]s was pointed out in XX at (98), the issues which the Supreme Court were considering in RT, arose in a very different context, namely the return of a non-political Zimbabwean to an area in which it was likely that he would have to provide a convincingly false account of his allegiance to the ruling party when stopped and questioned by ill-disciplined militia at roadblocks.

‘In contrast, as was pointed out in XX at (99) the Iranian authorities do not persecute individuals because of their political neutrality. Moreover, in the present case, and in the light of both the retained findings and those made by [UT] Judge Kebede as to the unlikelihood of the appellant having already come to the attention of the authorities and his lack of genuine political belief in the PJAK, the appellant was not in a position where he would have to prove his political loyalty, rather it would be one in which, as Judge Kebede found, the appellant would not be required to volunteer information about his activities in the UK.

‘… In my judgment … these finding[s] were ones which the [UT] judge was entitled to find on the basis of the evidence before her, and were reached in accordance with the relevant country guidance.’ (paragraphs 55 to 57).

3.2.12 The country information in this note does not indicate that there are ‘very strong grounds supported by cogent evidence’ to justify a departure from these findings.

3.2.13 See also the Country Policy and Information Note on Iran: Kurds and Kurdish political parties.

3.2.14 For further guidance on assessing risk, see the Asylum Instruction on Assessing Credibility and Refugee Status.

Back to Contents

## 3.3 Sur place activities – online

3.3.1 A person who is 'sur place' openly critical of the Iranian regime online may be subject to treatment on return to Iran, including harassment, arrest, ill-treatment, torture and criminal charges, that is sufficiently serious, by its nature or repetition, to amount to persecution.

3.3.2 Whether a person is likely to be at risk on return to Iran will depend on various factors outlined at paragraphs 3.3.7 to 3.3.15, therefore decision makers must undertake a nuanced consideration of those factors for each case. Decision makers must have particular regard to paragraphs 3.3.10 to 3.3.12 and 3.3.15 when considering a case for a person of Kurdish ethnicity.

3.3.3 Decision makers should also take into account that the Iranian authorities are likely to intensify their monitoring efforts abroad during periods of heightened political tension in Iran.

3.3.4 Each case must be considered on its facts with the onus on the person to show that they would be at real risk of serious harm or persecution on account of their actual or perceived political opinion, race or religion.

3.3.5 Between 2023 and 2024 there have been reported incidents of journalists and well-known online activists abroad having been targeted by cyberattacks, threatened (including threats made against family inside Iran), convicted in absentia, and, in one case, given a death sentence in 2023 for "corruption on Earth" (having been arrested while transiting the UAE several years prior). Those who maintain a low online profile and have not attracted adverse attention from the authorities are unlikely to be systematically monitored online, however, the monitoring of online dissidents abroad is likely to intensify during times of political tension inside Iran. Whilst the Iranian state is able to access and monitor user data by using malware and spear-phishing in the diaspora, the extent to which authorities can monitor the content of foreign social media platforms remains unclear (see Targeting citizens abroad, Monitoring citizens abroad, and Monitoring online activity abroad).

3.3.6 In the country guidance case XX (PJAK – sur place activities - Facebook) Iran CG [2022] UKUT 23 (IAC), heard 8 to 10 June 2021 and promulgated on 20 January 2022, the Upper Tribunal (UT) held that:

'The cases of BA (Demonstrators in Britain – risk on return) Iran CG [2011] UKUT 36 (IAC); SSH and HR (illegal exit: failed asylum seeker) Iran CG [2016] UKUT 00308 (IAC); and HB (Kurds) Iran CG [2018] UKUT 00430 continue accurately to reflect the situation for returnees to Iran. That guidance is hereby supplemented on the issue of risk on return arising from a person's social media use (in particular, Facebook) and surveillance of that person by the authorities in Iran' (paragraph 120).

3.3.7 Regarding surveillance by the Iranian authorities, in XX the UT held that:

- ‘Surveillance

‘There is a disparity between, on the one hand, the Iranian state’s claims as to what it has been, or is, able to do to control or access the electronic data of its citizens who are in Iran or outside it; and on the other, its actual capabilities and extent of its actions. There is a stark gap in the evidence, beyond assertions by the Iranian government that Facebook accounts have been hacked and are being monitored. The evidence fails to show it is reasonably likely that the Iranian authorities are able to monitor, on a large scale, Facebook accounts. More focussed, ad hoc searches will necessarily be more labour-intensive and are therefore confined to individuals who are of significant adverse interest. The risk that an individual is targeted will be a nuanced one. Whose Facebook accounts will be targeted, before they are deleted, will depend on a person’s existing profile and where they fit onto a “social graph;” and the extent to which they or their social network may have their Facebook material accessed.

‘The likelihood of Facebook material being available to the Iranian authorities is affected by whether the person is or has been at any material time a person of significant interest, because if so, they are, in general, reasonably likely to have been the subject of targeted Facebook surveillance. In the case of such a person, this would mean that any additional risks that have arisen by creating a Facebook account containing material critical of, or otherwise inimical to, the Iranian authorities would not be mitigated by the closure of that account, as there is a real risk that the person would already have been the subject of targeted on-line surveillance, which is likely to have made the material known.

‘Where an Iranian national of any age returns to Iran, the fact of them not having a Facebook account, or having deleted an account, will not as such raise suspicions or concerns on the part of Iranian authorities.

‘A returnee from the UK to Iran who requires a laissez-passer or an emergency travel document (ETD) needs to complete an application form and submit it to the Iranian embassy in London. They are required to provide their address and telephone number, but not an email address or details of a social media account. While social media details are not asked for, the point of applying for an ETD is likely to be the first potential “pinch point,” referred to in AB and Others (internet activity - state of evidence) Iran [2015] UKUT 257 (IAC). It is not realistic to assume that internet searches will not be carried out until a person’s arrival in Iran. Those applicants for ETDs provide an obvious pool of people, in respect of whom basic searches (such as open internet searches) are likely to be carried out’ (paragraphs 121 to 124).

3.3.8 Regarding Facebook and social media evidence generally, the UT in XX held that:

- ‘Guidance on Facebook more generally

‘There are several barriers to monitoring, as opposed to ad hoc searches of someone’s Facebook material. There is no evidence before us that the Facebook website itself has been “hacked,” whether by the Iranian or any other government. The effectiveness of website “crawler” software, such as Google, is limited, when interacting with Facebook. Someone’s name and

some details may crop up on a Google search, if they still have a live Facebook account, or one that has only very recently been closed; and provided that their Facebook settings or those of their friends or groups with whom they have interactions, have public settings. Without the person's password, those seeking to monitor Facebook accounts cannot "scrape" them in the same unautomated way as other websites allow automated data extraction. A person's email account or computer may be compromised, but it does not necessarily follow that their Facebook password account has been accessed.

'The timely closure of an account neutralises the risk consequential on having had a "critical" Facebook account, provided that someone's Facebook account was not specifically monitored prior to closure (paragraphs 125 to 126).

- 'Guidance on social media evidence generally

'Social media evidence is often limited to production of printed photographs, without full disclosure in electronic format. Production of a small part of a Facebook or social media account, for example, photocopied photographs, may be of very limited evidential value in a protection claim, when such a wealth of wider information, including a person's locations of access to Facebook and full timeline of social media activities, readily available on the "Download Your Information" function of Facebook in a matter of moments, has not been disclosed.

'It is easy for an apparent printout or electronic excerpt of an internet page to be manipulated by changing the page source data. For the same reason, where a decision maker does not have access to an actual account, purported printouts from such an account may also have very limited evidential value.

'In deciding the issue of risk on return involving a Facebook account, a decision maker may legitimately consider whether a person will close a Facebook account and not volunteer the fact of a previously closed Facebook account, prior to application for an ETD: HJ (Iran) v SSHD [2011] AC 596. Decision makers are allowed to consider first, what a person will do to mitigate a risk of persecution, and second, the reason for their actions. It is difficult to see circumstances in which the deletion of a Facebook account could equate to persecution, as there is no fundamental right protected by the Refugee Convention to have access to a particular social media platform, as opposed to the right to political neutrality. Whether such an inquiry is too speculative needs to be considered on a case-by-case basis.' (paragraphs 127 to 129).

3.3.9 The UT in XX also found that:

'The evidence about Facebook account closure is unequivocal. It may be reversed before 30 days, but not after that time, and after deletion, the data on the person's Facebook account is irretrievable, even if their password is later discovered. The only exceptions to this are two limited pieces of residual data - limited caches of data, for a temporary period, on internet search engines; and photographs (but not links) on other people's Facebook accounts and messages sent to other people. Facebook account closure

causes the data to be wholly inaccessible through or from Facebook or the user. However, if the data has been exported by a third party, that third party will continue to have access to the exported data, as stored' (paragraph 84).

3.3.10 The UT in XX acknowledged that, '… the Iranian state targets dissident groups, including religious and ethnic minorities, such as those of Kurdish ethnic origin' (paragraph 85).

3.3.11 In respect of the finding that a person of significant interest is, in general, reasonably likely to have been the subject of targeted Facebook surveillance, the UT in XX added:

'We refer to the level of political involvement of an individual, as in BA and HB; and the nature of "real-world" sur place activity, which would prompt such surveillance. By way of summary, relevant factors include: the theme of any demonstrations attended, for example, Kurdish political activism; the person's role in demonstrations and political profile; the extent of their participation (including regularity of attendance); the publicity which a demonstration attracts; the likelihood of surveillance of particular demonstrations; and whether the person is a committed opponent' (paragraph 92).

3.3.12 In XX the UT also found, 'Discovery of material critical of the Iranian regime on Facebook, even if contrived, may make a material difference to the risk faced by someone returning to Iran. The extent of the risk they may face will continue to be fact sensitive. For example, an Iranian person of Kurdish ethnic origin may face a higher risk than the wider population' (para 103).

3.3.13 In the 2015 reported case of AB and Others the UT also referenced to the opportunistic use of material deemed critical of the Iranian regime. It held:

'We do not find it at all relevant if a person had used the internet in an opportunistic way. We are aware of examples in some countries where there is clear evidence that the authorities are scornful of people who try to create a claim by being rude overseas. There is no evidence remotely similar to that in this case. The touchiness of the Iranian authorities does not seem to be in the least concerned with the motives of the person making a claim but if it is interested it makes the situation worse, not better because seeking asylum is being rude about the government of Iran and whilst that may not of itself be sufficient to lead to persecution it is a point in that direction' (paragraph 464).

3.3.14 The UT also went on to say:

'It is very difficult to establish any kind of clear picture about the risks consequent on blogging activities in Iran. Very few people seem to be returned unwillingly and this makes it very difficult to predict with any degree of confidence what fate, if any, awaits them. Some monitoring of activities outside Iran is possible and it occurs. It is not possible to determine what circumstances, if any, enhance or dilute the risk although a high degree of activity is not necessary to attract persecution' (paragraph 466).

3.3.15 The factors cited in XX, that is, Kurdish political activism and persons of Kurdish ethnic origin (paragraphs 92 and 103), and in AB and Others regarding the opportunistic use of material critical of the Iranian regime (paragraph 464), should be taken into account when assessing risk of

directed Facebook surveillance against a person of Kurdish ethnic origin, in view of the findings in HB, in that:

'Even "low-level" political activity, or activity that is perceived to be political, such as, by way of example only, mere possession of leaflets espousing or supporting Kurdish rights, if discovered, involves the same risk of persecution or Article 3 ill-treatment. Each case, however, depends on its own facts and an assessment will need to be made as to the nature of the material possessed and how it would be likely to be viewed by the Iranian authorities in the context of the foregoing guidance' (paragraph 98 (9)).

3.3.16 Also pointed out in the case of XX, and upheld in the Court of Appeal case of S, the Iranian authorities do not persecute individuals because of their political neutrality. The Court of Appeal found in S that where a person has carried out sur-place activities for reason(s) other than a genuinely held political belief, and where it is unlikely that the person has already come to the attention of the Iranian authorities, the person, on return to Iran, would not be required to volunteer information about their activities in the UK (see paragraph 3.2.7).

3.3.17 The Court of Appeal in S also held that: '… [T]here was no reason why the appellant could not close his Facebook accounts prior to the first pinch-point, when he applied for his emergency travel document, nor why he should disclose the existence of them, which would not have previously been known to the authorities, as like his attendance at demonstrations, their apparent contents did not reflect any genuinely held belief by the appellant …' (paragraph 49).

3.3.18 The country information in this note does not indicate that there are 'very strong grounds supported by cogent evidence' to justify a departure from these findings.

3.3.19 See also the Country Policy and Information Note on Iran: Kurds and Kurdish political parties.

3.3.20 For further guidance on assessing risk, see the Asylum Instruction on Assessing Credibility and Refugee Status.

Back to Contents

## 4. Protection

4.1.1 Where the person has a well-founded fear of persecution or serious harm from the state, they will not, in general, be able to obtain protection.

4.1.2 For further guidance on assessing state protection, see the Asylum Instruction on Assessing Credibility and Refugee Status Assessing Credibility and Refugee Status.

Back to Contents

## 5. Internal relocation

5.1.1 Where the person has a well-founded fear of persecution or serious harm from the state, they will not, in general, be able to internally relocate to escape that risk.

5.1.2 For further guidance on considering internal relocation and factors to be

taken into account see the Asylum Instruction on Assessing Credibility and Refugee Status.

Back to Contents

## 6. Certification

6.1.1 Where a claim is refused, it is unlikely to be certifiable as 'clearly unfounded' under section 94 of the Nationality, Immigration and Asylum Act 2002.

6.1.2 For further guidance on certification, see Certification of Protection and Human Rights claims under section 94 of the Nationality, Immigration and Asylum Act 2002 (clearly unfounded claims).

Back to Contents

# Country information

## About the country information

This section contains publicly available or disclosable country of origin information (COI) which has been gathered, collated and analysed in line with the research methodology. It provides the evidence base for the assessment.

The structure and content follow a terms of reference which sets out the general and specific topics relevant to the scope of this note.

This document is intended to be comprehensive but not exhaustive. If a particular event, person or organisation is not mentioned this does not mean that the event did or did not take place or that the person or organisation does or does not exist.

The COI included was published or made publicly available on or before **28 February 2025**. Any event taking place or report published after this date will not be included.

Decision makers must use relevant COI as the evidential basis for decisions.

Back to Contents

## 7. Domestic legal framework

7.1.1 The Iran Data Portal, an online portal which hosts social science data on Iran in both English and Persian[1], published an English translation of the The Constitution of the Islamic Republic of Iran. It stated: 'Article 24 (Freedom of the Press): Publications and the press have freedom of expression except when it is detrimental to the fundamental principles of Islam or the rights of the public. The details of this exception will be specified by law.'[2]

7.1.2 On 25 March 2016, the Iran Human Rights Documentation Center (IHRDC), an independent, non-profit organisation that documents and promotes accountability for human rights abuses in Iran[3], published a report entitled 'Restrictions on Freedom of Expression in the Islamic Republic of Iran'. The report, which cited various sources, stated:

'Over the years what can be considered "detrimental to the fundamental principles of Islam" has been defined very broadly, and it has even included various expressions of Islamic belief.

'The Press Law, last amended in 2009, expands the constitution's constraint on freedom of expression. Publishing atheistic articles or content that is prejudicial to Islamic codes, propagating luxury and extravagance, insulting Islam and its sanctities, offending senior Islamic jurists, quoting articles from the "deviant press, parties and groups which oppose Islam," and publishing statements against the Constitution are among actions expressly prohibited by Article 6 of this law.'[4]

7.1.3 In 2012, a London-based international organisation called Article 19, which advocates for the right to freedom of expression globally[5], published a report

[1] Iran Data Portal, About Us, no date
[2] Iran Data Portal, The Constitution … (pages 10 to 11), 2/3 December 1979, amended 28 July 1989
[3] IHRDC, Mission, undated
[4] IHRDC, Restrictions on Freedom of Expression in… Iran (paragraph 4.2), 25 March 2016
[5] Article 19, About us, no date

entitled 'Islamic Republic of Iran: Computer Crimes Law' (CCL report). The report, which cited various sources, stated:

'The Press Law of 1986, as amended in 2000, extends broad content-based restrictions from the traditional media to electronic and Internet-based modes of expression … [T]he Iranian Government has asserted that the Press Law applies to all internet-based publications …

'Although the law contains guarantees against censure and government control, it limits the role of the press to "constructive criticism" based on "logic and reason and void of insult, humiliation and detrimental effects." Reports may only be published in pursuit of one of five "legitimate objectives" including "to campaign against manifestations of imperialistic culture…and to propagate and promote genuine Islamic culture and sound ethical principles." Again, these normative objectives are ambiguous are [sic] therefore vulnerable to manipulation by law enforcement authorities.'[6]

7.1.4 The same source stated:

'The Penal Code of Iran contains a range of restrictions on expression that apply as the general law alternative to the Press Law of 1986. Authorities have tended towards use of the Penal Code rather than the Press Law because it does not require open trials in the presence of the jury.

'The Penal Code contains a range of expression-related offenses that carry excessive penalties. These include capital punishment or up to five years imprisonment for insulting religion, up to seventy-four lashes or two years imprisonment for creating anxiety and unease in the public's mind, spreading false rumours, or writing about acts which are not true. The Penal Code also criminalises insulting the Supreme Leader, insulting any of the leaders of the three branches of government, and satirising another person.

'The Computer Crimes Law [adopted in Iran in 2009 or 2010[7]] replicates many of these content-based penal provisions so that their application to electronic and Internet-based communications is beyond doubt.'[8]

7.1.5 The Article 19 CCL report also went on to state:

'The Computer Crimes Law is saturated with provisions that criminalise legitimate expression. Crimes against "public morality and chastity" and the "dissemination of lies" are engineered to ensnare all forms of legitimate expression. These include broad criminal defamation and obscenity provisions …

'… The Computer Crimes Law mandates severe sentences that penalise legitimate expression … [including] the availability of the death penalty for crimes committed against public morality and chastity. Other sanctions on legitimate expression include lengthy custodial sentences, draconian fines, and judicial orders to close organisations and ban individuals from using electronic communications. These penalties also apply to Internet Service Providers that fail to enforce content-based restrictions, incentivising the private sector to promulgate Iran's censorship culture.

[6] Article 19, Islamic Republic of Iran: Computer Crimes Law (page 18), 2012
[7] Article 19, Islamic Republic of Iran: Computer Crimes Law (page 6), 2012
[8] Article 19, Islamic Republic of Iran: Computer Crimes Law (pages 18 to 19), 2012

'… [T]he law contains no guarantee for the right to freedom of expression or access to information.'[9]

7.1.6 On 22 April 2024, the USSD published its '2023 Country Reports on Human Rights Practices' (USSD 2023 Country Report), which stated:

'The government often charged political dissidents with vague crimes, some of which carried the death penalty, such as "antirevolutionary behavior," "corruption on earth," "siding with global arrogance," "waging war against God," and "crimes against Islam." Prosecutors sought strict penalties against government critics for minor violations.

'The political crimes law defined a "political crime" as "propaganda" or "insult" against the ruling establishment, or acts committed with "the intent to reform the domestic or foreign policies of Iran," while those with the intent to "damage the foundations of the ruling establishment" were considered national security crimes. Insulting or defaming government officials, visiting heads of state, or political representatives were considered political crimes. Courts and the Public Prosecutor's Office retained responsibility for determining the nature of the crime.'[10]

7.1.7 An article published on 23 February 2022 by The Iran Primer, which provides a collection of essays by 50 of the world's top scholars on Iran and was launched by the United States Institute of Peace with the Woodrow Wilson International Center for Scholars[11], stated:

'In July 2021, Parliament introduced a new bill that could further limit public access. The legislation is called "Cyberspace Users Rights Protection and Regulation of Key Online Services." [more widely known as the "User Protection Bill"[12]] … The bill would essentially place Iran's Internet gateways in the hands of the armed forces; make it illegal to use virtual private networks (VPNs); and potentially criminalize those who use and distribute VPNs (although the language on the legal repercussions in the latest draft are still quite vague).'[13]

7.1.8 Also reporting on the new bill, the Committee to Protect Journalists (CPJ), a New York-based independent, nonprofit organisation that promotes press freedom worldwide[14], stated that it would, '… require people to register their ID to access the internet …', adding that, according to media reports, it was due to be ratified in early 2022[15].

7.1.9 Freedom House published a report entitled 'Freedom on the Net 2024' on 16 October 2024 (Freedom on the Net report). The report, which covered the period from 1 June 2023 to 31 May 2024, and cited various sources, also covered the new bill, stating: 'The IUPB [Internet User Protection Bill] requires foreign and domestic online platforms to register with a supervisory board and comply with Iranian laws or face penalties … It also requires that

[9] Article 19, Islamic Republic of Iran: Computer Crimes Law (pages 3 and 20), 2012
[10] USSD, 2023 Country Reports on Human Rights Practices (pages 19 to 20), 22 April 2024
[11] TWI, The Iran Primer: Power, Politics, and US Policy, 3 June 2013
[12] HRC, Detailed findings of … mission (paragraph 1135), 19 March 2024, updated 8 July 2024
[13] The Iran Primer, New "Protection" Bill on Internet Freedom, 23 February 2022
[14] CPJ, What We Do, no date
[15] CPJ, Iran's parliament moves forward with troubling bill to further restrict internet, 1 November 2021

foreign companies open offices within Iran.'[16]

7.1.10 On 23 July 2024, Article 19 published a report entitled 'Tightening the Net: Iran's new phase of digital repression' (the Tightening the Net report) which stated: 'While the [User Protection] Bill has yet to be passed by parliament or officially enforced, its main pillars have been quietly implemented.'[17] The report did not specify which aspects of the User Protection Bill it considered have been implemented.

7.1.11 On 13 December 2024, the UN Human Rights Office of the High Commissioner (OHCHR) published a press release which stated:

'Today, the Law on Protecting the Family through the Promotion of the Culture of Chastity and Hijab is reportedly set to come into force. It provides for the punishment of those aged 12 and above who fail to wear a hijab online … [T]he new law introduces more hefty fines and longer prison sentences of up to 15 years. It also allows for the possibility for judges to apply the death penalty under the offense of "corruption on earth" …

'"… [T]he severe economic punishments are likely to disproportionately impact vulnerable populations and groups, including … social media users," the [UN] experts said.'[18]

7.1.12 On 17 December 2024, an Amnesty International article about the new Chastity and Hijab law was updated to state: 'On 14 December 2024, state media reported that the promulgation of the law has been temporarily paused.'[19]

7.1.13 For more information about the punishments provided for under the new Chastity and Hijab law, see the Amnesty International article.

Back to Contents

## 8. Cyber surveillance in Iran

### 8.1 State control of online activity

8.1.1 A 12 January 2018 US Department of the Treasury press release stated: 'The Supreme Council of Cyberspace was created in 2012 by Iran's Supreme Leader to centralize and oversee the Iranian regime's Internet policymaking and regulation. Since its creation, and for the purported purpose of "protecting the country from negative content of cyberspace," the Supreme Council of Cyberspace has continued the Iranian regime's blocking of many social media sites and other Internet censorship efforts.'[20]

8.1.2 The USSD 2023 Country Report stated: 'The government restricted and disrupted access to the internet and censored online content … The Ministry of Culture and Islamic Guidance and the Ministry of Information and Communications Technology were the main regulatory bodies for content and internet systems, and they maintained monopoly control over internet

[16] Freedom House, Freedom on the Net 2024 (section B6), 16 October 2024
[17] Article 19, Tightening the Net: Iran's new phase of digital repression (page 5), 23 July 2024
[18] OHCHR, Iran: UN experts call for Hijab and Chastity law to be repealed, 13 December 2024
[19] Amnesty International, … New … veiling law …, 10 December 2024, updated 17 December 2024
[20] US Department of the Treasury, Treasury Sanctions Individuals and Entities …, 12 January 2018

traffic flowing in and out of the country.'[21]

8.1.3 The Tightening the Net report stated: 'The ethos of the [User Protection] Bill [see paragraphs 7.1.7 to 7.1.10 has led to aggressive forms of censorship, introducing filtering of practically all platforms and applications that are already not under the influence of the state … [and] an aggressive attack to disable and potentially criminalise circumvention tools. Underlying all these efforts is Iran's goal to consolidate all facets of internet use into the hands of the government and even the military.'[22]

8.1.4 On 15 May 2024, Access Now, an organisation that works to extend the digital rights of people internationally[23], published a report entitled 'Shrinking democracy, growing violence: internet shutdowns in 2023'. The report, which cited various sources, stated: 'Iranian authorities use a range of methods to interfere with internet access, silence people, and stifle dissent, from shutting down the global internet to force people onto the highly censored national intranet [the National Information Network (NIN), see paragraphs 8.1.8 to 8.1.9], to restricting mobile access and messaging platforms. In 2023, this authoritarian approach reached its peak during protests and crackdowns of ethnic minorities …'[24]

8.1.5 The Access Now report also ranked Iran the third highest, globally, for documented internet shutdowns in 2023[25], with 34 recorded shutdowns, an increase from 19 in 2022[26] (see paragraph 8.1.13 for 2024 data).

8.1.6 On 19 March 2024, the UN Human Rights Council (HRC) published detailed findings of its Iran fact-finding mission (HRC detailed findings report). The fact-finding mission was mandated 'to investigate alleged human rights violations in the Islamic Republic of Iran "related to the protests that began on 16 September 2022"'[27], which became known as the "Woman, Life, Freedom" movement (in response to the death of Mahsa Amini, a young Kurdish woman, in police custody for "improper hijab"[28] [29]). Carried out between the publication of its terms of reference, in July 2023[30], and the publication of its summary report on 2 February 2024 (see paragraph 8.6.1), the mission did not involve a visit to Iran[31] but was based on information from a variety of primary sources, including in-depth interviews with victims and eyewitnesses, as well as information from secondary and open sources[32]. The detailed findings report, which was updated on 8 July 2024, and cited various sources, stated:

'According to reliable information on data connectivity reviewed by the Mission, there has been no blanket Internet shutdown in the entire country in

[21] USSD, 2023 Country Reports on Human Rights Practices (pages 42 to 43), 22 April 2024
[22] Article 19, Tightening the Net: Iran's new phase of digital repression (page 5), 23 July 2024
[23] Access Now, About Us, no date
[24] Access Now, … [I]nternet shutdowns in 2023 (pages 46 to 47), 15 May 2024
[25] Access Now, … [I]nternet shutdowns in 2023 (page 6), 15 May 2024
[26] Access Now, … [I]nternet shutdowns in 2023 (page 46), 15 May 2024
[27] HRC, Detailed findings of … mission (paragraph 16), 19 March 2024, updated 8 July 2024
[28] Reuters, Iran steps up internet crackdown one year after Mahsa Amini death, 14 September 2023
[29] BBC News, Iran: A really simple guide to the protests, 15 September 2023
[30] HRC, Detailed findings of … mission (paragraph 11), 19 March 2024, updated 8 July 2024
[31] HRC, Detailed findings of … mission (paragraph 22), 19 March 2024, updated 8 July 2024
[32] HRC, Detailed findings of … mission (paragraphs 31 to 33), 19 March 2024, updated 8 July 2024

connection with the protests that began on 16 September 2022, either on the day or since. Instead, however, and as acknowledged by the Government, the authorities have implemented targeted shutdowns … This being said, the shutdowns affected vast parts of the territory of the country and at key times connectivity was reduced at the same time in several provinces where protests were ongoing … [D]isruptions could and did last from four hours to several days, including eight days. Disruptions lasted longer than individual protests in specific locations. Internet connectivity was not reinstated until the protests had receded.'[33]

8.1.7 On 20 February 2024, IranWire, an Iranian news website[34], published an article entitled 'Iranian Authorities Escalate Crackdown on VPNs' which stated: 'The Iranian Supreme Council of Cyberspace has criminalized the use of … VPNs … without a legal license, marking a significant escalation in restrictions on online access … The purchase and sale of VPNs were previously made illegal … Mojtahedzadeh [Ali, a legal expert] argued that the council oversteps its mandate and "criminalizes 80 million Iranians," including "top officials" who may rely on VPNs to access the internet.'[35]

8.1.8 An article published by the American Iranian Council (AIC), an educational organisation that provides research and policy analysis with the goal of improving US-Iran relations[36], which was updated in January 2025, stated:

'During his campaign, current president Masoud Pezeshkian [elected on 5 July 2024[37]] declared, "I will make every effort to reform the ineffective filtering system ... We must free the internet." He promised, "I will stand against filtering.["] … However … the government's ability to censor information and repress unfavorable news coverage remains strong and may have strengthened in recent years … The government has also sought to increase its control over Internet use by establishing its own intranet service: the National Information Network (NIN).'[38]

8.1.9 In June 2024, Friedrich-Ebert-Stiftung (FES), a German political foundation that focuses on social democracy values[39], published a report by the Miaan Group, a Texas-based group that advocates for human rights in Iran[40], on state control over internet access and usage during the Woman, Life, Freedom protests. The report (the June 2024 Miaan Group), which cited various sources, noted that '… the [Information and Communications Technology] ICT Ministry aims to connect 20 million households to the NIN … by 2026 …'[41]

8.1.10 On 14 November 2024, the Iranian Students' News Agency (ISNA), a 'Persian-language news organization run by Iranian university students'[42], published an article which stated: '… [T]he President said: "The

[33] HRC, Detailed findings … mission (paragraphs 1144 to 1148), 19 March 2024, updated 8 July 2024
[34] IranWire, About IranWire, no date
[35] IranWire, Iranian Authorities Escalate Crackdown on VPNs, 20 February 2024
[36] AIC, History, no date
[37] BBC News, Reformist … Pezeshkian elected Iran's president, 5 July 2024, updated 6 July 2024
[38] AIC, Myth vs. Fact: Censorship in Iran, updated 30 January 2025
[39] Ecoi.net, Friedrich-Ebert-Stiftung (FES), updated 1 December 2021
[40] Reuters, Iran steps up internet crackdown one year after Mahsa Amini death, 14 September 2023
[41] Miaan Group, … Iran's Progress in Censorship and Surveillance … (page 4), June 2024
[42] Worldcrunch, ISNA, no date

government's plan to remove filtering does not mean abandoning cyberspace, but will develop and strengthen governance and the optimal use of it by the people."'[43]

N.B. the ISNA information quoted above was originally published in Persian. All COI from this source has been translated using a free online translation tool. As such 100% accuracy cannot be guaranteed.

8.1.11 On 25 December 2024, Iran News Update (INU), an Iranian news website which describes itself as a 'counterweight to the state-run censorship in Iran'[44], published an article entitled 'Iran's Regime Eases Internet Restrictions Amid Mounting Crises'. The article stated:

'On Tuesday [24 December 2024], Iran's [Supreme Council of Cyberspace] … approved the lifting of blocks on "certain widely used foreign platforms," according to the state-run Islamic Republic News Agency (IRNA). WhatsApp and Google Play were named as the first applications to be unblocked.

'… While the exact timeline for implementing the decision remains unclear, IRNA reported that it was unanimously approved during a council meeting attended by the head of the judiciary and regime's President Masoud Pezeshkian …

'… The Iranian regime's announcement marks the start of what officials describe as a "multi-staged process" to reduce internet censorship. IRNA emphasized that the easing of restrictions "won't be limited to the removal of blocks on one or a few platforms." However, skepticism remains high, given the regime's history of suppressing online freedoms during periods of unrest.

'This move may be an attempt to placate public anger while avoiding broader structural reforms. Whether it signals a genuine shift in the regime's policy or a tactical concession to buy time amid growing pressures remains to be seen.'[45]

8.1.12 On 6 January 2025, Iran International, a London-based media outlet that provides news for Iranians both in and outside of Iran[46], published an article which stated: 'Starlink is prohibited … Iran's government has lobbied the International Telecommunication Union (ITU) to exclude the country from satellite internet coverage … The expanding reach of Starlink [a reported 20-fold increase in 2024 usage, to more than 100,000 estimated users[47]] represents a shift in Iran's internet landscape, offering a lifeline for those seeking unrestricted online access amidst heightened governmental control and censorship.'[48]

8.1.13 On 23 February 2025 Access Now published a report entitled 'Lives on hold: internet shutdowns in 2024' which ranked Iran joint 12th, globally, for documented internet shutdowns in 2024, with 3 recorded shutdowns[49] (see paragraph 8.1.5 for 2022 and 2023 data).

[43] ISNA, The government's plan to remove filtering …, 14 November 2024
[44] INU, About Us, 25 April 2013
[45] INU, Iran's Regime Eases Internet Restrictions Amid Mounting Crises, 25 December 2024
[46] Iran International, About Us, no date
[47] Iran International, 100,000 Iranians use Starlink …, 6 January 2025, updated 7 January 2025
[48] Iran International, 100,000 Iranians use Starlink …, 6 January 2025, updated 7 January 2025
[49] Access Now, Lives on hold: internet shutdowns in 2024 (page 6), 23 February 2025

8.1.14 For a graphic showing an outline of the responsibilities of internet stakeholders in Iran (based on its approved laws), see page 6 of a Tehran E-commerce Association report entitled 'Quality of Internet in Iran'. The report was translated into English and published on 18 July 2024 by Project Ainita, an Iran-focused project for online anonymity, security and freedom[50].

Back to Contents

## 8.2 Cyber police (FATA)

8.2.1 A joint report on Iran's criminal procedures based on a range of sources, dated December 2021, by the Norwegian Country of Origin Information Centre (Landinfo), the Office of the Commissioner General for Refugees and Stateless Persons (CGRS – Belgium) and the Swiss State Secretariat for Migration (SEM), noted:

'The Iranian Cyberspace Police, literally "police of the virtual space and information exchange" … commonly referred to by its acronym FATA was created in 2011. FATA is tasked with combating cybercrimes, such as financial scams and violations of privacy, as well as suppressing any form of online criticism perceived as propaganda against the state (political, religious, or otherwise). It is also involved in monitoring, tracking, intimidating, and arresting online activists, especially bloggers and those active on social media. Its responsibilities also include targeting those who create and sell virtual private network (VPN) accesses. Their responsibilities overlap with those of the Centre to Investigate Organized Crimes (CIOC) of the [Islamic Revolutionary Guard Corps] IRGC … However, while the latter mostly deals with issues related to national security, FATA is also tasked with monitoring morality-related offences in cyber space. They can include videos on social media of girls modelling, dancing or generally not complying with national Islamic dress codes or web sites advertising gambling …'[51]

8.2.2 The Iran Primer published an article in April 2023 which stated: 'Iran's national Cyber Police … has stations in dozens of cities across all 31 provinces.'[52]

8.2.3 The HRC detailed findings report stated: 'Along with the intelligence forces and the Basij, FATA constitutes the executive force of the Supreme Council of Cyberspace and the Prosecutor-General's Office to control cyberspace.'[53]

8.2.4 The German Federal Office for Migration and Refugees (BAMF) published a brief report on online activities and monitoring in Iran on 20 December 2024 (The BAMF brief report). The report, which cited various sources, stated: 'According to reports, FATA has about 42,000 volunteers who have good digital skills and a broad social base.'[54]

N.B. the BAMF information quoted above, and all other COI quoted from this source throughout the rest of this CPIN, was originally published in German. All COI from this source has been translated using a free online translation

[50] Project Ainita, About Project Ainita, 24 February 2012
[51] Landinfo and others, Iran; Criminal procedures and documents (page 20), December 2021
[52] The Iran Primer, Profiles: Iran's Intelligence Agencies, 5 April 2023
[53] HRC, Detailed findings of … mission (paragraph 1129), 19 March 2024, updated 8 July 2024
[54] BAMF, Country Brief Iran - Grid Activities - Grid Monitoring (page 1), 20 December 2024

tool. As such 100% accuracy cannot be guaranteed.

Back to Contents

## 8.3 Islamic Revolutionary Guard Corps (IRGC) Cyber Defense Command

8.3.1 The joint Landinfo, CGRS and SEM report noted:

'The IRGC Cyber Defense Command … is the cyber intelligence organization of the IRGC. Its tasks include monitoring and prosecuting organized cybercrime, terrorism, espionage, fighting against "online destruction of cultural and social values", and tracking insults or defamation of revolutionary values. Affiliated with the Cyber Defense Command is the Centre to Investigate Organized Crimes (CIOC) … This unit has been involved in various prominent cyber operations.

'The responsibilities of the IRGC Cyber Defense Command and the CIOC overlap with those of the Cyber Police (FATA). However, the CIOC mostly deals with issues related to national security, such as online material produced by Kurdish parties or other political movements. The IRGC Cyber Defense Command and the CIOC also deal with people advocating for Christianity on social media, as this is considered a matter of national security. The responsibilities of FATA focus more on common cybercrimes, including "moral crimes" …'[55]

8.3.2 A Reuters article, published on 14 September 2023, stated:

'Iran's hardline government introduced a bill [the User Protection Bill, see paragraphs 7.1.7 to 7.1.10] to parliament in 2021 that would effectively hand over control of the internet to the Islamic Revolutionary Guards Corps (IRGC) … An as-yet unpublished report by Miaan said the IRGC was seeking to gain absolute control over the internet in Iran … "Infractions will be dealt with by the military and the internet will become untouchable," Rashidi [Amir Rashidi, director of digital rights and security at Miaan[56]] said.'[57]

8.3.3 The USSD 2023 Country Report stated: 'Government organizations … presumed to be controlled by the IRGC … especially targeted citizens' activities on officially banned social networking websites, and they reportedly harassed persons who criticized the government or raised sensitive social problems online.'[58]

Back to Contents

## 8.4 State monitoring of online activity

8.4.1 Madeline Earp, a consultant technology editor[59], in an article for the CPJ that was published on 16 February 2023, wrote:

'It's not clear whether sanctions-hit Iran has been able to add phone-cracking tools to its extensive surveillance arsenal … But the use [in 2014] of Disk Drill [US-developed file recovery software for phones and computers

[55] Landinfo and others, Iran; Criminal procedures and documents (page 24), December 2021
[56] Reuters, Iran steps up internet crackdown one year after Mahsa Amini death, 14 September 2023
[57] Reuters, Iran steps up internet crackdown one year after Mahsa Amini death, 14 September 2023
[58] USSD, 2023 Country Reports on Human Rights Practices (pages 44 to 45), 22 April 2024
[59] CPJ, Madeline Earp, no date

that is widely available online[60]] … underscores that common consumer software can … be used against the press.

'… "Some (surveillance technology is) developed inside the country, but some is coming from China and Russia, and it's quite advanced," Amir Rashidi, a U.S.-based expert in digital rights and security in Iran, told CPJ.

'… Rashidi told CPJ that authorities could also seize control of social media accounts from devices in their custody, or by remotely intercepting login codes that some services send via text message. "It's easy for them to intercept those messages and hack into your account," said Rashidi.'[61]

8.4.2 The Iran Primer published an article on 17 February 2023 which stated: 'Dissent is widespread in Iran, but the agencies do not attempt to track every citizen. They tend to focus on organizations and networks, especially ones actively recruiting members and plotting against the government … They glean a lot of information from online activities … Agencies intercept electronic messages and scrub social media for criticism of the government.'[62]

8.4.3 The Freedom on the Net report, covering 1 June 2023 to 31 May 2024, stated: 'In June 2023, the social media accounts of several members of an independent artists organization were hacked, likely because of the organization's support of the Woman Life Freedom movement.'[63]

8.4.4 On 24 July 2023, the Department of Foreign Affairs and Trade for the Australian Government (DFAT) published a report which stated:

'The authorities monitor online content, including social media. Individuals repeatedly posting content that is openly critical of the government, its institutions and policies or deemed to be pushing moral boundaries may attract adverse attention, especially if the content goes viral …

'Given the high volume of social media interaction, most of which is unlikely to be of interest to authorities, it is unlikely that every social media user in Iran has their social media comprehensively monitored. Users with a public profile (including with large social media followings, particularly on Instagram) or who are politically active and post about politically sensitive topics (such as minority rights or about topics that are critical of the government) are more likely to be monitored …

'… DFAT also understands the Basij Cyber Council monitors online activity.'[64]

8.4.5 An article published by New Lines Magazine, an American global affairs magazine[65], on 5 September 2023, stated:

'It's believed that … [the CIOC] employs 45,000 people, and the British government sanctioned it in July [2023] for being "involved in cyber operations targeting political dissidents inside Iran, resulting in the arrest of

[60] CPJ, Iran's seizure of detained journalists' devices raises fears …, 16 February 2023
[61] CPJ, Iran's seizure of detained journalists' devices raises fears …, 16 February 2023
[62] The Iran Primer, Explainer: Tactics of Iranian Intelligence, 17 February 2023
[63] Freedom House, Freedom on the Net 2024 (section C8), 16 October 2024
[64] DFAT, DFAT Country Information Report Iran (paragraphs 2.127, 2.128 and 2.190), 24 July 2023
[65] New Lines Magazine, Introducing New Lines, no date

dozens of cyber activists and web administrators." With so many X [formerly Twitter] handles rhapsodizing about the deceased and current IRGC commanders and reiterating the most extreme visions of Iranian politics, a large number of the cyber headquarters' employees could be undercover X operatives.'[66]

8.4.6 The USSD 2023 Country Report stated: '… [T]here were reports that the government monitored private online communications … The government collected personally identifiable information in connection with citizens' peaceful expression of political, religious, or ideological opinion or beliefs … To prevent activities it considered antiregime, the government … closely monitored gatherings such as … online gatherings and networking ...'[67] The USSD did not elaborate on the extent to which the government monitored online communications.

8.4.7 The same USSD Country Report also stated: 'The government restricted the work of domestic activists and often responded to their inquiries and reports with … online hacking, and monitoring of individual activists and organization workplaces … Human rights activists reported … online hacking attempts … The government summoned activists … and confiscated personal belongings such as mobile phones … [and] laptops …'[68]

8.4.8 The HRC detailed findings report stated: 'The main institution in charge of … digital surveillance is the Communication Regulatory Authority (CRA), operating under the umbrella of the Ministry of Information and Communications Technology (MICT).'[69]

8.4.9 The same source stated: '… [T]he practice of summons and arrests connected with social media content shows that the authorities monitored individuals' social media activity … This is particularly the case when content was posted by persons with large followings and/or persons with social standing and/or fame or by persons of interest to the authorities, such as journalists, lawyers and human rights defenders, injured protesters, and where content went "viral" and received significant media attention.

'… Witnesses detained in connection with the [Mahsa Amini] protests stated that their interrogators from security and intelligence bodies had printed pages from their social media accounts and questioned them on the content during the interrogation …

'Several women narrated similar experiences of surveillance, attempts to hack their accounts, coordinated inauthentic behaviours such as attempts to flood accounts by fake followers to discredit or shut down the account, "shadow bans" and accounts disabled following mass reporting, impersonation, as well as smear campaigns online attacking their morality and questioning their loyalty to Iran or their links with foreign states, most notably the USA and Israel. Such experiences lead in many instances to women self-censoring, turning their accounts private if not shutting them

[66] New Lines Magazine, Tweeting Is Banned in Iran, but Not for …, 5 September 2023
[67] USSD, 2023 Country Reports on Human Rights Practices (pages 42 to 43 and 45), 22 April 2024
[68] USSD, 2023 Country Reports on Human Rights Practices (pages 60), 22 April 2024
[69] HRC, Detailed findings of … mission (paragraph 1129), 19 March 2024, updated 8 July 2024

down.'[70]

8.4.10 On 6 January 2024, Iran International published an article entitled 'Iran Unleashes Cyber Campaign To Expose Dissident Accounts' which stated:

'The Islamic Republic of Iran has launched a targeted campaign on X (formerly Twitter), with cyber agents revealing the identities of anonymous dissident users.

'… No one knows how the regime agents uncover anonymous users' identities and expose them on social media, or send messages to them to silence them … [I]ndividuals who use Iranian social media platforms expose their personal information to the government, who controls these platforms.

'The so-called "cyberies" employ various methods, with one of the most commonly used techniques being the creation of simple trends, such as "share a black&white photo of yourself" or "what is difficult about your job?". In these trends, individuals innocently share photos or details about their lives, unwittingly assisting in the identification of their accounts.

'Another method involves the use of paid accounts on X, which allows calling Application Programming Interfaces (APIs). Calling APIs allows the X user to access servers and retrieve all data on individuals interacting with his/her posts, helping them narrow down information to identify the actual person behind the account. According to IRGC's Basij paramilitary chief Gholamreza Soleimani, there are a significant number of these cyber units, with him stating in 2021 that there were "3,500 cyber battalions" supporting the regime online. Additionally, Iranian applications used for everyday activities like banking services and online shopping serve as another key source of information.

'… [R]ecent developments indicate the regime is now using X as a tool to help identify, interrogate and consequently detain dissidents …'[71]

8.4.11 The Iran International report also gave several examples of individuals whose identities were reportedly exposed by government-affiliated users or 'cyber agents'.

8.4.12 The February 2024 IranWire article stated: 'A seven-person working group has been established to monitor the status of VPN usage and report its findings to the Supreme Council of Cyberspace.'[72]

8.4.13 On 1 May 2024, Mandiant, an organisation that provides expertise on cyber defence solutions[73], published a report which stated:

'APT42 [also known as Charming Kitten, ITG18, TA453, and Yellow Garuda[74]], an Iranian state-sponsored cyber espionage actor, is using enhanced social engineering schemes [the practice of manipulating someone into giving up sensitive information, usually through exploiting human error or taking advantage of trust in digital communications[75]] to gain

[70] HRC, Detailed findings … (paragraphs 1164, 1166 and 1167), 19 March 2024, updated 8 July 2024
[71] Iran International, Iran Unleashes Cyber Campaign To Expose Dissident Accounts, 6 January 2024
[72] IranWire, Iranian Authorities Escalate Crackdown on VPNs, 20 February 2024
[73] Mandiant, About Mandiant, no date
[74] Anvilogic, APT42's Cyber Tactics From Credential Theft to Election Interference, 22 August 2024
[75] Norton, What is social engineering? Definition + protection tips, 20 July 2023

access to victim networks, including cloud environments. The actor is targeting Western and Middle Eastern NGOs, media organizations, academia, legal services and activists. Mandiant assesses APT42 operates on behalf of the Islamic Revolutionary Guard Corps Intelligence Organization (IRGC-IO).

'APT42 was observed posing as journalists and event organizers … These social engineering schemes enabled APT42 to harvest credentials and use them to gain initial access to cloud environments. Subsequently, the threat actor covertly exfiltrated data of strategic interest to Iran, while relying on built-in features and open-source tools to avoid detection.

'… [I]ts extensive credential harvesting operations … are often accompanied by tailored spear-phishing campaigns [a cyberattack that uses a personalised but deceptive email or social media message to gain confidential information from a specific individual or organisation for malicious purposes[76]] and extensive social engineering.'[77]

8.4.14 On 23 April 2024, IranWire published an article which stated:

'As part of the ongoing crackdown against women in Iran, authorities have now targeted social media accounts they deem "inappropriate." Kyomars Azizi, police commander of western Tehran province, stated they monitored social media and identified 21 Instagram pages "publishing inappropriate images and breaking norms." These pages, with large followings, were blocked, and legal action was taken against their moderators. Azizi emphasized ongoing police monitoring of online activity, warning people of legal consequences for "crimes committed in cyberspace."[78]

8.4.15 The June 2024 Miaan Group report stated:

'As the Islamic Republic cements NIN in place, it has invested more into developing and deploying technologies to identify, monitor, control, and punish those who deviate from its religious, social, and political mandates. In fact, according to a former government insider, one of the original long-term goals of the NIN is to establish a hyper-surveillance regime.

'… What Miaan's research has shown … is a clear attempt by the Islamic Republic to develop facial recognition technologies, as well as image processing software that can look at online images to see if they violate Iranian laws.'[79]

8.4.16 The same source also stated: '… To date, the only evidence that the government is employing facial recognition, a sophisticated artificial intelligence technology, is that officials have themselves said so. It is possible that officials made such claims primarily to intimidate the public and maintain social control.'[80]

8.4.17 The July 2024 Tightening the Net report by Article 19 stated: '… [D]ata from communications has been used to monitor and arrest users. Examples

[76] Norton, Spear phishing: Definition + protection tips, 19 July 2023
[77] Mandiant, Uncharmed: Untangling Iran's APT42 Operations, 1 May 2024
[78] IranWire, Iran Blocks Dozens of Social Media Accounts Amid Crackdown on Women, 23 April 2024
[79] Miaan Group, … Iran's Progress in Censorship and Surveillance … (pages 12 and 13), June 2024
[80] Miaan Group, … Iran's Progress in Censorship and Surveillance … (page 13), June 2024

range from collecting information on whether internet users have banned applications on their phones, as seen through the application Snapp, to, more recently, the SnappFoods application being used during the Mahsa Jhina Amini protests to geolocate and arrest activists.'[81]

8.4.18 The Tightening the Net report also stated: 'The Ministry of Culture and Islamic Guidance has been trying to launch the Cyberspace Monitoring System since February 2021. This system is a tool for peer reporting on people's use of social networks, websites, and online media …'[82]

8.4.19 A BBC News article, published on 16 September 2024, stated:

'Women in Iran have told the BBC how their online activity has been spied on by the authorities, leading to arrests, threats and beatings … Iran stepped up surveillance following nationwide women-led anti-establishment protests, after the death … of … Mahsa Amini … The recent wave of protests mainly spread through - and were documented on … [social media] platforms. But as a result of surveillance, tens of thousands of protesters were arrested within the first few months. A senior researcher at human rights organisation Article 19, Mahsa Alimardani says the majority of protesters were Gen Z [people born in the late 1990s and early 2000s[83]] and have a large digital footprint, which made "tracking the activities of protesters on social media or through their devices before and during detention" easy.'[84]

8.4.20 In January 2025, the European Union Agency for Asylum (EUAA) published country guidance which stated:

'The Islamic Republic employs a range of strategies to suppress dissent. A primary method is extensive surveillance, both domestically and internationally, utilising advanced technology to monitor communications and social media interactions. This enables the State to identify and target potential threats. A "cyber army" monitors online opinions, leading to threats, physical attacks, kidnapping and killing of some of those who express dissent, even outside Iran.

'… Iranian authorities have ramped up their surveillance capabilities, particularly through the use of state-controlled technologies such as mobile data and internet services.'[85]

Back to Contents

## 8.5 Use of malware

8.5.1 Lookout, a research and security organisation in the field of mobile threat intelligence[86], published an article on 27 April 2023 about Android mobile phone spyware it discovered, tied to the Iranian Police. Authored by Kyle Schmittle, Alemdar Islamoglu, Paul Shunk (all Security Intelligence Researchers), and Justin Albrecht (Lookout's Global Director for Mobile Threat Intelligence), it stated:

[81] Article 19, Tightening the Net: Iran's new phase of digital repression (page 14), 23 July 2024
[82] Article 19, Tightening the Net: Iran's new phase of digital repression (page 18), 23 July 2024
[83] Cambridge Dictionary, Gen Z, no date
[84] BBC News, "Lashed for a social media photo" in Iran, 16 September 2024
[85] EUAA, Country Guidance: Iran; Common analysis … (pages 21 and 25), January 2025
[86] Lookout, About Us, no date

'Researchers at Lookout have discovered a new Android surveillance tool which we attribute with moderate confidence to the Law Enforcement Command of the Islamic Republic of Iran (FARAJA). Named BouldSpy … we have been tracking the spyware since March 2020.

'… We believe FARAJA uses physical access to devices, likely obtained during detention, to install BouldSpy to further monitor the target on release.

'… We believe BouldSpy to be a new malware family based on the relatively small number of samples that we've obtained, as well as the lack of maturity around its operational security …

'… Notable surveillance capabilities

- 'Getting all account usernames available on the device and their associated types (such as Google, Telegram, WhatsApp and others)
- 'List of installed apps
- 'Browser history and bookmarks
- 'Live call recordings
- 'Call logs
- 'Take photos from the device cameras
- 'Contact lists
- 'Device information (IP address, SIM card information, Wi-Fi information, Android version, and device identifiers)
- 'List of all files and folders on the device
- 'Clipboard content
- 'Keylogs
- 'Location from GPS, network, or cell provider
- 'SMS messages (sent, received and drafts)
- 'Record audio from the microphone
- 'Take screenshots

'A notable capability of BouldSpy is that it can record voice calls over multiple Voice over IP (VoIP) apps as well as the standard Android phone app …'[87]

For a list of the VoIP and Android phone applications that BouldSpy is capable of recording voice calls from, see the Lookout article.

8.5.2 The same Lookout article also stated:

'Based on our analysis of exfiltrated data … BouldSpy has victimized more than 300 people, including minority groups such as Iranian Kurds, Baluchis, Azeris, and possibly Armenian Christian groups … Our analysis also revealed photos of drugs, firearms, and official FARAJA documents that

[87] Lookout, Lookout Discovers Android Spyware Tied to Iranian Police …, 27 April 2023

indicate potential law enforcement use of the malware. However, much of the victim data points to its broader usage, which indicates targeted surveillance efforts towards minorities within Iran. Notably, much of the malware's activities occurred during the height of the Mahsa Amini protests in late 2022.'[88]

8.5.3 Writing about BouldSpy, the HRC detailed findings report stated: 'Researchers noticed a spike in use in September 2022, which has steadily increased until at least February 2024.'[89]

Back to Contents

## 8.6 Arrest, detentions and convictions

8.6.1 On 2 February 2024, the HRC published a summary report for its 2023/2024 fact-finding mission (see paragraph 8.1.6 for details), which stated:

'The State authorities threatened, intimidated, summoned and arrested persons in connection with protest-related content posted on social media platforms. Such content included messages of solidarity with protesters, reports of violations committed by the State, pictures posted by injured protesters and offers of legal and medical assistance for protesters and their families. The authorities used social media content as evidence for criminal charges on various grounds, such as "propaganda against the system", "spreading lies" and "insulting the Supreme Leader". The content of personal Instagram accounts was used as evidence during criminal proceedings for charges that carried heavy punishments, including the death penalty …'[90]

8.6.2 The HRC detailed findings report added: '… While not all protest-related, according to the non-governmental organization Human Rights Defenders in Iran, from January 2011 to the end of August 2023, at least 1,315 individuals were reportedly arrested in relation to content posted on social media. In some cases, this resulted in severe punishments, including the death penalty.'[91]

8.6.3 On 9 February 2023, National Iranian American Council (NIAC) Action, an organisation aiming to provide a voice to the Iranian-American community[92], published an article which stated: '… [U]nlike previous crackdowns, wherein the Islamic Republic heavily targeted political activists and students with heavy penalties, this time the judicial system seems to have issued many more severe sentences against citizens who have thus far been relatively unknown. This dynamic is particularly apparent for citizens who have posted viral videos on social media, with many having received extraordinarily harsh sentences from the courts.'[93]

8.6.4 An article dated 29 February 2024 published by Radio Free Europe / Radio Liberty (RFE / RL), an organisation which aims 'to promote democratic values by providing accurate, uncensored news'[94], stated:

[88] Lookout, Lookout Discovers Android Spyware Tied to Iranian Police …, 27 April 2023
[89] HRC, Detailed findings of … mission (paragraph 1182), 19 March 2024, updated 8 July 2024
[90] HRC, Report of the … International Fact-Finding Mission … (paragraph 103), 2 February 2024
[91] HRC, Detailed findings of … (paragraph 1163), 19 March 2024, updated 8 July 2024
[92] NIAC Action, Mission and Vision, no date
[93] NIAC Action, Social media users who go viral given harsh prison sentences …, 9 February 2023
[94] RFE / RL, About RFE/RL, no date

'In the West Azerbaijan Province, police chief Rahim Jahanbakhsh announced the arrest of 50 people responsible for managing social-media pages that authorities say incited public unrest and discouraged election participation. The arrests, Jahanbakhsh noted, were conducted in coordination with judicial authorities, though the identities of those detained remain undisclosed. Jahanbakhsh also warned that publishing any content deemed provocative on social media would be considered a criminal offense.'[95]

8.6.5 On 28 May 2024, RFE / RL published an article which stated:

'Rights groups say Iranian authorities have intensified their crackdown on posts made by social media users following the death of President Ebrahim Raisi in a helicopter crash on May 19 [2024] … The crash was mocked by many users of Persian-language social networks. In turn, Iranian security and judicial agencies have responded vigorously to the online activities of citizens and media activists … [Some] have been charged, rights groups say, for "spreading lies and insulting the sanctity of service martyrs," for their comments on Raisi's death … Others say they have been warned by authorities for their online activities … The Judiciary Information Center of Kerman province announced that 254 individuals received telephone warnings for posting "offensive" content, while eight people faced judicial summons.'[96]

8.6.6 The June 2024 Miaan Group report stated: 'Iranian authorities continue to put direct pressure on content creators in the form of threats, interrogations, arrests, and punitive measures against online activists, social and political figures, celebrities, and influencers.'[97]

8.6.7 The Freedom on the Net report, covering 1 June 2023 to 31 May 2024, stated:

'The Iranian regime routinely arrests journalists and social media users for their online activities. Those affected in recent years have included prominent activists, Instagram celebrities, editors at independent news outlets, and citizen journalists associated with persecuted religious groups …

'Iranian authorities commonly engage in extralegal intimidation and violence. Journalists, bloggers, and activists who are serving prison sentences due to their online activities frequently experience maltreatment and torture while in detention.'[98] CPIT noted that the report did not define what it meant by 'routinely' or 'frequently'.

8.6.8 The EUAA country guidance stated: 'The EU sanctioned several individuals and entities as perpetrators of serious human rights violations including … arbitrary arrests over online criticism.'[99]

8.6.9 The BAMF brief report, published in December 2024, stated: 'Charges usually do not relate exclusively to virtual activities. Instead, there are often

[95] RFE / RL, Iran Cracks Down On Calls For Election Boycott, 29 February 2024
[96] RFE / RL, … Authorities Ratchet Up Crackdown On Critics …, 28 May 2024
[97] Miaan Group, … Iran's Progress in Censorship and Surveillance … (page 14), June 2024
[98] Freedom House, Freedom on the Net 2024 (sections C3 and C7), 16 October 2024
[99] EUAA, Country Guidance: Iran; Common analysis … (page 16), January 2025

combinations of different offences and profiles.'[100]

8.6.10 The AIC article stated: '… [D]ozens of journalists and activists have reported that their cell phone SIM cards have been blocked by Iranian authorities and are unable to purchase a new one. This restriction is being used as an alternative to arresting them or other methods that require official action to force them into silence.'[101]

8.6.11 For examples of individuals who have been arrested, detained, and convicted in connection with their online activities, see the following:

- paragraphs 1174 and 1177 to 1179 of the HRC detailed findings report for examples that occurred between late 2022 and 2023 in connection with online activities related to the Woman, Life, Freedom movement
- the NIAC Action article dated 9 February 2023 about the sentencing in late 2022, or cases outstanding as of February 2023, of various individuals who posted online either dance videos or videos of themselves (women) without hijab
- an IranWire article dated 8 May 2023, about the hanging of two men sentenced to death for blasphemy in connection with involvement in a Telegram channel called "Critique of Superstition and Religion"
- an Amnesty International article dated 16 May 2023, about a woman whose September 2022 death sentence, for "spreading corruption on earth" after she spoke out in support of LGBTQIA+ rights on social media and in a BBC documentary, was overturned
- an article dated 27 October 2023 by the Hengaw Organization for Human Rights (Hengaw), an organisation that covers human rights violations in Iran[102], about a man who was detained in Tehran after allegedly posting critical comments on online forums
- an IranWire article of 6 December 2023, about an Instagram blogger given a five-year suspended prison sentence, a fine, and a smartphone ban on charges including "inciting others to commit violent acts"
- a BBC News article dated 14 January 2024 about the release of 2 female journalists after more than a year in jail, charged with collaborating with the US government and colluding against national security. One of the journalists broke the news of Mahsa Amini's death by posting a captioned photograph, of Ms Amini's family after they learned their daughter had died, online. On 15 January 2024, a Guardian article reported new charges against the journalists after photos of them upon release, without hijabs,

[100] BAMF, Country Brief Iran - Grid Activities - Grid Monitoring (page 6), 20 December 2024
[101] AIC, Myth vs. Fact: Censorship in Iran, updated 30 January 2025
[102] Hengaw, About us, no date

were circulated on social media

- a BAMF briefing note, published on 5 February 2024, about the death of a student in Sistan and Baluchestan province, 3 days after being arrested by security forces for his online activities and protest support
- an RFE / RL article dated 9 February 2024 about charges of "insulting images of the sacred" made against a prominent Iranian online retailer
- a 12 March 2024 Iran International article about the arrest of 4 individuals linked to a video, circulated and viewed 100,000 times on X, which showed a confrontation between a cleric and a woman without the mandatory hijab in the city of Qom
- a 20 March 2024 article by NIAC Action about a prominent scholar given a one-year prison sentence after appearing in a video without hijab on social media
- a Center for Human Rights in Iran (CHRI) article dated 17 April 2024, about the detention of a female journalist who tweeted about being tasered and sexually harassed for being in public with her hair exposed
- an RFE / RL article dated 6 May 2024 about a man sentenced to death on charges of "corruption on Earth" after he put out calls for protests on his social media account
- the RFE / RL article dated 28 May 2024 about the crackdown on online critics following President Raisi's death (see paragraph 8.6.5) which gave examples of 3 individuals arrested due to their online activities
- an RFE / RL article dated 5 June 2024 about a literary editor and online activist (with a previous prison sentence), detained after responding to a tweet by the Supreme Leader with a simple full stop which went viral
- a BBC news article dated 16 September 2024 about a woman who was given a suspended sentence and 50 lashes after posting a photo on social media of herself in public without her hair uncovered (the article covered the similar stories of 2 other women and one man)
- an article dated 9 October 2024 by the Human Rights Activists News Agency (HRANA) about a journalist sentenced to 13 months and 16 days in prison after he published stories on his own Instagram account
- a BBC News article dated 2 December 2024 about an Iranian rapper whose April 2024 death sentence, for "corruption on earth", for spreading lies in cyberspace, among other offences, was overturned

Back to Contents

# 9. Social media usage in Iran

## 9.1 Social media platforms

9.1.1 The Freedom on the Net report, covering 1 June 2023 to 31 May 2024, citing various sources, stated:

'Facebook, SnapChat, TikTok, X, and YouTube are all blocked or filtered, as are major blog-hosting platforms, the navigation app Waze, the audio discussion app Clubhouse, and the messaging apps Viber, Telegram., and Signal. Instagram and WhatsApp, the only international platforms that remained accessible in Iran prior to September 2022, were blocked amid the nationwide Woman, Life, Freedom protests.

'Other foreign platforms including video gaming software, Skype, and PayPal remained blocked or filtered during the coverage period. The Google Play store and Apple's app store were filtered in September 2022. After a month of filtering, authorities unfiltered the Apple app store, although users still report issues accessing the site. As of June 2024, Google Play remained blocked; over 90 percent of mobile phone users in Iran use devices powered by Google's Android operating system, which distributes apps with Google Play.'[103]

9.1.2 The BAMF brief report, published in December 2024 added that applications such as Blogspot, Blogger, Wix and WordPress are also officially blocked in Iran[104].

9.1.3 The New Lines Magazine article, published on 5 September 2023, stated:

'… [T]he latest social media innovation, Threads, has also been blocked …

'At the same time as blocking major social media providers one after another, the Islamic Republic has furthered its work on a domestic internet, boasting a motley crew of applications, such as instant messaging apps and makeshift social media platforms, which the authorities encourage people to use as replacements for the "diabolical" Western apps designed to contaminate the minds of the pious Iranians … [D]espite their continuous disparagement of internationally used social media, the influential members of the ruling elite never abandoned those platforms, including X …'[105]

9.1.4 On 15 February 2024, Iran International published an article entitled 'Iran Orders Social Media Influencers To Get Advertising License' which stated: 'A recent mandate requir[es] … advertising licenses for social media accounts boasting over 5,000 followers in Iran …'[106]

9.1.5 The Iran International article published on 15 February 2024 stated: 'All major social networks … are blocked in Iran, but controls are readily sidestepped by VPNs (virtual private networks) and anti-filtering software.'[107]

9.1.6 The Tehran E-commerce Association report on the quality of the internet in Iran, which cited various sources, stated:

---

[103] Freedom House, Freedom on the Net 2024 (section B1), 16 October 2024
[104] BAMF, Country Brief Iran - Grid Activities - Grid Monitoring (page 3), 20 December 2024
[105] New Lines Magazine, Tweeting Is Banned in Iran, but Not for …, 5 September 2023
[106] Iran International, Iran Orders Social Media Influencers To Get … License, 15 February 2024
[107] Iran International, Iran Orders Social Media Influencers To Get … License, 15 February 2024

'… Iran … ranks among the top countries with the most severe restrictions on social networks …

'… Despite the implementation of the strictest restrictions, more than half of the users continue to use blocked platforms, specifically Instagram, WhatsApp, and Telegram. The imposition of network restrictions, price increases, and the numerous inconveniences to reduce the user base of these platforms have only succeeded in reducing their traffic or preventing further increases in their traffic consumption. This should not be mistaken as a reduction in their popularity among users.

'… The sustained user preference for blocked platforms like Instagram and Telegram indicates widespread use of VPN tools.

'… [Also,] many high-ranking officials of the country have consistently engaged in political activities on filtered social networks over the past years and have even sometimes announced their most important statements through these platforms …'[108]

9.1.7 The July 2024 Tightening the Net report by Article 19 stated:

'The Islamic Republic's efforts over the past decade to impose domestic platforms on Iranian users have failed, and a February 2024 government centre survey demonstrated that, despite censorship, Instagram, Telegram, and WhatsApp remain the most popular and widely-used platforms among Iranian users … VPNs are ubiquitous in Iran and the majority of Iranians use VPNs to access the international internet because many popular applications are already censored.'[109]

9.1.8 The Freedom on the Net report, covering 1 June 2023 to 31 May 2024, stated:

'… Iranian versions of popular social media apps, such as Bale, Rubika, and Soroush, receive significant financial support from the government as it continues to push users away from the international internet.

'… Aparat, an Iranian website similar to YouTube that enjoys less expensive tariff rates, is one of the most visited websites in Iran. Content on Aparat is governed in accordance with Iranian law, making it difficult for users to share or access socially or politically sensitive views.'[110]

9.1.9 The EUAA country guidance stated: 'Those with high numbers of followers on social media platforms have seen their mobile services cut off or social media accounts suspended.'[111]

9.1.10 The AIC article stated: 'While the Iranian government continues to restrict access to social media, new online platforms continue to emerge as old ones become more difficult to access …'[112]

Back to Contents

## 9.2 Number of users

[108] Tehran E-commerce Association, Quality of Internet in Iran (pages 29, 30 and 32), 18 July 2024
[109] Article 19, Tightening the Net: Iran's new phase of digital repression (page 14), 23 July 2024
[110] Freedom House, Freedom on the Net 2024 (sections B6 and B7), 16 October 2024
[111] EUAA, Country Guidance: Iran; Common analysis and guidance note (page 25), January 2025
[112] AIC, Myth vs. Fact: Censorship in Iran, updated 30 January 2025

9.2.1 A report entitled 'Digital 2024: Iran', published by DataReportal, a website that provides data-driven reports on online activity[113], stated:

'… [T]here were 48.00 million active social media user identities in Iran in January 2024 … [A]nalysis shows that social media users in Iran remained unchanged between early 2023 and the beginning of 2024 … The number of social media users in Iran at the start of 2024 was equivalent to 53.6 percent of the total population [estimated by DataReportal at 89.5 million in January 2024[114]], but it's important to stress that social media users may not represent unique individuals … More broadly, 65.6 percent of Iran's total internet user base [estimated at 73.14 million in January 2024[115]] (regardless of age) used at least one social media platform in January 2024.'[116]

9.2.2 The Iran International article published on 15 February 2024 stated: 'Nearly every Iranian with a smartphone has installed anti-filtering software that allows access to filtered applications and websites. Instagram is the second most popular social platform in Iran after Telegram with over forty million users. Both platforms are used by millions of small and home-based businesses for marketing.'[117]

9.2.3 On 17 October 2024, Iran International published an article entitled 'State-backed poll shows most Iranian students use foreign social media' which stated: 'An … ISPA [Iranian Students Polling Agency[118]] poll conducted in September [2024] revealed that … Instagram is the most popular platform among the broader population, with 56% of users, followed by Telegram (39.3%) and WhatsApp (33.3%). Among Iranian platforms, Ita and Rubika are the most frequently used, each with over 28% of users, excluding university students.'[119]

9.2.4 CPIT noted that Iran had an estimated population of around 88.4 million in 2024[120]. Therefore, based on the ISPA poll, in absolute numbers, there were approximately 49.5 million Iranians users of Instagram as of September 2024, 34.7 million users of Telegram, and 29.5 million users of WhatsApp.

Back to Contents

## 10. Surveillance outside Iran

### 10.1 Targeting citizens abroad

10.1.1 The Iran Primer's February 2023 article stated:

'In Europe and abroad, the agencies track dissidents in exile, some of whom have networks in Iran that agitate against the government. Intelligence agencies have targeted a broad range of exiled oppositionists, including monarchists, Kurdish separatist groups, dissidents who defected from the Islamic regime, and the Mujahedeen-e Khalq (MEK), a left-wing Islamist organization. They have also targeted individual activists and journalists,

[113] DataReportal, About, no date
[114] DataReportal, Digital 2024: Iran (Population of Iran in 2024), 23 February 2024
[115] DataReportal, Digital 2024: Iran (Internet use in Iran in 2024), 23 February 2024
[116] DataReportal, Digital 2024: Iran (Social media statistics for Iran in 2024), 23 February 2024
[117] Iran International, Iran Orders Social Media Influencers To Get … License, 15 February 2024
[118] ISPA, Iranian Students Polling Agency (ISPA), an Introduction, no date
[119] Iran International, … [M]ost Iranian students use foreign social media, 17 October 2024
[120] US CIA World Factbook, Iran, (People and Society), updated 12 February 2025

especially those involved in the Green Movement protests over the disputed 2009 presidential election as well as several subsequent rounds of unrest.

'… Sometimes, they lure exiled dissidents to countries neighboring Iran to be apprehended by Tehran's agents …

'… The [Ministry of Intelligence and Security] MOIS has historically focused on Europe, where many Iranian dissidents have sought refuge.'[121]

10.1.2 An article published by Article 19 in February 2023 stated:

'On 20 February [2023], Tom Tugenhadt, the UK's Security Minister … stated that he had spoken to his counterparts in France, Germany, and the United States about individuals who had been targeted in those countries …

'The authorities of the Islamic Republic have a long-standing track record of targeting dissidents abroad through intimidation, harassment, abductions and even extrajudicial killings. Recent years have seen a significant escalation of such extraterritorial threats against real and perceived dissidents. In its February 2023 statement, the Metropolitan Police stated that the police and intelligence agencies had foiled "15 plots since the start of 2022 to either kidnap or even kill British or UK-based individuals perceived as enemies of the regime".'[122]

10.1.3 A response to an information request dated 2 March 2023, by the Immigration and Refugee Board of Canada (IRBC), stated: '… [A] retired professor [see paragraph 10.2.1 for more details] stated that authorities will … sometimes directly "threaten" people in Canada, as they want to stop these people from being "active against the regime"[123]

10.1.4 A 27 March 2024 IranWire article stated:

'Testimonies from four Arab political activists corroborate allegations that Iran's security agencies actively coerce families to lure them to Turkey or neighboring countries for potential abduction and repatriation to Iran … While such coercive tactics have targeted journalists and civil and political activists abroad before, Arab activists interviewed by IranWire believe these pressures, often concealed from public scrutiny, persist predominantly in their community.'[124]

10.1.5 Reporters Without Borders (RSF) published a report on transnational repression of Iranian journalists in the UK, on 1 April 2024. The report, which cited various sources, stated:

'Iranian journalists working in countries as far afield as the United States, France, Germany, Sweden and the United Kingdom – countries which claim to champion press freedom – are regularly subjected to intimidation or attacks, both online and offline. Just like repression inside Iran, transnational repression, as attacks beyond borders are known, tends to increase at times when the eyes of the world are on Iran: thus, there has been a spike in harassment of exiled Iranians since late 2022, when protests erupted in Iran

[121] The Iran Primer, Explainer: Tactics of Iranian Intelligence, 17 February 2023
[122] Article 19, … [O]ppression beyond borders risks journalists' lives, 21 February 2023
[123] IRBC, Iran: Monitoring of Iranian citizens outside of Iran … (section 1.1), 2 March 2023
[124] IranWire, … Iran Systematically Targets Families of Arab Activists Abroad, 27 March 2024

following the death of Mahsa Amini.

'… Those working in Persian for prominent media platforms such as the BBC, Iran International, Deutsche Welle, Radio France Internationale, Voice of America, Radio Zamaneh and others are particularly likely to be targeted, as they are the most likely to reach large audiences at home.

'The range of tactics is wide. It includes, among others, physical attacks, detentions, defamation, asset freezes, harassment of family members, threats and harassment, judicial proceedings, and intrusive surveillance. In recent years, to these more traditional methods have been added a slew of digital techniques, most notably threats and intimidation delivered online. Physical and digital threats are often used together, and attacks are often gendered. The Iranian government and its proxies are the primary perpetrators of attacks …'[125]

10.1.6 The same source stated: 'Around 60% of RSF survey respondents [dozens of exiled Iranian journalists living in the United Kingdom in 2023] said their families had experienced threats or intimidation related to their work as journalists. This includes being called in for interrogations, applying economic penalties such as asset freezes or job loss, the removal of passports, travel bans, surveillance, tapping phone calls and detentions.'[126]

10.1.7 A 16 October 2024 report entitled 'Iran; Treatment by the authorities of family members of dissidents residing abroad' was written by the COI unit of the Belgium Office of the Commissioner General for Refugees and Stateless Persons (CGRS – CEDOCA). The report, citing a phone call with a researcher on transnational repression on 23 September 2024, stated:

'"Proxy punishment is one of the most widespread methods to repress dissidents abroad. It is widely used because it's one of the easiest ways to target someone and it's very efficient also, because it puts people in a dilemma over whether to continue their activism or not. And the Iranian regime uses this method substantially against everyone who has a public profile. (…) It is so easy and the Iranian security intelligence agencies have a lot of resources, also human resources, it doesn't cost them a lot to find out who the parents are, who the brother or sister is, and to pay them a visit. A simple visit will already send a very strong signal to someone."

'… "Transnational repression intensifies whenever there's political conflict or tension inside the country (…). So you will see this coming in waves, whenever the regime feels a challenge or feels threatened they will intensify this repression across borders."'[127]

10.1.8 The CGRS – CEDOCA report also outlined groups of people it said were targeted by proxy punishment between 2021 and 2024 which, while non-exhaustive, comprised journalists, activists, protesters, and Christians[128]. See the CGRS – CEDOCA report for more information including individual examples of proxy punishment for people in each of these groups.

10.1.9 The EUAA country guidance stated that the Iranian authorities '… carry-out

[125] RSF, … [T]ransnational repression of Iranian journalists in the UK (pages 3 and 5), 1 April 2024
[126] RSF, … [T]ransnational repression of Iranian journalists in the UK (page 3), 1 April 2024
[127] CGRS – CEDOCA, … [F]amily … of dissidents … abroad (pages 10 to 11), 16 October 2024
[128] CGRS – CEDOCA, … [F]amily … of dissidents … abroad (pages 11 to 20), 16 October 2024

activities abroad … by hiring criminal groups, arresting exiled dissidents, bringing them back to Iran and executing them.'[129] CPIT noted that the guidance did not go on to provide any more details in this regard.

10.1.10 On 21 October 2024, The Washington Institute for Near East Policy (TWI), an organisation that aims to 'advance a balanced and realistic understanding of American interests in the Middle East'[130], published an article, citing various sources, which stated:

'The Washington Institute has produced an interactive map drawing on … [a] dataset which depicts Iranian external operations - assassinations, abductions, intimidation and surveillance plots - around the world and shows a marked increase in Iranian operational activity in Europe, with many of these plots involving criminal recruits.

'… Iranian government officials are increasingly using drug traffickers and other criminals in Iran as middlemen to recruit criminals to carry out attacks abroad … Not only does Iran use individuals with a criminal past, but organised crime groups as well.'[131]

10.1.11 TWI's interactive map documented 44 plots and attacks (including assassinations, attacks, attack attempts, bombings, cyber, drone/rocket, kidnapping, recruitment, and threats), when filtered to show events against Iranian dissidents only, in the worldwide diaspora between 2023 and 2025[132].

10.1.12 For some examples of Iranian citizens, or organisations supporting Iranian citizens, abroad who have been targeted, see the following:

- pages 27 to 28 of the USSD 2023 Country Report about the threats to, and temporary relocation of, journalists at Iran International's London headquarters, and a March 2023 cyberattack against Washington DC-based National Union for Democracy in Iran after it unveiled a new "Maximum Support" policy focused on supporting Iranians
- a 30 May 2024 OHCHR press release about the stabbing of Iran International journalist, Pouria Zeraati, on 29 March 2024 outside his London home, and the September 2023 assault against another Iran International journalist, Kian Amani, at a hotel in New York
- an AP News article dated 22 October 2024 about the prosecution of a senior military official and 3 others with links to Iran's government for plotting to kill an Iranian American opposition activist and contributor to Voice of America, Masih Alinejad, who lived in exile in New York City

Back to Contents

## 10.2 Monitoring citizens abroad

[129] EUAA, Country Guidance: Iran; Common analysis and guidance note (page 16), January 2025
[130] TWI, About, no date
[131] TWI, Iranian External Operations in Europe: The Criminal Connection, 21 October 2024
[132] TWI, Iranian External Operations, updated 25 February 2025

10.2.1 The March 2023 IRBC response to an information request stated:

'In an interview [on 7 February 2023] with the Research Directorate, a lawyer, human rights activist, and senior fellow at the Centre for Advancing Canada's Interests Abroad of the Macdonald-Laurier Institute (MLI), who has expertise in Canada-Iran relations, noted that the MOIS and the IRGC's Intelligence Organization are the primary agencies conducting surveillance of Iranian citizens abroad.

'… The lawyer stated that they are aware of cases in which individuals suspect they are being physically monitored in Canada by Iranian authorities. The same source noted the example of an Iranian activist in Canada whose family in Iran was visited by authorities; authorities provided the family members with information indicating that they were aware of the activist's day-to-day activities in Canada - information that authorities "could only know if they were closely physically monitoring" the activist in Canada. In an interview [on 1 February 2023] with the Research Directorate, a retired professor at York University who has published books and articles on the leftist movement in Iran, diaspora, religious fundamentalism, secularism and multiculturalism … noted that sometimes those monitoring Iranian citizens abroad on behalf of the Iranian regime are students or businesspeople who are asked to monitor their peers. The same source stated that authorities are mainly interested in knowing what kinds of things these people are doing abroad.'[133]

10.2.2 The same response to an information request also stated that the lawyer told their Research Directorate: 'Those monitored in Canada by Iranian authorities "certainly" include people who are "very politically active," but can also include ordinary people "who might not engage in politics every day but may do so from time to time".'[134]

10.2.3 In June 2023, Switzerland's Federal Intelligence Service (FIS) published its annual situation report on Switzerland's security, which stated: 'The Iranian intelligence services have long been conducting surveillance on nationals who have fled the country and who are deemed to be influential. Many of these refugees have been living in Europe, including Switzerland, for years or even decades. Iranian surveillance of these diaspora communities may have been intensified yet again following the latest wave of protests.'[135]

10.2.4 A September 2023 'General Country of Origin Information Report on Iran' (the Iran COI report) published by the Netherlands Ministry of Foreign Affairs (BZ, Dutch abbreviation), citing various sources, stated: 'According to several sources, the political activities of people abroad who have certain links to Iran are monitored, because the Iranian authorities see them as a security risk. This policy applies no matter which ethnic group a person belongs to.'[136]

10.2.5 On 17 October 2024, the EUAA published a query response, covering the human rights situation in Iran between January 2023 and 7 October 2024.

[133] IRBC, Iran: Monitoring of Iranian citizens outside of Iran … (section 1), 2 March 2023
[134] IRBC, Iran: Monitoring of Iranian citizens outside of Iran … (section 1.1), 2 March 2023
[135] FIS, Switzerland's Security 2023 (page 64), June 2023
[136] BZ, General Country of Origin Information Report on Iran (page 27), September 2023

The response, which cited various sources, stated:

'In an interview with the EUAA [on 24 September 2024[137]], Leila Alikarami [an expert on Iranian law, a qualified attorney, and a member of Iran's Central Bar Association since 2002[138]] noted that:

'"[A]uthorities do not systematically monitor every Iranian national abroad. However, high-profile activists, journalists, and human rights defenders may be monitored outside the country and arrested upon their return. Typically, the passport police or the Islamic Revolutionary Guard Corps (IRGC) maintain lists of Iranian citizens who have active cases. If an individual's name appears on the passport police list, their passport will be confiscated by immigration authorities during the immigration process. If their name is on the IRGC list, they can be identified even after passing through immigration by IRGC officers present at the airport …"'[139]

10.2.6 TWI's interactive map documented 14 surveillance events, when filtered to show events against Iranian dissidents only, in the global diaspora between 2023 and 2025[140].

Back to Contents

## 10.3 Sur place activity

10.3.1 The Guardian published an article on 14 February 2023 which stated: '… [A] submission to a Senate inquiry by the Department of Home Affairs … said it was "aware of reports that pro-Iranian government informants are surveilling former Iranian residents protesting against the regime in Australia and threatening their relatives in Iran as a result."'[141]

10.3.2 The March 2023 IRBC response to an information request stated that the lawyer told their Research Directorate: 'Iranian authorities monitor their citizens' participation in events or protests in Canada.'[142]

10.3.3 The same IRBC response went on to state:

'The lawyer indicated that upon their return to Iran, "some" citizens whose activities abroad have been monitored by authorities are questioned on arrival at the airport. The same source added that for "some" returnees, authorities will retain the passport of the individual and will instruct them to return for additional questioning. Further and corroborating information could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.'[143]

10.3.4 The Iran COI report, published by the BZ in September 2023, stated: 'According to one [confidential] source, people who had been politically active in the West or were in structural contact with activists were also arrested and sentenced after their return.'[144]

---

[137] EUAA, Iran; Human rights situation … (footnote 175 on page 22 and page 33), 17 October 2024
[138] EUAA, Iran; Human rights situation (Q72-2024) (page 33), 17 October 2024
[139] EUAA, Iran; Human rights situation (Q72-2024) (page 22), 17 October 2024
[140] TWI, Iranian External Operations, updated 25 February 2025, accessed 27 February 2025
[141] The Guardian, Australia foils Iran surveillance plot …, 14 February 2023
[142] IRBC, Iran: Monitoring of Iranian citizens outside of Iran … (section 1.1), 2 March 2023
[143] IRBC, Iran: Monitoring of Iranian citizens outside of Iran … (section 2), 2 March 2023
[144] BZ, General Country of Origin Information Report on Iran (page 113), September 2023

10.3.5 On 22 September 2023, The Guardian published an article entitled 'Iranian activists across Europe are targets of threats and harassment'. The article stated:

'Iran and its agents appear to be orchestrating a Europe-wide campaign of harassment, surveillance, kidnap plots and death threats targeting political activists who are protesting against the regime.

'The Guardian has spoken to 15 Iranian campaigners who have been targeted in similar acts of repression across the UK, France, Germany, Spain, Switzerland and Sweden.

'In most of the cases, the activists have been warned by western police or security agencies that Iran is behind credible threats to their life in retribution for their activism on European soil.

'The attacks include hacking, cyber-attacks and online harassment that can include thousands of death threats sent over a week, and real-world threats.

'… In France, police have issued travel warnings to women organising protests against Iran's regime, warning there is a risk they could be kidnapped by a country that has a long history of hostage-taking. They were specifically warned not to travel to Turkey or the UAE.

"They explained to me that Iran's target is people having a media impact, especially on public opinion," said Mona Jaffarian, who has led protests in France.'[145]

10.3.6 Another Guardian article dated 18 December 2023 stated:

'The Guardian has spoken to a number of Iranians living in the UK who have taken part in or organised protests in the UK over the past year since [Mahsa] Amini's death and continue to fear for their lives. Iran is increasingly targeting people outside its borders in a tactic known as transnational repression, which aims to stifle debate or criticism … Some of the activists interviewed by the Guardian say they have also been victims of stalking, online doxing [exposing private or identifying information online about an individual or group without their consent, usually with malicious intent[146]] and character assassinations led by those supporting the regime in the UK.'[147]

10.3.7 A 20 February 2024 IranWire article stated:

'… [R]ecent developments suggest that security institutions have shifted their focus to individuals who participated in an anti-Islamic Republic rally in Berlin on October 22, 2022.

'IranWire has conducted interviews with 17 individuals whose passports and electronic devices were confiscated at various Iranian airports over the past fortnight.

'Despite the rhetoric of various Iranian officials welcoming the return of Iranians residing abroad, Iranians who participated in the Berlin rally have had their passports, mobile phones, laptops, and other electronic devices

[145] The Guardian, Iranian activists across Europe are targets …, 22 September 2023
[146] Stovall, Jacob, and Wolter, Teagan, for Encylopaedia Britannica, Doxing, updated 20 Feb. 2025
[147] The Guardian, … [H]ow Iran is targeting protesters in Britain, 18 December 2023

confiscated at Tehran Airport.

'… The number of Iranian diaspora members facing passport confiscation at various airports is immeasurable.

'However, it's evident that in recent weeks, security institutions have intensified pressure on this group, with IranWire receiving reports of dozens of Iranians effectively being detained in the country every week.

'… During interrogations of Iranians residing abroad, security and judicial authorities have claimed to have identified them through published images of protest gatherings of Iranians overseas.

'Numerous pictures and videos of these gatherings, particularly during the Woman, Life, Freedom protests, were published in both Persian and non-Persian media outside of Iran.

'However, relying only on these images to identify participants in the gatherings poses significant challenges.

'Matching these images with the identities of protesters outside Iran is nearly impossible.

'IranWire has learned that security institutions utilize specialized groups to monitor the Iranian diaspora.

'These "pseudo-security" groups are tasked with investigating, compiling and documenting the activities of active Iranians beyond the country's borders.

'Through scrutiny of social media accounts belonging to the Iranian diaspora members, these groups gather evidence of their presence at protest gatherings.

'This includes photographs, videos, and even content detailing travel arrangements to the protest site, individuals spotted at the gathering, or slogans chanted.'[148]

10.3.8 Another IRBC response to an information request, dated 22 April 2024, stated:

'In an interview with the Research Directorate [on 26 February 2024] … [the] retired professor from York University … stated that anti-government activists would "definitely" be detained when they return to Iran, and that "in most cases," this would happen "immediately" upon their arrival. When asked the same question [on 1 March 2024] about the treatment of anti-government activists who return to Iran, the HRANA [Human Rights Activists News Agency] representative indicated that regardless of whether they were political activists, students, or former refugees, an individual's treatment upon their return is "determined by their perceived threat to the regime," and this assessment is "influenced by a variety of factors," such as their activities abroad, their citizenship status, and which countries they are returning from. The same source added that "particular scrutiny" occurs for those with dual citizenship, individuals returning from "Sunni countries with connections to religious groups," and those returning from "Western countries due to

[148] IranWire, Crackdown on Diaspora Dissenters: Surge in Passport Seizures …, 20 February 2024

political activities".[149]

10.3.9 In June 2024, the EUAA published an 'Iran – Country Focus' report, covering events from 1 January 2023 to 17 April 2024, which stated: 'In an interview with EUAA, Barzoo Eliassi [associate Professor in the department of social work, Linnaeus University, Sweden[150]] noted … if complaints against someone outside Iran would be lodged with the Iranian authorities, this person would be summoned by the authorities upon their return to Iran.'[151]

Back to Contents

## 10.4 Monitoring online activity abroad

10.4.1 The March 2023 IRBC response to an information request stated:

'According to… [a] cybersecurity analyst [at a US-based human rights organisation focused on Iran and the Middle East, who is also a women's rights activist and was imprisoned in Iran for protesting the mandatory hijab before fleeing to Canada] [on 1 February 2023], to monitor its citizens in Canada, Iranian authorities use "phishing attacks" to gain information about a person. The source described an incident in which she was contacted via the professional networking site LinkedIn by "Iranian agents" who had "hacked" the account of an acquaintance and who then sent the analyst a weblink which "hacked" her email account and gained access to her passwords.'[152]

10.4.2 The same source also stated that: 'Authorities also monitor the "television and online activities" of its citizens abroad. Some individuals in Canada have had their family in Iran visited by authorities after they had participated in televised or online interviews; the lawyer reported having experienced this first-hand.'[153]

10.4.3 The USSD 2023 Country Report stated:

'… [I]n February [2023], Norwegian police warned that the Iranian regime had been engaging in digital surveillance of dissidents in Norway. The Head of Counterintelligence for the Norwegian Police Security Service Hanne Blomberg said Iranian authorities had been using the information obtained through cyberespionage to threaten, influence, and plot assassinations against dissidents. According to Blomberg, Iranian digital espionage involved hacking and gaining control of the mobile devices and computers of Iranians residing in Norway and infecting the devices with malware through malicious SMSs (texting) or emails.'[154]

10.4.4 On 18 June 2024, the German Federal Ministry of the Interior and Community (translated from German using Google Translate), published a report on the protection of its constitution, in which it stated: 'In 2023, Iranian cyber espionage in Germany mainly focused on the Iranian exile community in this country. Cyber attacks were characterised by sophisticated social engineering and the use of freely available malware that had been modified

[149] IRBC, … [A]nti-government activists … returning from abroad … (section 1.2), 22 April 2024
[150] EUAA, Iran – Country Focus (pages 25 and 109), 27 June 2024
[151] EUAA, Iran – Country Focus (page 63), 27 June 2024
[152] IRBC, Iran: Monitoring of Iranian citizens outside of Iran … (section 1.1), 2 March 2023
[153] IRBC, Iran: Monitoring of Iranian citizens outside of Iran … (section 1.1), 2 March 2023
[154] USSD, 2023 Country Reports on Human Rights Practices (page 27), 22 April 2024

for its specific purpose.'[155]

10.4.5 The July 2023 DFAT report noted that the adverse attention individuals may attract for repeatedly posting content online that is critical of the government, includes individuals based abroad[156]. The report also stated: 'Iranians with a public profile [see paragraph 8.4.4 for details] in Australia may also have their social media presence tracked by the Iranian government.'[157]

10.4.6 The Guardian's September 2023 article stated: 'Last month [August 2023], Germany's domestic intelligence agency issued a public warning about "concrete spying attempts" by … Iran-linked hacker group, Charming Kitten.'[158]

10.4.7 The Iran COI report, published by the BZ in September 2023, stated:

'… [T]here are indications that the Iranian intelligence services monitor opposition activities through social media and through individuals who work with them outside Iran. This can be concluded from the threats that Iranian political activists and journalists abroad receive by phone, email and/or on social media. These include threats to incarcerate members of the activist's family in Iran in Tehran's Evin prison unless they stop their activities.

'… A number of political activists and journalists abroad have been the target of cyber attacks. There are indications that their phone calls with their relatives in Iran are tapped.'[159]

10.4.8 The same COI report stated:

'According to various sources, it is not uncommon in Iran for a person to be convicted in absentia for activities abroad. This happens, for example, if someone abroad posts critical texts on social media. Several sources indicate that this has happened to well-known activists abroad. One example is Dubai-based former professional footballer Ali Karimi, who was convicted by the Iranian authorities after posting critical texts on his Instagram account in response to the death of Mahsa Amini.

'… An increasing number of reports have emerged of individuals being pressurised into providing the authorities with the passwords of their social media accounts. This gives the authorities access to social networks inside and outside Iran. In some cases, Iranians from the diaspora are asked to provide these passwords on arrival at an Iranian airport or on leaving Iran.'[160]

10.4.9 Wired, an American magazine which covers technology and its effect on society[161], published an article entitled 'The Scorched-Earth Tactics of Iran's Cyber Army' on 21 March 2023 which stated:

'Among the tactics used by the IRI's [Islamic Republic of Iran's] cyber agents - known colloquially as Cyberi - is old-school hacking. The Iran-linked hacker group Charming Kitten gained notoriety in 2020 for its spear-phishing

[155] Federal Ministry of the Interior and Community …, … 2023 Report … (page 63), 18 June 2024
[156] DFAT, DFAT Country Information Report Iran (paragraph 2.127), 24 July 2023
[157] DFAT, DFAT Country Information Report Iran (paragraph 2.128), 24 July 2023
[158] The Guardian, Iranian activists across Europe are targets …, 22 September 2023
[159] BZ, General Country of Origin Information Report on Iran (page 39), September 2023
[160] BZ, General Country of Origin Information Report … (pages 95 and 113 to 114), September 2023
[161] The Editors of Encyclopaedia Britannica, Wired, updated 4 February 2025

attempts on journalists, scholars, and policy experts in the West … [At the time of the articles writing] spear-phishing activities cyber groups TA453 and APT42, which are affiliated with the Iranian Revolutionary Guard Corps, have been increasingly prevalent …

'According to Amin Sabeti, founder of CERTFA [Computer Emergency Response Team in Farsi], a cybersecurity collective specializing in uncovering state-backed Iranian cyber activities, these operations have shifted their methods over the past few months, since most targets of interest are aware of the threat and have learned to protect themselves from spear-phishing. Instead, Sabeti says, they now use a "domino effect" strategy by taking aim at low-profile targets, whose credentials they harvest in order to build trust and gain access to higher-profile targets in their network. Early this month, for example, the Iranian Canadian human rights activist Nazanin Afshin Jam said that she received a spear-phishing link from a trusted colleague who had been hacked.'[162]

10.4.10 The EUAA Country Focus report stated: 'In an interview with EUAA, Barzoo Eliassi noted the presence of "a cyber army" … outside Iran, tasked to monitor opinions shared online.'[163]

10.4.11 The HRC detailed findings report noted that victims of the surveillance-ware, "BouldSpy", attributed to the National Police, include device users outside Iran[164].

10.4.12 The Mandiant report, which outlined 3 clusters of infrastructure used by the Iranian state-sponsored cyberespionage actor, APT42, to harvest credentials of those perceived as a threat to the Iranian regime and gain access to victim networks (see paragraph 8.4.13), stated of one of those clusters that: 'This effort was focused on targeting researchers and academia personnel in the U.S., Israel, and Europe.'[165]

10.4.13 The Freedom on the Net report, covering 1 June 2023 to 31 May 2024, noted that victims of cyberattacks by State hackers against activists and campaigners, include those in the diaspora[166].

10.4.14 The EUAA in its 17 October 2024 query response, citing its interview with Leila Alikarami on 24 September 2024 (see paragraph 10.2.5), stated:

'"… Ordinary Iranians are not systematically monitored unless they post sensitive content on social media, which could attract state interest. Not everyone is rigorously controlled at the airport. However, if an Iranian is arrested there for any reason, authorities will conduct an in-depth search of their computer and phone to review their online activities. Some Iranian activists have travelled to the country without being identified or arrested upon arrival at the airport. However, incidents have occurred where individuals posted something online while inside the country, revealing their presence and subsequently attracting attention from the authorities".'[167]

[162] Wired, The Scorched-Earth Tactics of Iran's Cyber Army, 21 March 2023
[163] EUAA, Iran – Country Focus (page 63), 27 June 2024
[164] HRC, Detailed findings of … mission (paragraph 1182), 19 March 2024, updated 8 July 2024
[165] Mandiant, Uncharmed: Untangling Iran's APT42 Operations, 1 May 2024
[166] Freedom House, Freedom on the Net 2024 (section C8), 16 October 2024
[167] EUAA, Iran; Human rights situation (Q72-2024) (page 22), 17 October 2024

10.4.15 An OHCHR press release dated 12 February 2025 stated:

> ‘The body of Sharmahd, who was reported to have died in custody in October 2024, has been released by Iran recently …
>
> ‘… Sharmahd, born in Iran, was a naturalised citizen of Germany and lived in the United States. He was a journalist and activist who had criticised the Government of Iran through his website.
>
> ‘In 2020, while transiting in the United Arab Emirates during a business trip, he was subjected to an “extraordinary rendition” by the Iranian authorities, who arrested him without a warrant.
>
> ‘… He was sentenced to death in 2023 for the capital offence of “corruption on Earth”, a sentence later confirmed by the Iranian Supreme Court.’[168]

Back to Contents

[168] OHCHR, … Experts deplore the death in custody of victim of arbitrary detention, 12 February 2025

# Research methodology

The country of origin information (COI) in this note has been carefully selected in accordance with the general principles of COI research as set out in the Common EU [European Union] Guidelines for Processing Country of Origin Information (COI), April 2008, and the Austrian Centre for Country of Origin and Asylum Research and Documentation's (ACCORD), Researching Country Origin Information – Training Manual, 2024. Namely, taking into account the COI's relevance, reliability, accuracy, balance, currency, transparency and traceability.

Sources and the information they provide are carefully considered before inclusion. Factors relevant to the assessment of the reliability of sources and information include:

- the motivation, purpose, knowledge and experience of the source
- how the information was obtained, including specific methodologies used
- the currency and detail of information
- whether the COI is consistent with and/or corroborated by other sources

Commentary may be provided on source(s) and information to help readers understand the meaning and limits of the COI.

Wherever possible, multiple sourcing is used and the COI compared to ensure that it is accurate and balanced, and provides a comprehensive and up-to-date picture of the issues relevant to this note at the time of publication.

The inclusion of a source is not, however, an endorsement of it or any view(s) expressed.

Each piece of information is referenced in a footnote.

Full details of all sources cited and consulted in compiling the note are listed alphabetically in the bibliography.

Back to Contents

# Terms of Reference

The ‘Terms of Reference’ (ToR) provides a broad outline of the issues relevant to the scope of this note and forms the basis for the country information.

The following topics were identified prior to drafting as relevant and on which research was undertaken:

- Legal context
- Cyber surveillance
    - Cyber police
    - Control and monitoring of online activity
    - Arrest and detentions
- Access to social media in Iran
    - Number of users
    - Social media platforms
- Sur place activities
    - state attitude and actions including
        - treatment of persons with a similar profile/activities in the country of origin
        - size, capacity and reach of the security services
        - size of the country’s missions in the UK and monitoring of diaspora
    - Treatment of people on return to the country of return, including those involved sur place activities

Back to Contents

# Bibliography

## Sources cited


Access Now,

About Us, no date. Accessed: 3 February 2025

Lives on hold: internet shutdowns in 2024, 23 February 2025. Accessed: 11 March 2025

Shrinking democracy, growing violence: internet shutdowns in 2023, 15 May 2024. Accessed: 3 February 2025

American Iranian Council (AIC),

History, no date. Accessed: 3 February 2025

Myth vs. Fact: Censorship in Iran, updated 30 January 2025. Accessed: 3 February 2025

Amnesty International,

Good news: Sareh Sedighi-Hamadani's death sentence overturned, 16 May 2023. Accessed: 28 March 2025

Iran: New compulsory veiling law intensifies oppression of women and girls, 10 December 2024, updated 17 December 2024. Accessed: 11 February 2025

Anvilogic, APT42's Cyber Tactics From Credential Theft to Election Interference, 22 August 2024. Accessed: 19 February 2025

AP News, US charges Iran Revolutionary Guard official in alleged plot to kill a human rights activist in NYC, 22 October 2024. Accessed: 18 February 2025

Article 19,

About us, no date. Accessed: 28 January 2025

Islamic Republic of Iran: Computer Crimes Law, 2012, Accessed: 5 February 2025

Tightening the Net: Iran's new phase of digital repression, 23 July 2024. Accessed: 3 February 2025

UK: Islamic Republic's oppression beyond borders risks journalists' lives, 21 February 2023. Accessed: 12 February 2025

Australian Department of Foreign Affairs and Trade (DFAT), [Iran] Country Information Report, 24 July 2023. Accessed: 17 February 2025

BBC News,

Iran: A really simple guide to the protests, 15 September 2023. Accessed: 3 March 2025

Iran frees Niloufar Hamedi and Elaheh Mohammadi, jailed for covering Mahsa Amini death, 14 January 2024. Accessed: 18 February 2025

Iranian rapper freed after death sentence overturned, 2 December 2024. Accessed: 3 March 2025

"Lashed for a social media photo" in Iran, 16 September 2024. Accessed: 14 February 2025

Reformist Masoud Pezeshkian elected Iran's president, 5 July 2024, updated 6 July 2024. Accessed: 10 February 2025

Cambridge Dictionary, Gen Z, no date. Accessed: 4 February 2025

Center for Human Rights in Iran (CHRI), Iran Ramps Up Violence and Repression Against Women and Girls Amid Regional Tensions, 17 April 2024. Accessed: 4 February 2025

Committee to Protect Journalists (CPJ),

Iran's parliament moves forward with troubling bill to further restrict internet, 1 November 2021. Accessed: 5 February 2025

Iran's seizure of detained journalists' devices raises fears of fresh arrests, convictions, 16 February 2023. Accessed: 11 February 2025

Madeline Earp, no date. Accessed: 5 February 2025

What We Do, no date. Accessed: 5 February 2025

DataReportal,

About, no date. Accessed: 26 February 2025

Digital 2024: Iran, 23 February 2024. Accessed: 26 February 2025

Ecoi.net, Friedrich-Ebert-Stiftung (FES), updated 1 December 2021. Accessed: 19 February 2025

European Union Agency for Asylum (EUAA),

Country Guidance: Iran; Common analysis and guidance note, January 2025. Accessed: 13 February 2025

Iran – Country Focus, 27 June 2024. Accessed: 13 February 2025

Iran; Human rights situation (Q72-2024), 17 October 2024. Accessed: 14 February 2025

Federal Ministry of the Interior and Community (Germany) (translated from German using Google Translate), Brief summary 2023 Report on the Protection of the Constitution, 18 June 2024. Accessed: 27 February 2025

Federal Office for Migration and Refugees (Germany) (BAMF),

Briefing Notes (KW06/2024), 5 February 2024. Accessed: 18 February 2025

Country Brief Iran - Grid Activities - Grid Monitoring, 20 December 2024. Accessed: 11 February 2025

Freedom House, Freedom on the Net, 16 October 2024. Accessed: 4 February 2025

Hengaw Organization for Human Rights (Hengaw),

About us, no date. Accessed: 20 February 2025

A detained protester has officially faced charges of Sāb Al-Nabi and Muhārebeh, 27 October 2023. Accessed: 20 February 2025

Human Rights Activists News Agency (HRANA), Journalist Hossein Jafarian

Sentenced to Imprisonment, 9 October 2024. Accessed: 20 February 2025

Immigration and Refugee Board of Canada (IRBC),

Iran: Monitoring of Iranian citizens outside of Iran, including political opponents and Christians, by Iranian authorities; monitoring of Iranian citizens in Canada; consequences upon return to Iran (2021–March 2023) [IRN201321.E], 2 March 2023. Accessed: 27 February 2025

Iran: Treatment by the authorities of anti-government activists, including those returning from abroad; treatment of individuals critical of the state response to the 2020 Ukraine International Airlines (UIA) Flight 752 (PS752) downing (2022–March 2024), 22 April 2024. Accessed: 27 February 2025

Iran Data Portal,

About Us, no date. Accessed: 28 January 2025

The Constitution of the Islamic Republic of Iran (English), approved by referendum on 2 and 3 December 1979, amended on 28 July 1989. Accessed: 28 January 2025

Iran Human Rights Documentation Center (IHRDC),

Mission, undated. Accessed: 28 January 2025

Restrictions on Freedom of Expression in the Islamic Republic of Iran, 25 March 2016. Accessed: 28 January 2025

Iranian Students' News Agency (ISNA), The government's plan to remove filtering does not mean abandoning cyberspace, 14 November 2024. Accessed: 4 February 2025

Iranian Students Polling Agency (ISPA), Iranian Students Polling Agency (ISPA), an Introduction, no date. Accessed: 5 February 2025

Iran International,

About Us, no date. Accessed: 19 February 2025

Iran Arrests Four Over Sharing Video Of Hijab Incident With IITV, 12 March 2024. Accessed: 5 February 2025

Iran Orders Social Media Influencers To Get Advertising License, 15 February 2024. Accessed: 5 February 2025

Iran Unleashes Cyber Campaign To Expose Dissident Accounts, 6 January 2024. Accessed: 4 February 2025

State-backed poll shows most Iranian students use foreign social media | Iran International, 17 October 2024. Accessed: 5 February 2025

100,000 Iranians use Starlink to defy internet curbs, 6 January 2025, updated 7 January 2025. Accessed: 7 February 2025

Iran News Update (INU),

About Us, 25 April 2013. Accessed: 4 February 2025

Iran's Regime Eases Internet Restrictions Amid Mounting Crises, 25 December 2024. Accessed: 4 February 2025

IranWire,

About IranWire, no date. Accessed: 4 February 2025

Crackdown on Diaspora Dissenters: Surge in Passport Seizures at Iranian Airports, 20 February 2024. Accessed: 3 March 2025

Iran Blocks Dozens of Social Media Accounts Amid Crackdown on Women, 23 April 2024. Accessed: 20 February 2025

Iranian Authorities Escalate Crackdown on VPNs, 20 February 2024. Accessed: 4 February 2025

Iranian Blogger Gets Suspended Prison Sentence, 6 December 2023. Accessed: 20 February 2025

IranWire Exclusive: Iran Systematically Targets Families of Arab Activists Abroad, 27 March 2024. Accessed: 3 March 2025

Two Men Hanged in Iran in Blasphemy Case Amid Surge in Executions, 8 May 2023. Accessed: 12 February 2025

Landinfo – Norwegian Country of Origin Information Centre, CGRS-CEDOCA – Office of the Commissioner General for Refugees and Stateless Persons (Belgium), COI unit, SEM – State Secretariat for Migration, Iran; Criminal procedures and documents, December 2021. Accessed: 10 February 2025

Lookout,

About Us, no date. Accessed: 13 February 2025

Lookout Discovers Android Spyware Tied to Iranian Police Targeting Minorities: BouldSpy, 27 April 2023. Accessed: 13 February 2025

Mandiant,

About Mandiant, no date. Accessed: 4 February 2025

Uncharmed: Untangling Iran's APT42 Operations, 1 May 2024. Accessed: 4 February 2025

Miaan Group, The Internet in the Women, Life, Freedom Era; Iran’s Progress in Censorship and Surveillance – and Options for European Policymakers (published by Friedrich-Ebert-Stiftung (FES)), June 2024. Accessed: 14 February 2025

National Iranian American Council (NIAC) Action,

Mission and Vision, no date. Accessed: 20 February 2025

Prominent Iranian Scholar Arrested Amid Stand Against Compulsory Hijab and Women’s Oppression, 20 March 2024. Accessed: 20 February 2025

Social media users who go viral given harsh prison sentences in Iran, 9 February 2023. Accessed: 3 March 2025

Netherlands Ministry of Foreign Affairs (BZ), General Country of Origin Information Report on Iran, September 2023. Accessed: 27 February 2025

New Lines Magazine,

Introducing New Lines, no date. Accessed: 11 February 2025

Tweeting Is Banned in Iran, but Not for the Regime’s Supporters, 5 September 2023. Accessed: 11 February 2025

Norton,

What is social engineering? Definition + protection tips, 20 July 2023. Accessed: 28 February 2025

Spear phishing: Definition + protection tips, 19 July 2023. Accessed: 28 February 2025

Office of the Commissioner General for Refugees and Stateless Persons (Belgium) (CGRS – CEDOCA), Iran; Treatment by the authorities of family members of dissidents residing abroad, 16 October 2024. Accessed: 3 March 2025

Project Ainita, About Project Ainita, 24 February 2012. Accessed: 6 February 2025

Radio Free Europe / Radio Liberty (RFE / RL),

About RFE/RL, no date. Accessed: 14 February 2025

Iran Cracks Down On Calls For Election Boycott, 29 February 2024. Accessed: 17 February 2025

Iranian Activist Sentenced To Death For Social Media Posts, 6 May 2024. Accessed: 17 February 2025

Iranian Authorities Ratchet Up Crackdown On Critics After Raisi's Death, 28 May 2024. Accessed: 17 February 2025

Iranian Blogger Detained After Posting Only A Period In Response To Ayatollah's Picture, 5 June 2024. Accessed: 14 February 2025

Iranian Retailer Digikala Charged Over Mugs Prosecutor Says “Insult” Islam, 9 February 2024. Accessed: 18 February 2025

Reporters Without Borders (RSF), “Watch out because we’re coming for you”: An RSF report on unprecedented transnational repression of Iranian journalists in the UK, 1 April 2024. Accessed: 27 February 2025

Reuters, Iran steps up internet crackdown one year after Mahsa Amini death, 14 September 2023. Accessed: 3 February 2025

Stovall, Jacob, and Wolter, Teagan, for Encyclopaedia Britannica, Doxing, updated 20 February 2025. Accessed: 3 March 2025

Switzerland – Federal Intelligence Service (FIS), Switzerland's Security 2023, June 2023. Accessed: 27 February 2025

Tehran E-commerce Association, Quality of Internet in Iran; Analytical Report on Disruptions, Restrictions, and Internet Speed in Iran (Third Report – Spring 2024), (published and translated into English by Project Ainita), 18 July 2024. Accessed: 6 February 2025

The Editors of Encyclopaedia Britannica, Wired, updated 4 February 2025. Accessed: 7 February 2025

The Guardian,

Australia foils Iran surveillance plot and vows to bring foreign interference “into the light”, 14 February 2023. Accessed: 3 March 2025

Iranian activists across Europe are targets of threats and harassment, 22 September 2023. Accessed: 27 February 2025

Iranian journalists celebrating release from jail charged for not wearing hijab, 15 January 2024. Accessed: 20 February 2025

"We live with a gun to our heads": how Iran is targeting protesters in Britain, 18 December 2023. Accessed: 3 March 2025

The Iran Primer,

Explainer: Tactics of Iranian Intelligence, 17 February 2023. Accessed: 12 February 2025

New "Protection" Bill on Internet Freedom, 23 February 2022. Accessed: 5 February 2025

Profiles: Iran's Intelligence Agencies, 5 April 2023. Accessed: 5 February 2025

The Washington Institute for Near East Policy (TWI),

About, no date. Accessed: 27 February 2025

Iranian External Operations, updated 25 February 2025. Accessed: 27 February 2025

Iranian External Operations in Europe: The Criminal Connection | The Washington Institute, 21 October 2024. Accessed: 27 February 2025

The Iran Primer: Power, Politics, and US Policy, 3 June 2013. Accessed: 28 March 2025

UN Human Rights Council (HRC),

Detailed findings of the independent international fact-finding mission on the Islamic Republic of Iran, 19 March 2024, updated 8 July 2024. Accessed: 11 February 2025

Report of the Independent International Fact-Finding Mission on the Islamic Republic of Iran, 2 February 2024. Accessed: 11 February 2025

UN Human Rights Office of the High Commissioner (OHCHR),

Iran: Experts deplore the death in custody of victim of arbitrary detention, 12 February 2025. Accessed: 3 March 2025

Iran: UN experts call for Hijab and Chastity law to be repealed, 13 December 2024. Accessed: 11 February 2025

Violence and threats against journalists reporting on Iran from abroad must stop, warn UN experts, 30 May 2024. Accessed: 14 February 2025

US Central Intelligence Agency (CIA) World Factbook, Iran, updated 5 February 2025. Accessed: 6 February 2025

US Department of the Treasury, Treasury Sanctions Individuals and Entities for Human Rights Abuses and Censorship in Iran, and Support to Sanctioned Weapons Proliferators, 12 January 2018. Accessed: 11 March 2025

US State Department (USSD), 2023 Country Reports on Human Rights Practices, 22 April 2024. Accessed: 5 February 2025

Wired, The Scorched-Earth Tactics of Iran's Cyber Army, 21 March 2023. Accessed: 28 February 2025

Worldcrunch, ISNA, no date. Accessed: 4 February 2025

Back to Contents

### Sources consulted but not cited

Amnesty International,

Iran: Draconian campaign to enforce compulsory veiling laws through surveillance and mass car confiscations, 6 March 2024. Accessed: 17 February 2025

The State of the World's Human Rights 2023, 24 April 2024. Accessed: 12 February 2025

Association for the Promotion of Open Society (APOS), "Siam", The Hidden Tool of the Islamic Republic for Suppressing Protests, 26 October 2024. Accessed: 20 February 2025

Austrian Centre for Country of Origin and Asylum Research and Documentation (ACCORD), Query response on Iran: Activities abroad that could lead to surveillance by Iranian authorities, consequences upon return (translated from German), 10 July 2024

BBC News, Iran charges journalists after BBC report on teen protester's death, 2 May 2024. Accessed: 17 February 2025

Cyberscoop, Iranian hackers impersonate journalists in social engineering campaign, 1 May 2024. Accessed: 7 February 2025

Euronews, Iran maintains block on WhatsApp and Instagram, 1 February 2023. Accessed: 3 February 2025

Federal Office for Migration and Refugees (Germany) (BAMF), Briefing Notes Summary, 31 December 2024. Accessed: 14 February 2025

FilterWatch,

A Cyber Power That Wasn't, no date. Accessed: 20 February 2025

Next-Generation Filtering; Phishing with Governable Templates Analytical, March 2024. Accessed: 20 February 2025

France 24, Iranian parliament to consider law targeting "celebrities" who defy hijab law, 28 July 2023. Accessed: 12 February 2025

Gadget News, Shocking report of the parliament on the statistics of the use of filter-breakers in Iran, 17 November 2023. Accessed: 14 February 2025

Gov.UK, UK sanctions, 28 August 2019, updated 10 October 2024. Accessed: 28 January 2025

Harwood-Baynes, Megan, for Sky News, #IraniansStandWithIsrael: Iran bans speaking out online in support of Israel – but it has not deterred some, 15 April 2024. Accessed: 4 February 2025

Human Rights Watch (HRW),

"We Will Find You" A Global Look at How Governments Repress Nationals Abroad, 22 February 2024. Accessed: 18 February 2025

World Report 2025, 17 January 2025. Accessed: 6 February 2025

Internet Governance Project (IGP), Caught in the Crossfire: The Impact of Sanctions on Iranian Internet Users, 22 October 2024. Accessed: 26 February 2025

Iran International,

Iranian Baluch Activist Killed Amid Ongoing Tensions, 16 March 2024. Accessed: 12 February 2025

US Codifies Sanctions Exemption to Help Iranians Access Internet, 18 May 2024. Accessed: 4 February 2025

IranWire, Iranian Journalist Sentenced for Instagram Posts, 10 October 2024. Accessed: 14 February 2025

MI5, Director General Ken McCallum gives latest threat update, 8 October 2024. Accessed: 27 February 2025

Office of the Commissioner General for Refugees and Stateless Persons (Belgium), COI unit (CGRS – CEDOCA), Iran; Surveillance of the diaspora by the Iranian authorities (translated from Dutch), 10 May 2023. Accessed: 21 February 2025

Radio Free Europe / Radio Liberty (RFE / RL),

Iran Blocks “Blind Date” As Part Of Social-Media Crackdown, 9 April 2024. Accessed: 20 February 2025

Iranian Cyberpolice To Ratchet Up Crackdown On Social Media Critics, 6 May 2024. Accessed: 7 February 2025

Iran Tries To Tighten Grip On Internet By Officially Outlawing VPN Use, 23 February 2024. Accessed: 18 February 2025

Suspects Who Published Video Of Hospital Fight Arrested In Iran, 12 March 2024. Accessed: 17 February 2025

Techloy, Iran is finally lifting its ban on foreign Internet platforms, updated 25 December 2024. Accessed: 4 February 2025

The Guardian, Iranian authorities plan to use facial recognition to enforce new hijab law, 5 September 2022. Accessed: 11 February 2025

United Against Nuclear Iran (UANI), Supreme Council of Cyberspace (SCC), no date. Accessed: 28 January 2025

US Department of the Treasury, Treasury Sanctions Senior Iranian Officials Overseeing Violent Protest Suppression and Censorship, 24 April 2023. Accessed: 29 January 2025

World Bank, Individuals using the Internet (% of population) – Iran, Islamic Rep., no date. Accessed: 6 February 2025

Back to Contents

# Version control and feedback

## Clearance

Below is information on when this note was cleared:

- version **2.0**
- valid from **2 April 2025**

---

**Official – sensitive: Not for disclosure – Start of section**

The information in this section has been removed as it is restricted for internal Home Office use.

**Official – sensitive: Not for disclosure – End of section**

---

Back to Contents

## Changes from last version of this note

Updated COI and assessment.

Back to Contents

## Feedback to the Home Office

Our goal is to provide accurate, reliable and up-to-date COI and clear guidance. We welcome feedback on how to improve our products. If you would like to comment on this note, please email the Country Policy and Information Team.

Back to Contents

## Independent Advisory Group on Country Information

The Independent Advisory Group on Country Information (IAGCI) was set up in March 2009 by the Independent Chief Inspector of Borders and Immigration to support them in reviewing the efficiency, effectiveness and consistency of approach of COI produced by the Home Office.

The IAGCI welcomes feedback on the Home Office's COI material. It is not the function of the IAGCI to endorse any Home Office material, procedures or policy. The IAGCI may be contacted at:

**Independent Advisory Group on Country Information**
Independent Chief Inspector of Borders and Immigration
1st Floor
Clive House
70 Petty France
London
SW1H 9EX
Email: chiefinspector@icibi.gov.uk

Information about the IAGCI's work and a list of the documents which have been reviewed by the IAGCI can be found on the Independent Chief Inspector's pages of the gov.uk website.

Back to Contents