LANDINFO

Utlendingsforvaltningens fagenhet for landinformasjon

Temanotat

Iran

Internett og sosiale medier

9. november 2022

Alle henvendelser om Landinfos rapporter kan rettes til:

Landinfo
Utlendingsforvaltningens fagenhet for landinformasjon

Fredrik Selmers vei 6
Postboks 2098 Vika
0125 Oslo
Tel: 23 30 94 70
E-post: landinfo@landinfo.no
www.landinfo.no

Om Landinfos temanotater

Utlendingsforvaltningens fagenhet for landinformasjon (Landinfo) innhenter og analyserer informasjon om samfunnsforhold og menneskerettigheter i land som Utlendingsdirektoratet (UDI), Utlendingsnemnda (UNE) og Justis- og beredskapsdepartementet har behov for kunnskap om.

Landinfos temanotater er basert på opplysninger fra nøye utvalgte kilder. Opplysningene er behandlet i henhold til anerkjente kvalitetskriterier for landinformasjon og Landinfos retningslinjer for kilde- og informasjonsanalyse.

Temanotatene bygger på både skriftlig og muntlig kildemateriale. En del av informasjonen som formidles, er innhentet gjennom samtaler med kilder på informasjonsinnhentingsreiser. Landinfo tilstreber bredde i kildetilfanget, og så langt mulig er det innhentet informasjon fra kilder som arbeider uavhengig av hverandre. Alt benyttet kildemateriale er fortløpende referert i temanotatene. Hensyn til enkelte kilders ønske om anonymitet er ivaretatt.

Notatene gir ikke et uttømmende bilde av temaene som undersøkes, men belyser problemstillinger som er relevante for UDIs og UNEs behandling av utlendingssaker.

Landinfo er en faglig uavhengig enhet, og informasjonen som presenteres, kan ikke tas til inntekt for et bestemt syn på hva praksis bør være i utlendingsforvaltningens behandling av søknader. Landinfos temanotater gir heller ikke uttrykk for norske myndigheters syn på de forhold og land som omtales.

About Landinfo's reports

The Norwegian Country of Origin Information Centre, Landinfo, is an independent body within the Norwegian Immigration Authorities. Landinfo provides country of origin information (COI) to the Norwegian Directorate of Immigration (Utlendingsdirektoratet – UDI), the Immigration Appeals Board (Utlendingsnemnda – UNE) and the Norwegian Ministry of Justice and Public Security.

Reports produced by Landinfo are based on information from carefully selected sources. The information is collected and analysed in accordance with common methodology for processing COI and Landinfo's internal guidelines on source and information analysis.

To ensure balanced reports, efforts are made to obtain information from a wide range of sources. Many of our reports draw on findings and interviews conducted on fact-finding missions. All sources used are referenced. Sources hesitant to provide information to be cited in a public report have retained anonymity.

The reports do not provide exhaustive overviews of topics or themes, but cover aspects relevant for the processing of asylum and residency cases.

Country of Origin Information presented in Landinfo's reports does not contain policy recommendations nor does it reflect official Norwegian views.

Summary

A large proportion of the Iranian population, at least 70 percent, are active Internet users. Since 2009, the Iranian authorities have spent considerable resources on developing infrastructure, but also on controlling its use. Censorship and surveillance are extensive. A cyber police has been established, and several other government agencies have tasks related to monitoring internet and social media. In addition, Iranian authorities have developed a local, state-controlled network, National Information Network (NIN).

Social media platforms and messaging tools such as Telegram, Twitter, Facebook, YouTube and Signal are blocked, but various "bypass tools" – applications such as VPN – are widespread. The regime-critical debate takes place largely on social media. For illegal opposition parties, internet is the preferred channel for information sharing.

Iranian authorities have a specific focus on people who may influence public opinion in Iran, such as those who have many followers on social media. This also applies to Iranians living abroad. Iranian journalists working for international media houses are closely monitored.

Sammendrag

En stor andel av den iranske befolkningen, minst 70 prosent, er aktive brukere av internett. Etter 2009 har iranske myndigheter brukt store ressurser på utbygging av infrastruktur, men også på å kontrollere bruken av internett. Sensur og overvåking er omfattende. Det er etablert et eget politi for datakriminalitet (cyber-police), og flere andre myndighetsorganer har oppgaver knyttet til overvåking av internett og sosiale medier. I tillegg har myndighetene etablert et lokalt, statskontrollert nettverk, National Information Network (NIN).

Sosiale medieplattformer og meldingstjenester som Telegram, Twitter, Facebook, YouTube og Signal er blokkerte, men ulike «omgåelsesverktøy» – som VPN-applikasjoner – er utbredt. Den regimekritiske debatten foregår i stor grad på sosiale medier. For ulovlige opposisjonspartier er internett den foretrukne kanalen for informasjonsdeling.

Iranske myndigheter har et særlig fokus på personer som kan påvirke opinionen i Iran, eksempelvis de som har mange følgere i sosiale medier. Det gjelder også iranere bosatt i utlandet. Iranske journalister som arbeider for internasjonale mediehus, blir nøye fulgt med på.

Innhold

1 Innledning 6

2 Iran og internett 7

2.1 Knekkpunktet var i 2009 7

2.2 Myndighetsorganer som utvikler og styrer internettpolitikken 8

2.2.1 Iranian Cyber Police (FATA) 9

2.2.2 Revolusjonsgarden (IRGC) og Ministeriet for etterretning 10

2.3 Utvikling av eget nett – National Information Network (NIN) 10

3 Tilgang til internett i dag 12

3.1 Sterk politisk kontroll 13

3.1.1 Politisk uro fører til nedstengning 13

3.1.2 Konsekvenser av sanksjonspolitikken 16

3.2 Utstrakt bruk av sensur og overvåking 17

3.2.1 Blokkering og filtrering 18

3.2.2 Cyberangrep og overvåking på internett 19

3.3 Kontrollen over cyberspace blir sterkere 22

4 Nytt lovforslag om ytterligere internettbegrensninger 22

4.1 Innholdet i lovforslaget 23

4.2 Potensielle konsekvenser dersom lovforslaget vedtas 23

5 Strategier for å unngå sensur og blokkeringer 25

5.1 Selvsensur 25

5.2 Bruk av omgåelsesverktøy som VPN 25

6 Bruk av sosiale medier og meldingstjenester 26

6.1 Særskilt om Telegram 28

6.2 Nettaktivitet som oppfattes som regimefiendtlig 29

6.2.1 De kurdiske partiene 29

6.2.2 Kristne konvertitter 30

7 Profiler av særlig interesse for myndighetene 31

7.1 Personer som kan påvirke opinionen i Iran 32

7.2 Iranere i utlandet 32

7.2.1 Iranske journalister i internasjonale medier 33

8 Arrestasjoner og domfellelser 34

8.1 Lovgivning som kan komme til anvendelse 34

8.2 Personer som straffeforfølges som følge av aktivitet på internett 36

9 Referanser 39

1 Innledning

Teknologien har de siste tiårene endret det iranske samfunnet og livet til store deler av den iranske befolkningen. Dette notatet beskriver utviklingen og bruk av internett og sosiale medier i Iran. Blant spørsmålene som belyses er disse:

- I hvilken grad er internett tilgjengelig for den iranske befolkningen?
- Hvordan overvåker og sanksjonerer myndighetene bruk av internett, og hvilke deler av myndighetsapparatet bedriver slik virksomhet?
- Hvilken profil har de nettbrukerne som kommer i myndighetenes søkelys?
- Hvilke konsekvenser kan ulovlig bruk av internett og sosiale medier ha for den enkelte bruker?
- I hvilken grad følger iranske myndigheter med på iranske borgeres digitale aktiviteter i utlandet?

Det er relativt mye tilgjengelig informasjon om utbredelsen av internett og bruk av sosiale medier i Iran. Notatet er ikke uttømmende, men beskriver temaer som antas å være relevante for utlendingsforvaltningen.

Internett og sosiale medier er i en rivende utvikling. Det er derfor lagt vekt på å benytte aktuelle kilder, med mindre det dreier seg om beskrivelse av historiske forhold. Informasjon som presenteres lener seg på kilder som antas å ha etterrettelig kunnskap om notatets tematikk. Notatet bygger i all hovedsak på åpne kilder som nyhetsartikler, akademiske artikler og rapporter fra organisasjoner som rapporterer særskilt om tilgang til og bruk av internett i ulike land, eksempelvis Freedom House. I tillegg har menneskerettighetsorganisasjoner som Article 19 og Center for Human Rights in Iran søkelys på ulike sider av den digitale utviklingen i Iran. Ingen av disse organisasjonene er fysisk til stede i Iran. Tilgangen til primærkilder, det vil si internettbrukere som oppholder seg i Iran, er derfor noe begrenset.

Det er vanskelig å tegne et eksakt bilde av den digitale overvåkingen og kontrollen som iranske myndigheter står bak. Det ligger i sakens natur at dette er virksomhet som foregår i det skjulte, og informasjon om virksomheten er verken verifiserbar eller etterprøvbar.

Teknisk informasjon om oppbygging av internett, i Iran og verden for øvrig, samt tekniske beskrivelser av hvordan nedstenging og sensur faktisk foregår, belyses ikke i notatet. Oppbyggingen av iransk forvaltning og rettsvesen er kompleks, og mange instanser er involvert i digitaliseringen av samfunnet. Et notat av dette format og omfang er ikke egnet til å belyse alle sider av dette, men beskriver hovedlinjene og de viktigste strukturene.

Første versjon av notatet ble publisert 31. mai 2021. Denne versjonen er oppdatert i tråd med utviklingen som har funnet sted etter dette, og inneholder nye informasjonsbiter vi anser som relevante. Blant annet har vi omtalt det nye lovforslaget om ytterligere internettbegrensning som er under utarbeidelse. Researchen til denne oppdateringen ble avsluttet i starten av november 2022. Protestene som startet i september samme år, var på det tidspunktet fortsatt pågående.

2 Iran og internett

Iranske myndigheter driver omfattende sensur og kontroll av borgernes internett-bruk. Freedom House-prosjektet *Freedom on the Net* analyserer hvorvidt internett er fritt tilgjengelig i en rekke land. Tre ulike kriterier kartlegges; tilgang, begrensninger på innhold og brukerrettigheter. Iran har lav score på kriteriene og internett-tilgangen betegnes som «not free» (Freedom House 2021).

FNs spesialrapportør for menneskerettigheter i Iran (UN Special Rapporteur 2021, s. 7; 2022, s. 10) uttrykker bekymring for myndighetenes gjentatte forstyrrelser av telekommunikasjonen. Rapportøren peker på at nedstenging av internett og blokkering av nettsteder og applikasjoner representerer brudd på iranernes rett til ytringsfrihet. Han uttrykker videre bekymring for at sosiale medieplattformer som Telegram, Twitter, Facebook og YouTube er blokkert.

2.1 Knekkpunktet var i 2009

Myndighetenes holdning til internett endret seg etter presidentvalget i 2009. Før den tid hadde iranske myndigheter i liten grad fokus på internett, og de hadde liten forståelse for hvilken politisk kraft som kunne ligge i digitale medier. Den iranske befolkningen er høyt utdannet, og i 2009 var om lag en tredjedel av befolkningen brukere av internett. Hele to tredjedeler av befolkningen brukte også smarttelefon. På tross av at mange iranere var aktive brukere av internett og sosiale medier, anså myndighetene dette å være uten særlig risiko (Ehlson et al. 2012, s. 11).

Den konservative kandidaten Mahmoud Ahmadinejad ble i juni 2009 utropt til vinner av presidentvalget. Mange iranere bestred valgresultatet og flere millioner gikk ut i gatene for å protestere. Hossein Mousavi, kandidaten som utfordret Ahmadinejad, valgte grønn som farge til kampanjen sin. Demonstrasjonene ble betegnet som «den grønne bevegelsen». Internett og sosiale medier, særlig Twitter og Facebook, var viktige plattformer i mobiliseringen av protestene, og for å spre nyheter om protestene til utlandet (Ehlson et al. 2012; Small Media 2017, s. 8).

I 2010 ble det iranske anlegget for anrikelse av uran utsatt for et avansert datavirus, Stuxnet. Viruset utnyttet sikkerhetshull i Windows til å angripe

industrielle installasjoner. Angrepet, som det antas at USA og Israel sto bak, påførte det iranske anlegget enorme skader. Det bidro til at iranske myndigheter erkjente hvilket skadepotensial og sårbarhet som bruk av digitale nettverk innebærer (Bekkevang 2017, s. 14; Gilbrant 2010).

Etter 2009/2010 har myndighetene fått større fokus på internett og sosiale medier, men også på IT-sikkerhet og offensiv cyberevne generelt. Mange sosiale plattformer, herunder Twitter og Facebook, ble forbudt i kjølvannet av 2009-protestene. Overvåking, sensur og kontroll har blitt mye sterkere etter 2009 (Ehlson et al. 2012; Gilbrant 2010).

2.2 Myndighetsorganer som utvikler og styrer internettpolitikken

Øverste leder, Ayatollah Ali Khamenei, frykter internett og den vestlige innflytelsen internett representerer. Han mener at internett kan undergrave Den islamske republikken. Khamenei har derfor forsøkt å sentralisere kontrollen over landets internettpolitikk under egen myndighet (CHRI 2018b, s. 18).

Informasjons- og kommunikasjonsteknologien (IKT) er kontrollert av myndighetene, både gjennom direkte eierskap og politisk kontroll (Article 19 2020, s. 23; Freedom House 2021). På bakgrunn av et dekret etablerte øverste leder i 2012 et råd – Supreme Council of Cyberspace (SCC). Rådet har 27 medlemmer og spiller en viktig rolle ved at det meisler ut strategien på dette politikkområdet. De er ansvarlig for utvikling av generelle retningslinjer for styring av cyberspace (CHRI 2018b, s. 18).

SCC ledes av landets president, men består i stor grad av medlemmer som Øverste leder har håndplukket. Ifølge Center for Human Rights in Iran (CHRI 2018b, s. 18) innebærer dette at presidenten og representanter for hans kabinett bare spiller en beskjeden rolle. Under valgkampen forut for presidentvalget i 2017 lovet forhenværende president Hassan Rouhani å beskytte iranernes tilgang til det globale internettet. Rouhani var ikke i stand til å innfri løftet. Det er i stor grad de konservative kreftene, de såkalte «hardlinerne», som har styrt myndighetenes håndtering av internett (CHRI 2018b, s. 8; Freedom House 2020, s. 10). Nåværende president Ebrahim Raisi regnes som en hardliner som har strengere regulering av internett høyt på dagsorden (Al-Monitor 2021b; diplomatkilde, e-post november 2021).

Slik Landinfo forstår det, har CCDOC (Committee Charged with Determining Offensive Content) ansvar for å ta avgjørelser om hva som regnes som ulovlig innhold på nett, basert på de generelle retningslinjene utarbeidet av SCC. Komitéen er bredt sammensatt; en rekke ministerier, sikkerhetsmyndighetene, men også den statlige kringkastingen IRIB (Islamic Republic of Iran Broadcasting) er representert. CCDOC utarbeider oversikter over nettsteder som skal filtreres eller blokkeres, og kommuniser dette til relevante myndigheter for

implementering (Article 19 2017, s. 19). Freedom House (2021) understreker at slike beslutninger ofte er vilkårlige, og at det foreligger lite informasjon om beslutninger og prosesser i komiteen. Det er flere myndighetsorganer som kan beslutte blokkering eller filtrering uten at CCDOC har vært involvert (Article 19 2017, s. 19-20; Freedom House 2021).

Grunnlovens artikkel 175 forbyr privat kringkasting. Iranske myndigheter har monopol over alle TV- og radiosendingsanlegg gjennom IRIB. Telecommunication Company of Iran (TCI), som eies av Revolusjonsgarden (IRGC),[1] styrer all internett-trafikk inn og ut av landet (DFAT 2020, s. 44; U.S. Department of State 2022, s. 33-34).

2.2.1 Iranian Cyber Police (FATA)

Som ledd i arbeidet med å styrke kontrollen over internett, fikk Iran i januar 2011 en egen avdeling innen politiet som skulle forebygge og etterforske data-kriminalitet – Iranian Cyber Police (FATA) (Article 19 2020, s. 9). Det er relativt lite tilgjengelig informasjon om FATA; både om hvordan de opererer, og hvilke metoder de benytter.

FATA skal bekjempe cyberkriminalitet og slå ned på nettbasert kritikk mot staten. Avdelingen følger med på og sporer nettaktivister, og disse kan utsettes for trakassering eller bli arrestert. En annen målgruppe er personer som utvikler og selger VPN-løsninger (Landinfo, CGRS & SEM 2021, s. 20).

Ifølge Small Media (u.å.) har om lag 42 000 frivillige tilknytning til FATA. Mannskapet ser ut til å være ungdommer med gode digitale ferdigheter, og som har fått opplæring innen etterretning og overvåking. En viktig del av opplæringen er å ikke etterlate spor som kan koble virksomheten til sikkerhetstjenestene. Samtidig er dette et prioritert område for myndighetene, og de som tjenestegjør har myndighetenes støtte og opererer under stor grad av immunitet (Article 19 2017, s. 6).

I oktober 2018 opplyste lederen for FATA, Seyyed Kamal Hadiyanfar, at de hadde hatt mer enn 133 000 saker og hadde arrestert nesten 75 000 personer for nettaktivitet siden 2010. Ifølge Small Media brukes det høye antallet arrestasjoner i en kampanje for å skape frykt blant iranske nettbrukere og underbygge narrativet om FATAs evne til å overvåke sosiale medier i stor skala (Small Media u.å.).

Likevel er det, med enkelte få unntak, lite offentlig oppmerksomhet om enkeltsaker. Det er lite tilgjengelig informasjon om hva som skjer med internett-brukere som har blitt arrestert av FATA, om de får juridisk bistand og hvilken

[1] Irans revolusjonsgarde – Islamic Revolutionary Guard Corps – ble opprettet i 1979 for å forsvare revolusjonen. Revolusjonsgraden rapporterer til Øverste leder.

eventuell straff som idømmes (Small Media u.å.).

2.2.2 Revolusjonsgarden (IRGC) og Ministeriet for etterretning

Flere andre myndighetsorganer har også oppgaver knyttet til overvåking av internett og sosiale medier. Generelt foreligger det imidlertid lite konkret informasjon om struktur, oppgavefordeling og organisering av kontroll og overvåking av internett og sosiale medier.

Ifølge kilder som Article 19 (2017, s. 8) har konsultert, spiller både IRGC og Ministeriet for etterretning (*Ettelaat*) en viktig rolle. Center to Investigate Organised Crimes (CIOC) arresterer og forhører aktivister tilknyttet sivilsamfunnet eller politiske miljøer. Hensikten skal være å forebygge terrorhandlinger, kriminalitet samt regimekritisk og ulovlig politisk virksomhet. CIOC er tilknyttet IRGCs Cyber Defense Command. Videre har den frivillige paramilitære styrken Basij, under IRGCs ledelse, en rolle i å overvåke aktivitet på internett (Article 19 2017, s. 8).

Disse har til dels overlappende oppgaver med FATA, men fokuset er forskjellig. Alle enhetene overvåker internett og sosiale medier, og har fokus på både enkeltpersoner og organisasjoner. Ifølge en iransk jurist (digitalt møte 2021) har imidlertid IRGC fokus på nasjonal sikkerhet og aktivitet som utfordrer regimet. De har en målrettet innsats rettet mot høyt profilerte aktivister eller utenlandske enheter (Small Media u.å.). Den iranske juristen (digitalt møte 2021) mener det er rimelig å anta at kristen og misjonerende aktivitet på sosiale medier er innenfor IRGCs mandat, fordi det dreier seg om regimets integritet. FATA, derimot, har fokus på aktiviteten til vanlige iranere på sosiale medier, eksempelvis innlegg med «happy dancing» på taket, spill eller gambling i liten skala. Dette er gjerne profiler som ikke får nasjonal eller internasjonal mediedekning. Ifølge Small Media (u.å.) kan det være en av årsakene til at det er relativt liten oppmerksomhet knyttet til FATA og deres virksomhet.

2.3 Utvikling av eget nett – National Information Network (NIN)

Iranske myndigheter erkjente tidlig at en universell blokkering av tilgangen til internett hadde store økonomiske kostnader og ville føre til betydelig misnøye i befolkningen. Det var en pris som regimet ikke var villig til å betale. En strategi fra myndighetenes side for å bedre kontrollen over internettbruken, ble derfor å få iranske borgere over på et eget nett, på folkemunne kalt «Halal Internet» (MacLellan 2018). SHOMA er en annen betegnelse som hyppig benyttes om det lokale nettet (Freedom House 2020).

Tidligere høgskolelektor i cybersikkerhet ved Institutt for forsvarsstudier (IFS) Bjørn Svenungsen (mai 2021) forklarte at National Information Network (NIN) kan sammenlignes med et «intranett» for hele Iran. Det er et egnet verktøy til å

overvåke iranernes nettbruk, og iverksette tiltak som eksempelvis hel eller delvis nedstengning. Stuxnet-angrepet i 2010 var antagelig en medvirkende årsak til beslutningen om å utvikle NIN.

Myndighetene markedsfører NIN som et «raskere, sikrere og billigere nett». Ved å styrke lokale plattformer og utarbeide gode, tekniske løsninger forsøker myndighetene å presse iranerne over på NIN hvor sensur og overvåkning er enklere å gjennomføre. Den formelle lanseringen var 28. august 2016, men iranske myndigheter jobber fortsatt med å utvikle systemet (CHRI 2018b, s. 34; Freedom House 2021; diplomatkilde, e-post november 2022). NIN er et statskontrollert nettverk med søkemotor og e-posttjenester. Det er mulig å gjennomføre bank- og handelstransaksjoner, og få tilgang til innhold produsert i Iran uten å bruke internasjonale tjenester. NIN gjør det mulig for myndighetene å skille mellom internasjonal og nasjonal internett-trafikk. For å få tilgang til det globale nettet, må iranere gå gjennom NIN. Dermed gis myndighetene mulighet til å stenge tilgangen til det globale internettet, men holde det nasjonale nettet helt eller delvis åpent (CHRI 2018b, s. 26-27; Freedom House 2021).

Sanksjonene mot Iran brukes av iranske myndigheter som et argument for den sterke kontrollen og utviklingen av et eget nett. Angivelig skal det lokale nettet bidra til å redusere den iranske sårbarheten overfor USA. NIN anses å være en strategi for å stoppe spredning av vestlig kultur og innflytelse på internett, men det er også et verktøy for økt overvåking av innhold av uønsket politisk, kulturell og religiøs karakter. Iran's Telecommunications Company, som eies av IRGC, har en sentral rolle i utviklingen av NIN (Article 19 2020, s. 23-25; CHRI 2018b, s. 20, 27). Et eksempel på at myndighetene har større kontroll på det nasjonale nettet, er at man må registrere seg med navn og telefonnummer på alle applikasjoner (diplomatkilde, e-post november 2022).

For å gjøre det mer attraktivt å benytte det lokale nettet, brukes statlige subsidier for at det skal være betydelig billigere å surfe på de lokale serverne. I tillegg er hastigheten økt markant. På tross av massiv markedsføring og innsats fra iranske myndigheters side, viser statistikk at det er de utenlandske plattformene som fortsatt er de mest brukte blant iranere (Article 19 2020, s. 23-25; CHRI 2018b, s. 27).

Ifølge en rapport fra IKT-ministeriet[2] var 80 prosent av infrastrukturen for NIN fullført i august 2019. I byene var dekningen hundre prosent, mens på landsbygda hadde 78 prosent fått tilgang til nettverket (Article 19 2020, s. 23; Freedom House 2020). Ifølge Freedom House er det uenighet mellom IKT-ministeriet og SCC om andelen som har tilgang, noe som muligens bunner i ulike definisjoner av NIN. Akkurat hvor langt utbyggingen av NIN har kommet, er derfor ikke kjent (Freedom House 2021).

[2] IKT er en forkortelse for informasjons- og kommunikasjonsteknologi.

3 Tilgang til internett i dag

Generelt er det vanskelig å anslå hvor stor andel av en befolkning som benytter internett og hva de ulike estimatene bygger på – om det er selvrapportering eller annet grunnlag. Center for Human Rights in Iran (CHRI 2018b, s. 7) pekte i 2018 på at internettbruken i Iran hadde økt voldsomt. Iran er et av landene i Midtøsten med flest internettbrukere, og mange bruker det også i jobbsammenheng. Tall fra Article 19 viser at 57,4 millioner av en befolkning på 82 millioner brukte internett i 2020, hvilket utgjør en andel på om lag 70 prosent (Article 19 2020, s. 13). Andre kilder hevder at tallet kan være høyere (Dagres 2022, s. 4). Basert på tall fra Statistical Centre of Iran, oppga den Internasjonale Telekommunikasjons-unionen (2020) at rundt 84 prosent av befolkningen brukte internett i 2020.

SCC er ambisiøs når det gjelder utbygging av infrastruktur. I februar 2020 var det uttalte fem-års målet at hele befolkningen skulle ha tilgang til mobilt internett, og at fire av fem iranere skulle ha tilgang gjennom bredbånd (Freedom House 2021).

Iranske myndigheter satser med andre ord tungt på utbygging av landsomfattende infrastruktur for IKT. Ifølge tall fra IKT-ministeriet var det i 2019 installert 240 000 km fiberoptiske kabler over hele landet. Som følge av dette har forekomsten av bredbånd og hastighet økt betydelig de siste årene (Freedom House 2021).

De fleste iranere bruker mobilnettet for å få tilgang til internett. Tall fra mai 2022 viser at medianhastigheten for nedlasting var på 26,10 Mbps for bredbånd og 10,34 Mbps for mobilnett (Freedom House 2021, 2022). Hastigheten er avhengig av tjenesteleverandør, hvor du befinner deg og hvor mye du betaler (diplomatkilde, e-post mai og november 2022).

Det er de fattigste, bosatt i rurale strøk, som ikke har blitt med på den digitale utviklingen. Etter at myndighetene erkjente alvoret i korona-pandemien, ble skoler og universiteter stengt, og elevene ble henvist til digital undervisning. En lærer som jobber i et fattig nabolag, opplyste at han ikke var i stand til å komme i kontakt med to tredjedeler av elevene sine. Det handler delvis om at det ikke er internettdekning i alle deler av landet, men det dreier seg også om pris. Ifølge en lærer koster bredbåndstilknytning om lag 9 euro i måneden. Dekning av internett vil dermed tilsvare 8 prosent av en minimumslønn på 110 euro (Ershad 2020). [3]

Iransk statsforvaltning har relativt gode systemer når det gjelder administrasjon, registre og dokumentutstedelse. Ulike offentlige tjenester har blitt digitalisert (Landinfo 2020, s. 10). Det nasjonale ID-kortet *kart-e melli* er et elektronisk smartkort med databrikke. Databrikken inneholder elektronisk lagret foto,

[3] Dette tallet er sannsynligvis mye høyere i dag, ettersom iranske internettleverandører økte prisene med mellom 60 og 100 prosent i april 2022 (Freedom House 2022).

fingeravtrykk og signatur. Kortet utleveres med PIN-koder som gir innehaveren tilgang til offentlige tjenester via internett (Landinfo 2021a, s. 20-23).

Visum til Iran utstedes elektronisk og visumsøkeren får ikke lengre stempel eller visumsticker i passet. Iransk grensekontroll har tilgang til visumet gjennom et digitalt e-visumsystem (Nasjonalt ID-senter, e-post 2021).

Også rettsapparatet er i stor grad digitalisert. Nye juridiske saker registreres via portalen AdlIran, og her loggføres utviklingen i saken. Det er etablert egne kontorer over hele landet som bistår personer som ikke har tilgang til internett, eller har datamaskin. Likevel brukes det papirbaserte systemet fremdeles, særlig i rurale strøk, av hensyn til den delen av befolkningen som ikke har tilgang til internett. Unntatt fra AdlIran er enkelte høyprofilerte saker som går for Revolusjonsdomstolen (iransk jurist, e-post 2021).

3.1 Sterk politisk kontroll

Myndighetene har kontroll over sentral infrastruktur, men også sterk kontroll over aktørene i markedet. De legger til rette for befolkningens internettbruk ved å bygge ut infrastruktur og øke hastigheten. Samtidig har kontrollen over bruken økt betydelig. Miaan Group er spesialisert på digital sikkerhet i Midtøsten. Ifølge direktør Amir Rashidi (som gjengitt i Bergman & Fassihi 2020) blir Iran stadig mer aggressive i kontrollen av internett, både når det gjelder sensur, overvåking og hacking. Nettsteder for nasjonale nyhetsmedier, nyhetsbyråer og andre aktører risikerer sensur, sanksjoner og i verste fall nedleggelse eller blokkering (Article 19 2020, s. 13).

Iranske myndigheter må balansere ulike hensyn; det er viktig for store deler av den iranske befolkningen å ha tilgang til internett. Samtidig er det viktig for regimet at internett ikke skal kunne brukes som et kraftfullt verktøy for den politiske opposisjonen.

3.1.1 Politisk uro fører til nedstengning

Myndighetene har de seneste årene benyttet delvis eller total nedstengning av internett ved store demonstrasjoner og sosial uro. Taktikken og omfanget av nedstengningene varierer. Sett fra iranske myndigheters ståsted, dreier dette seg om sikkerhet, og det er SNSC (Supreme National Security Council)[4] som tar beslutninger om nedstengning. I og med at Telecommunication Company of Iran (TCI) styrer all internett-trafikk, har myndighetene verktøyet som trengs for å

[4] SNSC er hjemlet i Grunnlovens artikkel 176. Rådet ble etablert i 1989 og er under Øverste leders kontroll. Deres mandat er forsvar, sikkerhet og utenrikspolitikk (Article 19 2020, s. 11; Constitution of Iran 1979).

kutte befolkningens tilgang til internett i perioder med protester og uro (Article 19 2020, s. 39).

Ved midnatt 15. november 2019 varslet myndighetene at prisene på drivstoff skulle økes; 50 prosent prisøkning på rasjonert drivstoff og 300 prosent økning for drivstoff på det frie markedet. Dette utløste store demonstrasjoner. Mange sivile ble drept under protestene; 304 personer er bekreftet drept, men uavhengige kilder hevder at det reelle antallet er mye høyere (Danish Immigration Service 2020, s. 8).

Iranske myndigheter svarte på protestene med å stenge ned internett. Beslutningen om å stenge internett-tilgangen ble gjort av SNSC, som først vedtok en 24-timers nedstenging, som senere ble utvidet (Article 19 2020, s. 17; Freedom House 2020). Brukerne av internett ble ikke forhåndsvarslet om nedstengningen, og parlamentet var ikke involvert i beslutningen. Internettleverandørene[5] – som er under myndighetenes kontroll – ble pålagt å kutte brukernes tilgang. Tilgangen til uavhengige nasjonale og utenlandske nyhetssider, sosiale medier og kommunikasjonsplattformer, men også Instagram ble stengt. Nedstengningen gjaldt både bredbånd og mobilnettet. Det var en tilnærmet total nedstengning i seks dager, men full internett-tilgang var ikke tilbake før 27. november (Article 19 2020, s. 17; Freedom House 2020; NetBlocks 2019).

Både før og etter november 2019 har internett og sosiale medier blitt benyttet for å mobilisere til protester og spre informasjon om det som skjer, med påfølgende nedstengning fra myndighetene. Da det brøt ut store demonstrasjoner i forbindelse med at 22 år gamle Mahsa Amini døde etter å ha blitt arrestert av moralpolitiet i september 2022, svarte iranske myndigheter med å begrense internettilgangen. Det ble rapportert om forstyrrelser på store tjenester som Instagram og Whatsapp som gjorde tjenestene vanskelige eller umulig å bruke (Al Jazeera 2022).

I 2021 og i mai 2022 gjennomførte myndighetene flere lokale nedstengninger i forbindelse med protester i provinsene Khuzestan og Sistan og Baluchestan (Dagres 2022; Filterwatch 2021; Rashidi 2022a). I januar 2020, da Iran ved en feiltakelse skjøt ned et ukrainsk passasjerfly, var det store demonstrasjoner som førte til nedstengning av internett (Freedom House 2020). I desember 2017 og etter årsskiftet i 2018 var det protester og opptøyer i mange store byer. Myndighetene svarte med å blokkere tilgangen til Telegram og tilgangen til Instagram var sterkt redusert i perioder (Frenkel 2018).

[5] Såkalte ISP; Internet Service Providers.

Myndighetene oppnår flere ting med å stenge eller begrense tilgangen til internett (Article 19 2020, s. 17; MacLellan 2018):

- Mobilisering blir vanskeligere i og med at sosiale medier og meldings-applikasjoner stenges ned.
- Volden og omfanget av demonstrasjonen kan ikke dokumenteres.
- Omverden får ikke innsyn i hva som skjer i landet. Dokumentasjon som bilder og videoer kan ikke lastes opp.
- Det blir lettere for staten å kontrollere narrativet om demonstrasjonene. Ved store mobiliseringer har det ofte kommet motstridende rapporter om hva som faktisk skjer.

Myndighetene benytter total nedstengning kun i situasjoner som de anser å være særlig utfordrende, og tidsmessig begrenses nedstengningen til et minimum. Prisen for nedstengning kan være høy; den har både en økonomisk kostnad ved at handel og økonomiske transaksjoner stopper opp, og mulighet for kommunikasjon med forretningsforbindelser og forsyningskjeder stenges. Nedstenging kan også påvirke kritiske tjenester til befolkningen, eksempelvis tilgangen til helsetjenester, banktjenester og liknende. Myndighetene kan imidlertid unnlate å blokkere NIN, og på den måten opprettholdes offentlige tjenester og kritiske tjenester som blant annet sykehusnettverk og banktjenester, og kontroll av luftfart og skipsfart. Dermed blir landet mindre sårbart og prisen for nedstengningen mindre, samt at det blir lettere for myndighetene å overvåke innbyggerne (Article 19 2020, s. 14; Svenungsen 2021).

Under demonstrasjonene i 2019 ble tilgangen til det globale internettet i hovedsak stengt ned, men myndighetene beholdt tilgangen til noen tjenester på det nasjonale nettet. På den bakgrunn benekter myndighetene at en «shutdown» fant sted, fordi iranere delvis hadde tilgang til tjenester på det nasjonale nettet (Article 19 2020, s. 4, 12, 17; Freedom House 2020). Under demonstrasjonene høsten 2022 valgte myndighetene heller å begrense tilgangen til spesifikke tjenester som blir brukt av mange, og å gjennomføre lokale nedstengninger. Dette til forskjell fra den totale nasjonale nedstengningen i november 2019 (Rashidi 2022b).

Nyhetsnettstedet The Intercept avslørte i oktober 2022 detaljer om en program-vare som blant annet lar myndighetene begrense mobilbrukeres datahastighet (såkalt *throttling*). Videre kan myndighetene følge med på hvor mobilbrukeren befinner seg og hente ut informasjon om mobileierens navn, adresse og ID-nummer. Informasjonen fra Intercept var basert på lekkede dokumenter (Biddle & Hussain 2022). Nettstedet Filterwatch jobber for å spre informasjon om iransk internettpolitikk og de menneskerettslige konsekvensene, og følger situasjonen nøye. Filterwatch påpeker at det finnes eksempler på at personer som har befunnet seg i geografisk nærhet til demonstrasjoner, har fått tilsendt sms-er fra

myndighetene som advarer mottakeren mot å delta i protestene (Filterwatch 2022c).

I forbindelse med demonstrasjonene i september 2022 annonserte SpaceX-grunnlegger Elon Musk at han hadde gjort selskapets satellitt-baserte internettjeneste Starlink tilgjengelig for iranerne. Selv om denne tjenesten i teorien kan gi tilgang til internett selv under nedstengninger, anses det i praksis ikke som et alternativ ennå. Dette er en tjeneste som krever innførsel og installering av infrastruktur, noe man antar iranske myndigheter ikke vil godta, og som i tillegg vanskeliggjøres av sanksjoner og handelsblokade (Motamedi 2022b; Newman 2022).

3.1.2 Konsekvenser av sanksjonspolitikken

I 2015 inngikk landene i FNs sikkerhetsråd og EU en avtale – Joint Comprehensive Plan of Action – med Iran. Ifølge den såkalte atomavtalen skulle sanksjonene som var innført mot Iran opphøre. Til gjengjeld skulle Iran tillate innsyn i, og begrense omfanget av deres kjernefysiske program. I mai 2018 valgte Trump-administrasjonen å bryte avtalen og gjeninnføre sanksjoner mot landet. Dette på tross av at Det internasjonale atomenergibyrået (IAEA) hevdet at Iran overholdt sin del av avtalen. Andre vestlige land ønsket å opprettholde avtalen, men trakk etter hvert selskapene sine ut av Iran da Trump truet med handelsboikott (Bratberg & Raake 2021).

Ifølge ekspert på IKT og sikkerhet Amir Rashidi (som gjengitt i CHRI 2021b) bidrar sanksjonspolitikken til at teknologiselskaper som tilbyr internettrelaterte produkter, frykter amerikanske sanksjoner. Derfor selger ikke selskapene produkter, tjenester eller apper til iranere. Dette fører til at iranere blir prisgitt nasjonal infrastruktur; befolkningen henvises til å bruke iranske kommunikasjons-verktøy og tjenester. Blant annet må iranere laste ned apper med den lokale «app-store» Cafe Bazaar som registrerer hva som er på telefonen. Dermed blir brukeren mer eksponert for myndighetenes overvåking og kontroll. Dette utgjør en betydelig digital sikkerhetsrisiko, særlig for de som tilhører den politiske opposisjonen og aktivistmiljøer (Article 19 2020, s. 26; CHRI 2021b).

Det ville, ifølge Rashidi, innebære store fremskritt for iranernes digitale sikkerhet hvis eksempelvis Google hadde gitt iranere tilgang til tjenester og verktøy på operativsystemet Android. Det samme gjelder Apple-tjenester. For å bruke Apple-applikasjoner, må brukeren opprette en Apple-ID. For å opprette en slik ID, må telefonnummer oppgis, men iranske telefonnummer godtas ikke (CHRI 2021b).

Blokkering og filtrering kan omgås ved bruk av tekniske løsninger (se 5.2.). En del slike verktøy kan derimot ikke brukes i Iran, ettersom de er avhengige av tjenester som ikke er tilgjengelige på grunn av sanksjonspolitikken mot landet, som for eksempel Amazon Cloud og Google Cloud (Article 19 2020, s. 26).

I september 2022 annonserte det amerikanske finansdepartementet at de utvidet unntakene for sanksjonene mot Iran. Det vil si at amerikanske teknologiselskaper nå kan tilby iranerne tjenester som sosiale media-plattformer, samarbeidsverktøy og VPN-programmer, samt skytjenester som disse er avhengige av (CHRI 2022a; U.S. Department of the Treasury 2022). En diplomatkilde opplyste i november 2022 at lettelsene har hatt effekt. Blant annet har VPN-tjenesten EkspressVPN blitt mer tilgjengelig.

3.2 Utstrakt bruk av sensur og overvåking

I tillegg til nedstenging har myndighetene en rekke andre verktøy de kan benytte. Sensur og overvåking kan ha ulike uttrykk i Iran, og begrunnes ut fra ulike hensyn. Et hensyn er myndighetenes ønske om å skjerme borgerne mot utenlandsk og vestlig påvirkning. Et annet viktig hensyn er å hindre regimefiendtlig aktivitet (MacLellan 2018).

En annen grunn til overvåking kan være motivert av utsiktene til å få tilgang til verdifull informasjon. Daværende fiskeriminister Per Sandberg var sommeren 2018 på et privat besøk til Iran. Besøket fikk stor oppmerksomhet av flere grunner. En av grunnene var at Sandberg hadde med egen tjenestetelefon på reisen. PST konkluderte med at det var «sannsynlig» at dette hadde gitt iranske etterretningstjenester informasjon. Ifølge PST må det legges til grunn at all kommunikasjon, både tale og datatrafikk, til og fra telefonen var tilgjengelig for iranske myndigheter så lenge telefonen hadde vært koblet til mobilnettverk og internett (Spence 2018).

Regimefiendtlig aktivitet tolkes bredt. Et aktuelt eksempel er håndteringen av Covid-19 i den tidlige fasen. Da pandemien brøt ut våren 2020, ble journalister og personer som omtalte viruset på sosiale medier tatt inn til avhør og enkelte ble arrestert. Journalisten Mohammad Mosaed ble fengslet av IRGC i februar 2020 for å ha kritisert myndighetenes håndtering av pandemien. Han ble dømt til nesten fem års fengsel, men klarte i 2021 å flykte til Tyrkia (Freedom House 2021).

Øverste leder Khamenei oppfordret i mars 2020 innbyggerne om ikke å overvurdere viruset, og tjenestemenn i IRGC mente at viruset kunne være produkt av et amerikansk biologisk angrep (Jedina 2020). Tidlig i 2020 kunngjorde lederen av FATA, Vahid Majid, at det var opprettet en arbeidsgruppe som skulle bekjempe det han omtalte som «rykter» om spredning av viruset på nett. I april 2020 opplyste FATA om at 3600 personer skal ha blitt arrestert på dette grunnlaget (Freedom House 2021). Iran ble hardt rammet av Covid-19. Per juli 2022 var mer enn 140 000 registrert døde i pandemien (WHO 2022).

3.2.1 Blokkering og filtrering

Definisjoner

En strategi som myndighetene benytter, er å sperre tilgangen til nettsteder og apper for landets internettbrukere. Dette omtales gjerne som *blokkering* (blocking) eller *filtrering* (filtering).

Slik Landinfo forstår det, finnes det ikke standardiserte definisjoner av disse begrepene. Organisasjonene Open Observatory for Network Interference (OONI) og Censored Planet jobber med å måle internettsensur over hele verden. OONI peker på at filtrering gjerne brukes uoffisielt som et paraplybegrep om ulike former for internettsensur. Begrepet «filternet» (=filtered internet) brukes også mye i Iran når man snakket om det sensurerte nettet. Filtrering kan også brukes om sensur av spesifikke nøkkelord innad i en app (OONI, e-post august 2021). Censored Planet peker på at blokkering/filtrering kan assosieres med ulik type teknologi for hvordan tilgangen hindres (Censored Planet, e-post september 2021).

Begge kildene er samstemte om at det ikke er konsekvent bruk av begrepene blokkering/filtrering i litteraturen om internettsensur. Mange kilder definerer heller ikke hvordan de bruker begrepene. Derfor har Landinfo valgt å ikke definere begrepene ytterligere. Hovedpoenget er imidlertid at tjenestene har blitt gjort utilgjengelig for brukere i Iran.

En annen metode for å begrense tilgangen til ulike internett-tjenester er såkalt *throttling*. Metoden innebærer at myndighetene med vilje senker hastigheten slik at tjenestene blir vanskelige eller umulige å bruke (Article 19 2021).

Nettsteder og apper som blokkeres/filtreres

Myndighetene begrenser tilgangen til titusenvis av nettsteder, permanent eller midlertidig. Store nettsteder og apper som Twitter, Facebook, Telegram, YouTube og Signal er blokkerte tjenester i Iran, i likhet med bloggtjenester som Wix, Blogspot, Blogger og WordPress.

De to store sosiale media-tjenestene Instagram og Whatsapp er fortsatt tilgjengelige. Det har likevel blitt rapportert om tidvise forstyrrelser på begge tjenestene, senest i forbindelse med protestbølgen som startet i september 2022 (Freedom House 2021).

Selv om Instagram er tilgjengelig, har iranske myndigheter blitt beskyldt for å prøve å påvirke innholdet i tjenesten. En nåværende og en tidligere innholds-moderator sier til BBC at iranske myndighetsrepresentanter skal ha tilbudt dem flere tusen euro for å fjerne kontoer til aktivister og journalister, eksempelvis

kontoen til den profilerte aktivisten Masih Alinejad (Ghobadi 2022). Det finnes også eksempler på at myndighetene skal ha tvunget personer til å fjerne innlegg på Instagram (et eksempel er sangeren Shervin Hajipour, se 8.2). Meta har også fått kritikk for at mye persiskspråklig innhold blir fjernet av automatiserte modereringsprosesser. For eksempel fjernes innhold om protester fordi slagord som «død over Khamenei» bryter med Metas retningslinjer om voldelige ytringer (CHRI 2022b).

Nettsteder til internasjonale nyhetsmedier, menneskerettighetsorganisasjoner, den politiske opposisjonen, etniske og religiøse minoriteter, samt andre regimekritiske nettsteder blokkeres. Det samme gjelder nettsteder som representerer en annen oppfatning av islam enn den nasjonale doktrinen i Iran, eller informasjon om uenighet mellom ulike deler av myndighetsapparatet. I tillegg kan det dreie seg om sider med umoralsk og usømmelig innhold. Apper og nettsteder med tilknytning til utlandet, og spesielt USA og Israel, kan også bli blokkert (Freedom House 2020, 2021).

Innenlandske nyhetssider og nettsteder som publiserer myndighetskritisk innhold blokkeres også. Anar Press og Aban Press har begge blitt blokkert, og sjefredaktørene ble arrestert i april 2019. Freedom House viser til flere nettsteder som tidvis blokkeres og tidvis er tilgjengelig (Freedom House 2020).

3.2.2 Cyberangrep og overvåking på internett

Ifølge CHRI (2018b, s. 48) er nettangrep på internett og sosiale medier utbredt. Det gjelder særlig angrep rettet mot kontoer til sivile og politiske aktivister, journalister, akademikere og innflytelsesrike kulturpersoner. Dette er utvilsomt strategier som myndighetene bruker mye ressurser på. Omfanget og effekten er vanskelig å anslå, men det skaper uansett stor frykt og bekymring blant de som bruker internett, særlig de som tilhører den politiske opposisjonen (Article 19 2017, s. 37).

Det er IRGC, og i mindre grad Ministeriet for etterretning, som står bak nett-angrepene (CHRI 2018b, s. 48). Ifølge Article 19 (2017, s. 32-37) er det to kategorier hackere som tjenestegjør for myndighetene:

- Den første gruppen er «amatører» som må trenes og kontrolleres. De utfører enkle oppgaver, eller oppgaver med lav risiko, eksempelvis å ødelegge eller fjerne nettsteder til opposisjonen.
- Den andre gruppen har større kompetanse, og utfører oppgaver som er mer strategisk viktige.

Hackerne får instrukser med relevante mål og prioriteringer, og instruksene styrer hvilke mål som skal angripes.

Metoder som benyttes

Metodene som benyttes spenner over et bredt spekter – fra å spre datavirus, gjennomføre angrep som skader programvare, apper og maskiner, til å bryte seg inn i datasystemer. Hvilken metode som velges er tilpasset motivet for angrepet. I enkelte tilfeller er hensikten å bedrive skjult overvåking. I andre tilfeller tar de kontroll over kontoen for å angripe andres konto, eller for å spre falsk informasjon (CHRI 2018b, s. 48).

En utbredt strategi er å innhente informasjon på individnivå og infiltrere ulike digitale nettverk. Ifølge Article 19 (som gjengitt i Migrationsanalys 2020, s. 20, 21) består en stor del av overvåkningen i å overtale den enkelte bruker til å oppgi passordene sine. En rekke utspekulerte metoder benyttes. Det rapporteres om at myndighetene oppretter falske kontoer på sosiale medier som skriver provoserende og regimekritiske kommentarer.[6] De som responderer på kommentarene, kommer i myndighetenes søkelys. De falske profilene brukes også til å sende venneforespørsler, og infiltratører kan dermed få innpass i lukkede nettverk (Article 19 2017, s. 25).

CHRI (2018b, s. 48-57) peker på følgende metoder:

- **DDoS (Distributed denial of service attacks)**

Hensikten er å gjøre et nettsted utilgjengelig, og dermed hindre spredning av informasjonen på nettstedet. Metoden brukes hovedsakelig mot kritikere av regimet og dissidenter.

- **Phishing**

Phishing er en strategi hvor internettbrukere, ofte gjennom e-post, SMS eller lignende, «lokkes» til å logge seg inn på nettsider eller oppgi data for innlogging. Ifølge Article 19 (2017, s. 36) har etterligninger av Facebook-kontoer og e-post-adresser til menneskerettighetsorganisasjoner og politiske grupper blitt brukt i en slik hensikt, og har dermed åpnet veien til overvåking. Taktikken har blitt brukt for å få tilgang til Telegram-kontoer, og andre tjenester som benyttes av blant annet kvinneaktivister og den politiske opposisjonen.

Rapporter fra Miaan Group og Check Point Research hevder at det som antas å være myndighetsaffilierte iranske hackere, har fått tilgang til informasjon i krypterte meldingsapplikasjoner som Telegram og WhatsApp. De har også kommet inn på tidligere antatt sikre mobiltelefoner og datamaskiner. Begge rapportene peker på phishing som en mye brukt metode for å få tak i informasjon, for eksempel at brukere lures til å gi fra seg passord på falske påloggingssider eller applikasjoner. Installasjon av malware omtales også som en vanlig metode (se forklaring i punktet under). Angrepene er i stor grad rettet mot etniske og

[6] Eksempelvis fjernet Meta i september 2021 et nettverk med falske kontoer på Instagram og Facebook. Meta mente de var knyttet til IRGC (Meta 2022).

religiøse minoriteter, samt politiske dissidenter, journalister, menneskerettighets-forkjempere, advokater og studentaktivister. Dette underbygger, ifølge Miaan og Check Point Research, at det er staten som står bak. Både individer og grupper har blitt angrepet. En stor andel av de som har blitt hacket oppholder seg i utlandet, blant annet i USA, Canada, Tyskland, Danmark etc. Phishing og malware-verktøy som kan bli rettet mot «vanlige» iranere har også blitt utviklet (Article 18 2020; Bergman & Fassihi 2020; Check Point Research 2020; Miaan Group 2020)

- **Malware**

Dette dreier seg om ondsinnet programvare som installeres (ofte gjennom phishing-angrep) på en digital enhet, for eksempel en datamaskin eller mobiltelefon, ofte uten at eieren oppdager det. Dataprogrammet kan samle inn informasjon og avlytte innehaveren av kontoen. Malware kan også utrette skade, for eksempel ved å slette filer eller overstyre andre programmer. Malware oppdages vanligvis ikke av antivirusprogrammer.

- **Message Tapping**

Mange tjenester på internett sender tilgangskoder på SMS for å autentisere brukeren (for eksempel ved bruk av tofaktorautentisering). Dersom kodene kommer i feil hender, får uvedkommende lett tilgang til kontoer.

- **Fake Applications**

Gjennom distribusjon av piratkopierte eller lokale versjoner av populære applikasjoner, får myndighetene tilgang til å avlytte og overvåke kommunikasjon og aktivitet. Det hevdes at 42 millioner Telegram-brukere har fått bruker-ID og telefonnummer lekket og eksponert på nett. Dette skal angivelig ha skjedd fordi enkelte brukere lastet ned usikre kopier av Telegram-apper (Badiei 2020, s. 10). I tillegg utarbeides skreddersydde dokumenter eller applikasjoner til nøye utvalgte mål, eksempelvis til medlemmer av Mujahedin-e Khalq (MKO). Når dokumentet åpnes eller appen lastes ned, aktiveres malware-programmet som gjør at angriperne får tilgang til tilnærmet all informasjon på enheten (Bergman & Fassihi 2020).

Ifølge Freedom House (2021) er det uklart hvorvidt iranske myndigheter kan overvåke meldingsinnhold på utenlandske og krypterte sosiale media-plattformer. Lokale plattformer gir ikke samme beskyttelse som de internasjonale tjenestene med tanke på brukerdata. Tidligere høgskolelektor Bjørn Svenungsen uttalte til Landinfo (2021) at det ikke er holdepunkter for at iranske myndigheter får tilgang til godt kryptert materiale. Landinfo forstår det likevel slik at det finnes metoder iranske myndigheter kan benytte for å skaffe seg tilgang til innhold i slike tjenester. Som allerede nevnt i metodeoversikten kan dette gjøres gjennom phishing-angrep og installering av malware, hvor myndighetene skaffer seg tilgang til kontoer og enheter, og dermed også innholdet på disse.

3.3 Kontrollen over cyberspace blir sterkere

Det store antallet personer som jobber for dem har tidligere vært det iranske cyberapparatets fortrinn – ikke teknologi og kunnskap. Sammenlignet med land som Kina, Russland og USA ble Irans cyberkapabilitet i 2018 beskrevet som relativt lite sofistikert (Anderson & Sadjapour 2018, s. 5).

Ifølge flere kilder som svenske Migrationsanalys (2020, s. 19) har konsultert, er kontrollen over cyberspace blitt sterkere og mer omfattende de siste årene. Etter drapet på general Suleimani i januar 2020, økte omfanget av cyberangrep rettet mot USA voldsomt, og angrep mot amerikanske myndighetsnettsteder økte med 50 prosent. Nettsidene ble erstattet med et svart skjermbilde, eller en skriftlig beskjed på både persisk og engelsk samt flere bilder – blant annet av det iranske flagget eller av øverste leder. Angrepene kunne spores tilbake til iranske IP-adresser (Finsveen 2020). Et annet eksempel er cyberangrepene mot Albania i 2022. Flere statlige portaler ble angrepet, i tillegg til det albanske politiets informasjonssystem. Albanske myndigheter mener Iran står bak angrepene, og har kuttet alle diplomatiske bånd til landet. Iranske myndigheter nekter for å være innblandet (Elezi & Gholami 2022).[7]

Ifølge Bjørn Svenungsen (som gjengitt i Finsveen 2020) er ikke Iran helt på teknologisk nivå med USA, Kina og Russland. Iranske cyberangrep synes uansett å være «godt organisert», ifølge Svenungsen.

I telefonsamtale (mai 2021) presiserte Bjørn Svenungsen at per 2021 er Iran fortsatt langt bak USA og Kina når det gjelder kapasitet til å gjennomføre offensive cyberangrep. Det er svært kostbart og tar lang tid å utvikle slike kapabiliteter, noe som gir fortrinn til teknisk avanserte stater. Iran benytter som regel kjente sårbarheter, og utvikler i begrenset grad egen skadevare. Ellers bemerket Svenungsen at Iran synes å ha størst fokus på trusselen fra egen befolkning.

4 Nytt lovforslag om ytterligere internettbegrensninger

Siden 2018 har iranske myndigheter jobbet med et lovforslag som kan føre til enda flere begrensninger på hva iranere får tilgang til på nett. Forslaget har møtt stor motstand i samfunnet og beskrives av menneskerettighetsorganisasjoner som en stor trussel mot iranernes ytringsfrihet og personvern på nett. Lovutkastet har

[7] Forholdet mellom de to landene har vært anstrengt etter at Albania i 2013 tillot MEK-medlemmer å bosette seg i landet.

skiftet navn flere ganger, og heter nå offisielt Cyberspace Regulatory System (Article 19 2021; Kazemi 2022).[8]

4.1 Innholdet i lovforslaget

Innholdet i lovforslaget er ikke offentlig kjent ettersom forslaget har blitt utarbeidet i en lukket komité.[9] Organisasjonene Committee to Protect Journalists (CPJ 2021) og Article 19 (2021) har gjennomgått et tidligere utkast som ble offentliggjort i juli 2021. De peker på noen hovedpunkter:

- Utenlandske teknologi-selskaper må registrere seg med en iransk representant og rette seg etter iransk lovgivning for å kunne tilby plattformer og nettsteder i Iran. Trosser de dette, vil myndighetene først senke hastigheten på tjenesten, og deretter blokkere tilgangen fullstendig når et lokalt alternativ er utviklet.
- En arbeidsgruppe vil ta kontrollen over infrastrukturen som kobler Iran på det globale nettet. Arbeidsgruppen vil bestå av blant annet de væpnede styrkene, IRGC og etterretningsministeriet (HRW 2022).
- Brukere må registrere seg med ID hos internettleverandørene for å få tilgang til internett. Internettleverandørene blir pålagt å samle inn brukerdata og avlevere dette til myndighetene ved forespørsel.
- Produksjon, salg og distribusjon av VPN og andre proxy-tjenester blir kriminalisert (se også 5.2). En annen kilde opplyser at også bruk av VPN potensielt *kan* bli forbudt (Dagres 2022, s. 28).
- En undergruppe av SCC, Supreme Regulatory Commission (SRC), skal få utvidet mandat til å regulere hva iranere kan få tilgang til på nett. Ansvaret vil overlappe med andre organer. Kommisjonen er kjent for å stå nær støtte-spillerne til Øverste leder (Article 19 2022; Esfandiari 2022).

4.2 Potensielle konsekvenser dersom lovforslaget vedtas

Analytikeren Amir Rashidi sier til nettstedet IranWire (Miresmaeili 2022) at ettersom innholdet i lovforslaget fortsatt er uklart, er det vanskelig å si noe presist om det fremtidige skadeomfanget. Det er imidlertid åpenbart at forslaget er et angrep på iranernes ytringsfrihet, personvern og tilgang til informasjon. Rashidi hevder at iranske myndigheter er fast bestemte på å innskrenke iranernes tilgang

[8] Forslaget omtales noen ganger med sitt gamle navn – (User) Protection Bill, eller Tarh-e Siyanat på persisk.

[9] Parlamentet gav en intern parlamentarisk komité fullmakt til å utarbeide forslaget uten at resten av parlamentet var involvert. Det har derfor hersket usikkerhet om forslagets innehold. Komitéen godkjente et forslag i en avstemning i februar 2022, men resultatet ble senere annullert fordi prosedyrereglene ikke var fulgt (Article 19 2021; Kazemi 2022). Parlamentet besluttet deretter å oppløse komitéen og behandle lovforslaget på ordinær måte (Azarhoosh 2022).

til det frie internettet, og det er ikke helt utenkelig at iranernes tilgang til det globale nettet blokkeres helt.

Slik lovforslaget fremsto i juli 2021, blir det vanskeligere for iranere å bruke internasjonale tjenester. Dersom internasjonale selskaper ikke går med på iranske myndigheters krav og tjenestene forsvinner, kan internett-brukerne presses over på de lokale alternativene (Article 19 2021; Rashidi & Mostofi 2021). Kilder har advart mot at nasjonale apper, for eksempel meldingsapper, er mer usikre med tanke på sikkerhet og personvern enn de tilsvarende internasjonale versjonene. De største meldingsappene i Iran har alle tette bånd til statlige virksomheter (Kazemi 2021).[10]

Dersom iranerne mister tilgangen til internasjonale plattformer, kan det medføre økonomiske konsekvenser. Mange iranske småbedrifter er avhengige av sosiale medier for å promotere produkter og tjenester. Særlig har Instagram blitt en svært mye brukt plattform for kjøp og salg av varer og tjenester (Berger 2021; Dagres 2022, s. 28; se også punkt 6). Ifølge en diplomatkilde (e-post oktober 2021) førte den 11 dager lange nedstengningen av internett i 2019 til millioner av dollar i tap for internettbaserte bedrifter.

Forslaget om å gi sikkerhetsstyrkene økt kontroll over infrastrukturen som kobler Iran til det globale internettet trekkes frem som svært problematisk. Organisasjonen Article 19 (2021) kaller dette punktet «deeply concerning» og mener dette vil gjøre det enda enklere for myndighetene å gjennomføre nedstenginger og sensur.

Et system der befolkningen får tilgang til ulike nivåer av det sensurerte nettet kan være blant konsekvensene. Faktorer som for eksempel alder og yrke vil kunne styre hva man får tilgang til av innhold på nett (Dagres 2022, s. 28; diplomatkilde, e-post oktober 2021).

Det rapporteres om at flere av elementene i planen allerede praktiseres. Iranske medier skrev i september 2022 at SCC skal ha utstedt et direktiv som definerer SRCs sammensetning og mandat (se 4.1). Det skal også ha blitt utpekt medlemmer til kommisjonen (Article 19 2022; Esfandiari 2022). Et annet eksempel er de ulike tilgangsnivåene nevnt i forrige avsnitt. Myndighetene bekreftet i september 2022 at de hadde sendt lister til IKT-ministeriet med navn over personer som skal få full tilgang til det usensurerte nettet. Noen regimetro journalister og akademikere skal allerede ha fått en slik tilgang (Dagres 2022, s. 28; Filterwatch 2022b). Kilder påpeker også at det har blitt vanskeligere å bruke VPN i landet. Generelt har det vært meldt om dårlig forbindelse til det globale internettet siden høsten 2021 (Isfahani 2021; Motamedi 2022a; diplomatkilde, e-

[10] IKT-ministeren uttalte i mars 2022 at sikkerhetsstyrkene kunne få tilgang til brukerdata i nasjonale meldingsapper i «spesielle tilfeller». Hva som utgjør et slikt spesielt tilfelle ble ikke definert (Filterwatch 2022a).

post januar 2022). Myndighetene har videre uttalt at salg av VPN-tjenester nå er kriminelt, ifølge en diplomatkilde (e-post, november 2022). Kilden kjenner ikke til at noen har blitt dømt for dette.

5 Strategier for å unngå sensur og blokkeringer

På tross av den omfattende sensuren, blokkeringen/filtreringen og cyber-angrepene, finner iranere ulike måter å håndtere dette på. Det dreier seg om et bredt spekter av strategier – fra bruk av krypterte tilkoblinger, til selvsensur eller å unnlate å benytte digitale medier for ikke å bli sporet.

5.1 Selvsensur

Sosiologen Ali Honari (Honari 2018, juli-september, s. 7-9) har forsket på aktivisters strategier i møte med repressive regimer og overvåking på nett. Etter det omstridte presidentvalget i 2009, har mange journalister, aktivister og bloggere benyttet pseudonym. Andre skriver under en annen identitet enn deres egen når de poster regimekritiske innlegg på internett. Det forekommer også at skribenter ber andre om å publisere eget materiale online.

Det har åpenbare ulemper å ikke benytte egen identitet; det gir ingen prestisje eller individuell status. Derfor foretrekker mange å benytte eget navn, men begrenser risikoen ved å være forsiktige og utøve stor grad av selvsensur. Aktivister som har vært fengslet blir ekstra forsiktige. En av Honari's informanter sa det slik: I thought whatever I write should be defensible in court (Honari 2018, juli-september, s. 8,9).

Nettbaserte nyhetsmedier og -byråer følges tett av myndighetene. Mediene risikerer sensur, sanksjoner eller til og med nedleggelse fra myndighetene. Den omfattende overvåkingen, kombinert med de strenge straffene som personer som ytrer seg kritisk risikerer, bidrar til omfattende selvsensur. Resultatet er at det er temaer og diskusjoner som aldri blir tatt i det offentlige ordskiftet (Article 19 2020, s. 13).

5.2 Bruk av omgåelsesverktøy som VPN

På tross av myndighetenes forsøk på å kontrollere befolkningens bruk av internett, kan blokkerte eller filtrerte nettsteder bli tilgjengelig via kryptert tilkobling. Sosiologen Honari fant i sin studie at ulike «omgåelsesverktøy» – applikasjoner som VPN (Virtual Private Networks) – er utbredt. Iranere er kreative, mange har gode digitale ferdigheter, og verktøyene distribueres gjennom ulike kanaler (Honari 2018, juli-september, s. 7). Daværende høgskolelektor Bjørn Svenungsen uttalte til Landinfo i mai 2021 at selv om Google og Apple-produkter er vanskelig

tilgjengelig for iranere på grunn av de amerikanske sanksjonene, finnes en rekke private selskaper som har utviklet VPN-løsninger som også er tilgjengelig i Iran.

På tross av myndighetenes forsøk på å begrense bruken, er utbredelsen av VPN omfattende. Temaet er gjenstand for politisk debatt, og de strafferettslige sidene fremstår noe uklare. Ifølge Freedom House (2020, s. 27) er det ikke straffbart å bruke VPN, men det er derimot straffbart å selge eller markedsføre slike tjenester. Lovligheten av VPN skal imidlertid være blant temaene i det foreslåtte lovutkastet (se kapittel 4).

VPN betyr at trafikken mellom enheten og nettverket/serveren man kobler seg til blir kryptert og all trafikk fra en enhet går gjennom en server før den går videre til internett. Trafikk som går gjennom serveren blir kryptert, og kan i utgangspunktet ikke hackes, spores eller overvåkes. Internettleverandøren får ikke tilgang til søkeloggen fordi nettaktiviteten er knyttet til VPN-serverens IP-adresse (Beste VPN Norge u.å.; Norton 2021).

Det er flere grunner til at mange, også iranere, bruker VPN og lignende tjenester (Beste VPN Norge u.å.):

- VPN gir anonymitet på internett ved at det er IP-adressen til serveren som vises, og egen IP-adresse skjules. Ingen kan spore brukerens aktivitet på nett.
- VPN beskytter mot overvåkning ved at brukeren blir «usynlig».
- Ved å bruke en VPN-server utenfor landet, kan brukeren omgå sensur og blokkering av nettsteder.

6 Bruk av sosiale medier og meldingstjenester

På 2000-tallet begynte det som Article 19 (2017, s. 23) beskriver som «blogging fever». De senere årene har sosiale medier blitt viktige plattformer. På tross av at mange sosiale media og meldingstjenester er blokkert (se kapitte 3.2.1), viser en undersøkelse utført av Iranian Students Polling Agency (ISPA) fra februar 2021 at 74 prosent av iranere over 18 år bruker sosiale media og meldingsapper (omtalt i Dagres 2022, s. 4).

Det er et paradoks at Irans lederskap, slik som øverste leder Ali Khamenei, er aktive brukere av den blokkerte tjenesten Twitter, blant annet som ledd i utenrikspolitikken og retorikken mot USA. Tidligere president Hassan Rouhani var også aktiv på Twitter under sitt presidentskap, og alle de syv utvalgte kandidatene i det iranske presidentvalget i 2021 hadde Twitter-kontoer (Arouzi & Luce 2019; Berger & Taylor 2021; Dagres 2022, s. 16).

Instagram er en av få sosiale medier som er tillatt. Instagram er svært populært og har mange brukere. Den nederlandske journalisten Thomas Erdbrink har bodd i Iran en årrekke. Han er gift med en iransk kvinne, snakker persisk og har vært korrespondent for The New York Times. I en TV-serie ser han på ulike sider av det iranske samfunnet, herunder fenomenet Instagram. Ifølge Erdbrink er det ikke aviser eller TV-kanaler, men Instagram som er den viktigste kommunikasjons-kanalen i landet (Erdbrink 2018). Instagram er ofte brukt som en nyhetskilde og som en plattform for å diskutere politikk, skriver Freedom House (2021). Også under protestene som brøt ut i september 2022 ble Instagram brukt aktivt til å dele politisk innhold (diplomatkilde, e-post november 2022).

Et av Erdbrinks intervjuobjekter arbeider med sensur av TV-programmer. Han forteller at Instagram har flyttet grensene for hva som kan vises for et iransk publikum. Både hud og kroppsformer vises på Instagram uten at det får følger for de som legger det ut. Men det finnes grenser; da en gruppe ungdommer la ut en iransk versjon av en vestlig musikk- og dansevideo, ble de arrestert. De måtte be om unnskyldning på iransk TV for usømmelig oppførsel, og ble idømt en betinget straff. En av de involverte har i ettertid blitt «Instagram-stjerne» og har 180 000 følgere. Enkelte bruker plattformen til å spre politiske budskap. Kvinner har demonstrert mot den lovpålagte bruken av hodeplagg. Videoer har blitt spredd av kvinner som holdt hodeplagget på en pinne. Dette ble ikke akseptert, og kvinnene ble arrestert av moralpolitiet (Erdbrink 2018).

En hovedgrunn til at Instagram ikke forbys, er de potensielle økonomiske konsekvensene (diplomatkilde, e-post november 2022). Tjenesten har blitt en viktig plattform for kjøp, salg og annonsering av varer og tjenester. Nesten 30 prosent av alle iranske Instagram-sider anslås å være bedriftsrelaterte (Berger 2021). Bedrifter i ulike størrelser bruker Instagram for å promotere produkter som klær og smykker, eller for å reklamere for tannlegetjenester og skjønnhets-behandlinger. Spisesteder er avhengige av Instagram for å ta imot reservasjoner (Dagres 2022).

En annen grunn er at plattformen brukes aktivt av det iranske regimet og deres tjenestemenn. Tidligere president Rouhani har mer enn to millioner følgere, og Instagram spilte en betydelig rolle under presidentvalget i 2017. Øverste leder Ayatollah Khamenei hadde i juli 2022 om lag 4,9 millioner følgere på sin persisk-språklige Instagram-konto (Ayatollah Seyed Ali Khamenei u.å.)). Ifølge Erdbrink (2018) legger han daglig ut oppdateringer, eksempelvis taler, bilder, fordømming av andre land og liknende.

I likhet med verden for øvrig, har influensere blitt et fenomen også i Iran. Enkelte av dem har titusener av følgere, og har stor sosial og kulturell innflytelse. En skuespiller, Taraneh Alidoosti, hadde i 2017 mer enn fem millioner følgere. Influenserne fokuserer på temaer som kultur, mat og klær (Erdbrink 2018; Small Media u.å.). Gaming er en vanlig hobby i Iran, og live-strømming av videospill

har blitt mer populært de seneste årene. De mest populære influenserne og online-gamerne kan tjene store pengesummer på blant annet reklameinntekter og donasjoner (Dagres 2022, s. 6-7).

6.1 Særskilt om Telegram

Small Media skrev i 2017 (s. 7) at det hadde vært en vridning i bruken av sosiale medieplattformer de siste årene – fra Facebook og Twitter til Instagram og Telegram. Telegram Messenger ble etablert i 2014 av de russiske brødrene Pavel og Nikolai Durov. Appen var primært utarbeidet for å omgå russisk overvåkning (Small Media 2017, s. 12).

Meldinger sendt med Telegram er som standard kryptert, og appen kan brukes til å sende meldinger, bilder, videoer, lyd og andre filtyper. Telegram fungerer som en kilde for deling av nyheter samt personlige meldinger. I tillegg til å være en app for direkte meldinger, fungerer det også som en vert for ulike «kanaler» som sender innhold til abonnenter (MacLellan 2018).

Brukerbasen i Iran vokste med stor hastighet, og Telegram ble raskt en av de mest populære plattformene i landet. Telegram hadde anslagsvis 40 millioner månedlige brukere i et land med i overkant av 80 millioner innbyggere. Nyhetsbyråer- og nyhetsmedier, satellitt TV-kanaler, men også iranske myndigheter har benyttet appen som plattform for å formidle informasjon (Small Media 2017, s. 12).

Telegram ble en viktig arena for regimekritikere, aktivister og sivilsamfunn, både i Iran og i utlandet. Det ble delt informasjon og ytringer som det var utenkelig å legge ut på åpne fora i Iran. Telegram ble vert for store mengder sensitive data; informasjon som potensielt kunne sette mange av deres brukere i fare (Badiei 2020, s. 10).

Etter hvert som populariteten steg, innførte myndighetene nye restriksjoner på Telegram og tilsvarende tjenester. Kanaler med mer enn 5000 abonnenter ble bedt om å registrere kanalen hos myndighetene, og gi administrativ tilgang slik at myndighetene fikk adgang til å overvåke kontoen. Kanalene kunne bli bedt om å fjerne innhold som utfordrer den islamske republikken, eller oppfordringer om eksempelvis å delta på demonstrasjoner (MacLellan 2018).

På grunn av populariteten og det høye antallet brukere, hadde myndighetene stort fokus på Telegram. Etter masseprotestene i 2017 og 2018, ble Telegram forbudt i mai 2018. Det var ikke myndighetsorganene som normalt håndterer slike spørsmål som tok beslutningen, men øverste leder Khamenei og rettsapparatet. Tidligere president Rouhani var uttalt motstander av forbudet, men var ikke i stand til å stoppe det. Ifølge CHRI (2018a, s. 11) illustrerer dette hvor irrelevant

og marginalisert president Rouhani var, og at det er de konservative kreftene i landet som styrer internettpolitikken.

Iranerne ble oppfordret til å gå over til Soroush messenger, en iransk-utviklet plattform. Soroush var imidlertid ingen suksess. De som forlot Telegram, gikk i all hovedsak over til WhatsApp. Men Telegram var fortsatt populær, særlig som et talerør for regimekritiske krefter, men også regimevennlige medier kom etter hvert tilbake til Telegram, antagelig fordi Telegram var svært effektivt til å spre informasjon. I april 2019 var den statlige TV-kanalen og presidentens pressekontor tilbake på Telegram. En forklaring på dette var behovet for å nå bredt ut med informasjon og tiltak knyttet til flommen som rammet Iran våren 2019 (Article 19 2020, s. 24; Marchant 2019; Radio Farda 2019).

Telegram har vært blokkert i Iran siden 2018. Likevel er det fortsatt en svært mye brukt app, og iranerne bruker VPN for å omgå myndighetenes blokkering. Ifølge en artikkel i New York Times bruker «alle» Telegram, selv besteforeldre som vanligvis ikke beveger seg på digitale plattformer (Schwirtz 2021). Det statlig-støttede Statistical Center of Iran (SCI) rapporterte i 2021 at 45 millioner iranere brukte appen. En 2022-undersøkelse fra Iranian Students Polling Agency (ISPA) viser at Whatsapp har blitt den aller mest populære appen i Iran, etterfulgt av Instagram. Telegram kommer på en tredjeplass (CHRI 2022b; Gjevori 2022).

6.2 Nettaktivitet som oppfattes som regimefiendtlig

Det er i dagens Iran snevre rammer for hva som kan diskuteres i det offentlige rom. Det er mange temaer som det ikke, under noen omstendigheter, er mulig å rette et kritisk søkelys mot. Det er ikke rom for en regimekritisk opposisjon eller debatt, og temaer som det iranske regimets legitimitet, Øverste leder, profeten og imamene i shia-islam kan ikke diskuteres eller kritiseres i en offentlig debatt.

Landinfo får jevnlig spørsmål relatert til konvertering til kristendommen og tilknytning til de kurdiske partiene. Spørsmålene dreier seg ofte om kommunikasjonsmønster samt bruk av internett og sosiale medier. Fordi dette er to grupper som vi får spesielt mange henvendelser om, har vi valgt å omtale disse her.

6.2.1 De kurdiske partiene

Medlemskap, tilknytning eller aktivitet for de kurdiske partiene er forbudt i Iran, og kan straffes strengt. Partienes kommunikasjonsmønster og informasjonsarbeid endres i takt med den teknologiske utviklingen. Tidligere var løpesedler, tidsskrifter og analoge radiostasjoner viktige kanaler, men dette har gradvis endret seg. Allerede i 2013 hadde de fleste kurdiske partiene begynt å bruke internett for å kommunisere internt, men også for å nå ut med sitt politiske budskap (DIS & DRC 2013, s. 14).

I dag er internett den foretrukne, og antagelig også den sikreste kanalen for informasjonsdeling. Samtidig har partiene høy bevissthet om at digitale kommunikasjonsplattformer må benyttes med varsomhet på grunn av iranske myndigheters overvåkning. Ifølge Kurdistan Human Rights Network (som gjengitt i DIS 2020, s. 20) er partimedlemmer opplært til å beskytte seg. Brukere av sosiale medier som ikke beskytter seg, kan bli identifisert, og dermed eksponere både seg selv og andre for myndighetenes søkelys.

Digitale medier og internett har altså gitt de forbudte partiene økt mulighet til å spre sitt budskap, samt å kommunisere med medlemmer og sympatisører, også inne i Iran. Partiledelsen i Komala-CPI (oktober 2019) opplyste i samtale med Landinfo at internett har gjort det lettere enn tidligere å spre partiets budskap blant iranske kurdere. Også PJAK[11]s ledelse (oktober 2019) bekreftet dette; internett og sosiale medier er viktige plattformer for å kommunisere med personer som oppholder seg i Iran. Partiets nettside henvender seg både til egne medlemmer og andre (PJAK u.å.).

6.2.2 Kristne konvertitter

Etter at konvertittkirkene ble stengt i perioden fra 2009 til 2013, har kristne konvertitter blitt tvunget til å utøve sin tro i private hjem, i såkalte hjemmekirker. Internett og sosiale medier har stor betydning for kristne konvertitter i Iran – både for å komme i kontakt med andre konvertitter i Iran, og for å knytte kontakter i utlandet (Landinfo 2017, s. 9).

Evangeliske grupper og konvertitter har etablert kontakt med og mottar støtte fra kristne grupper i Nord-Amerika og Europa. Nettbaserte kirker, applikasjoner og sosiale medier som for eksempel Facebook og YouTube brukes til forkynnelse og gudstjenester, til å utveksle ideer, gi uttrykk for sin tro samt drive misjonsarbeid rettet mot muslimske iranere. Telegram er en særdeles viktig kanal for iranske konvertitter (Landinfo 2017, s. 9; Migrationsanalys 2020, s. 23). Bibelen på persisk kan gratis lastes ned fra nettet, og mye annet kristent materiell er også tilgjengelig.

En kilde som danske Udlændigestyrelsen (DIS & DRC 2018, s. 6) har konsultert, påpekte at visse søkeord brukes som basis for elektronisk overvåking, eksempelvis «kirke», «Jesus», «kristen» og «dåp». Dersom en kristen først har kommet i myndighetenes søkelys, er det grunn til å tro at vedkommende blir nøye fulgt med på. Mange kristne konvertitter er kjent med dette og tar forholdsregler ved at de slår av telefonen og annet elektronisk utstyr når de møtes i hjemmekirkene.

[11] PJAK (Partî Jiyanî Azadî Kurdistan) er en iransk-kurdisk organisasjonen, som på engelsk oftest oversettes til Free Life Party of Kurdistan eller Party of Free Life of Kurdistan.

Article 18, en kristen menneskerettighetsorganisasjon som arbeider for religionsfrihet i Iran, opplyser at konvertitter som er pågrepet, tvinges til å oppgi påloggingsinformasjon til ulike kontoer og sosiale medier. De blir videre tvunget til å overlevere telefoner og datamaskiner til myndighetene. Organisasjonen påpeker at problemet forsterkes ved at mange kristne mangler kunnskap om digital sikkerhet (Migrationsanalys 2020, s. 21). Arrestasjoner skjer ofte under razzier. Også tilstedeværende personer som ikke blir arrestert under slike razzier kan for eksempel få mobiltelefon beslaglagt (Article 18 et al. 2021, s. 10). Under avhør med myndighetene, konfronteres konvertitter også med ting de har skrevet eller delt online (Open Doors 2022, s. 32).

7 Profiler av særlig interesse for myndighetene

Selv om sikkerhetsapparatet bruker mye ressurser på å følge med på iraneres aktivitet på internett og sosiale medier, er det ikke mulig å ha fokus på alle brukere av internett og sosiale medier. Det foreligger ikke eksakt informasjon om hvilke nettprofiler som vekker iranske myndigheter sin interesse, og som de dermed bruker ressurser på å overvåke. Generelt er det primære fokuset til sikkerhetstjenesten i Iran å beskytte regimet og hindre all aktivitet som kan undergrave regimets kontroll og myndighet. Det er grunn til å tro at den samme prioriteringen ligger til grunn for disponering av ressurser i etterforskning og overvåking av aktivitet på nett.

Svenske utlendingsmyndigheter (Migrationsanalys 2020, s. 19, 22) finner holdepunkter for at det er særlig enkeltpersoner og grupper som kan utgjøre en trussel mot regimet som er i fokus. Det dreier seg om aktører som utfordrer regimet, og som ikke deler regimets politiske og religiøse ståsted. Personer, grupper eller medier som har publisert materiale som kan skade den islamske republikkens omdømme og oppslutning, er dermed åpenbart i søkelyset.

Spekteret som kan være av interesse er bredt. Ifølge U.S. State Department (U.S. Department of State 2021, s. 35) kan både bloggere, brukere av sosiale medier og online-journalister bli arrestert. Illustrerende for bredden er advarselen som myndighetene kom med i april 2019 mot å legge ut bilder av den store flommen sørvest i landet. De som trosset forbudet, kunne bli tiltalt for «disturbing public opinion». I den sørvestlige Khuzestan-provinsen skal 24 brukere av sosiale medier ha blitt arrestert for å ha spredd «fake news» om flommen (Amnesty International 2020). I oktober 2019 skal myndighetene ha arrestert Instagram-profilen Sahar Tabar for blant annet blasfemi og for «encouraging youth to corruption». Bakgrunnen var innlegg på hennes konto som viste resultatene av de mange plastiske operasjoner hun hadde tatt (Malekian 2019). Organisasjonen International Federation of Journalists rapporterte om at flere journalister mottok rettslige advarsler i forbindelse med dekningen av valget i 2021. Flere skal ha blitt trakassert av FATA og IRGCs cyber-avdeling (omtalt i Freedom House 2021).

7.1 Personer som kan påvirke opinionen i Iran

Personer som anses å ha en interessant profil gjennom sitt arbeid, sine kontakter eller aktivitet – og som dermed kan påvirke opinionen i Iran – risikerer å bli utsatt for omfattende overvåkning. Mange følgere på sosiale medier kan være en indikator på mulig innflytelse, og øker sannsynligheten for at personer følges tett av iranske sikkerhetsmyndigheter. Kanaler og medier med mange følgere, som eksempelvis Telegram, blir som tidligere nevnt fulgt ekstra godt med på (Migrationsanalys 2020, s. 23).

Personer som uttrykker seg gjennom kunst, kultur og musikk er en gruppe som det er grunn til å tro at myndighetene følger med på. Den populære, men kontroversielle musikeren Shahan Najafi, framfører tekster som omhandler sensitive temaer som sensur, teokrati og homofobi. Statsaffilierte hackere brøt seg inn på Instagram-kontoen hans i 2016, og profilbildet til artisten ble erstattet med flagget til Den islamske republikken (Simin & Rauchfleisch 2019, s. 1-2).

7.2 Iranere i utlandet

Iranere i utlandet er underlagt iransk lov, og kan ifølge straffeloven (Penal Code 2013, artikkel 7) straffeforfølges i Iran for lovbrudd begått i utlandet. En iransk jurist (digialt møte 2021) nyanserte bildet, og forklarte at det primært er sikkerhetsrelaterte lovbrudd – av både intern og ekstern karakter – som straffeforfølges i Iran selv om lovbruddene er begått i utlandet. Juristen mente videre at forhold som konsum av alkohol og usømmelig adferd begått av iranske borgere i utlandet ikke straffeforfølges i Iran.

Forskerne Collin Anderson og Karim Sadjadpour (2018, s. 47) påpeker at internett legger til rette for kommunikasjon mellom iranere og den iranske diasporaen, men har også økt myndighetenes mulighet for overvåking av disse miljøene. Forskeren Marcus Michaelsen ved Universitetet i Amsterdam (2018, s. 249-250, 255) viser hvordan digital kommunikasjonsteknologi har endret dynamikken ved å gi dissidenter fra autoritære regimer mulighet til å forbli relevante aktører i den interne debatten, selv etter at de har forlatt landet. De kan fortsette sitt engasjement for politisk endring og menneskerettigheter fra eksil. De har en plattform til å påvirke utviklingen i hjemlandet og de internasjonale, fysiske grensene er mindre viktige. Men, påpeker Michaelsen, det gir også myndighetene mulighet til å overvåke og til å reagere mot opposisjonelle miljøer i utlandet. Siden 2009 har det vært flere tilfeller av at skadelig programvare og hackere har angrepet iranske motstandere og kritikere i diasporaen. Selv om det er vanskelig å med sikkerhet fastslå at det er statlige aktører som står bak, viser undersøkelser at angrepene stammer fra Iran.

Iranske myndigheter følger med på egne borgeres aktiviteter i utlandet. Digital overvåking er en av flere metoder som benyttes, og er trolig i hovedsak rettet mot religiøse og etniske minoriteter, samt regimekritiske aktivister. Ifølge en rapport

fra Miaan Group har det som antas å være myndighetstilknyttede hackere et klart mål om å få tilgang til informasjon fra iranske opposisjonsgrupper i USA og Europa. Som eksempel nevnes et angrep rettet mot iranske dissidenter i Sverige. En skadelig programvare ble presentert som et persisk instruksjonsverktøy for iranere som ønsket svensk førerkort (Bergman & Fassihi 2020).

Myndighetene overvåker grupper som har en uttalt målsetting om å utfordre regimet i Teheran, eksempelvis Mujahedin-e Khalq, og grupper som fokuserer på regimets menneskerettighetsbrudd (Bergman & Fassihi 2020). Analytiker Amir Rashidi ved Center for Human Rights in Iran (som gjengitt i Cedoca 2020, s. 7) hevder at iranske myndigheter har søkelys på enkelte aktivister som har reist fra landet, og de følger med på sosiale medier og nettaktivitet. Rahimi påpeker imidlertid at det er aktivister med høy profil, eller de som har kontakt med den politiske opposisjonen i Iran som er interessante for iranske myndigheter.

Også familiene til aktive regimekritikere i eksil kan bli satt under overvåkning. En av metodene som brukes er digital overvåkning. Kildene er derimot ikke omforente om hvor systematisk overvåkningen er (Landinfo 2021b, s. 8-9).

7.2.1 Iranske journalister i internasjonale medier

Iranske myndigheter har en særlig interesse for personer i utlandet som har et stort publikum i Iran, og som dermed kan påvirke den iranske opinionen. De siste årene har iranske journalister som arbeider for internasjonale, persiskspråklige medier og mediehus blitt fulgt nøye med på.

Iranske myndigheter bruker et bredt spekter av virkemidler for å presse iranske journalister som jobber i utlandet til taushet. Direktøren for BBC World Service, Francesca Unsworth, hevdet i 2017 (som gjengitt i Reporters Without Borders 2017) at 150 personer med tilknytning til BBC Persian (nåværende og tidligere ansatte, samt bidragsytere) har fått sine eiendeler i Iran «frosset» og at de ikke kan gjennomføre økonomiske transaksjoner der. Familier til journalister innkalles til intervjuer, ofte med etterretningstjenesten, og de utsettes for press. Foreldre som har besøkt journalistbarna sine i utlandet, blir innkalt til omfattende avhør når de kommer hjem. Familiemedlemmer i Iran brukes til å presse journalistene til stillhet. I perioder med politisk uro og protester øker presset, ofte i den hensikt at det ikke skal rapporteres i internasjonale medier om uroen (Deutsche Welle 2019).

Truslene mot iranske journalister i utlandet materialiseres i form av nettangrep og trusler på sosiale medier. Om lag 200 iranske journalister som bor utenfor Iran skal ha mottatt sjikanerende meldinger. Om lag en fjerdedel av disse, 50 journalister, har fått drapstrusler. Journalister som jobber for Londonbaserte medier, trues med bortføring (Reporters Without Borders 2020). Trusler mot ansatte i BBC Persian og andre persisk-talende journalister utenfor Iran skal ha økt («intensified») i løpet av 2021, opplyste BBC i en presseuttalelse fra desember

samme år. Blant annet skal noen av de ansatte i BBC Persian i London ha mottatt dødstrusler (Al-Monitor 2021a).

På grunn av presset, både mot egen person og familiemedlemmer i Iran, velger en del journalister å skrive under pseudonym (Michaelsen 2017, s. 468; Reporters Without Borders 2017). Særlig synes de som arbeider for BBC Persian å være i iranske myndigheters søkelys. Men, det dreier seg ikke utelukkende om BBC-ansatte. Journalister i blant annet Radio Farda,[12] Voice of America, Deutsche Welle og Radio France Internationale er også utsatt, ifølge Reporters without Borders (2017, 2020).

Sammenfatning

Det synes å være tre forhold som avgjør om, og i hvilken grad, iranere i utlandet er i myndighetenes søkelys:

- Tilhører personen den politiske opposisjonen som utfordrer det iranske regimet og den islamske revolusjonen?
- Er personen synlig i den iranske offentligheten? Har vedkommende eksempelvis mange følgere i sosiale medier, eller tilhører mediehus med stort nedslagsfelt i Iran?
- Hvilken type kritikk fremmes? Er den innenfor eller utenfor grensen for hva som aksepteres (se kap. 6.2)?

8 Arrestasjoner og domfellelser

Det er forbudt å ytre seg kritisk om det iranske regimet, Øverste leder eller om andre sensitive temaer. Forbudet gjelder også på internett og sosiale medier. De som trosser forbudet, kan bli straffeforfulgt og idømt strenge straffer (Freedom House 2020).

8.1 Lovgivning som kan komme til anvendelse

Straffeloven inneholder flere vagt formulerte straffebud med svært vide straffe-rammer. Dette gir dommere et stort rom for skjønnsutøvelse, og bidrar til vilkårligheten og uforutsigbarheten som kjennetegner straffeutmåling i iranske domstoler. Straffelovens bok 2 kapittel 8 (artikkel 279 – 285) regulerer anklager om *moharebeh* (å føre krig mot Gud). Den som blir funnet skyldig i tiltalen om å føre krig mot Gud, kan idømmes dødsstraff ved henging. Straffelovens kapittel 9 (artikkel 286 – 288) omhandler *efsad-e-fel-arz* (korrupsjon på jorden) som også kan straffes med døden. Formodningen om uskyld ble fjernet for forbrytelsene

[12] Det persiske programmet for Radio Free Europe i Praha.

som et ledd i endringen av straffeloven i 2013. Samtidig ble tolkningsrommet for begge bestemmelsene utvidet (Penal Code 2013; iransk jurist, e-post 2021).

Kritikk av islam og alt som kan defineres som gudsbespottelse og ærekrenkelse av profeten Muhammed, hans datter Fatima og de tolv shia-muslimske imamene er forbudt og straffbart i henhold til den iranske straffelovens artikler 262 og 263, samt artikkel 513 i bok 5. Forbrytelsene straffes med fengsel, pisking eller dødsstraff (Penal Code 1996/2013).

Straffelovens bok 5 kapittel 1 (artiklene 498 – 512) omhandler nasjonal sikkerhet. Straffelovens artikler 498, 499 og 500 hjemler straff mot regimefiendtlig propaganda eller støtte til opposisjonsgrupper. Strafferammen er fra tre måneder til ti års fengsel, og/eller bøter. Straffeutmålingen varierer ut fra hvilken posisjon og type organisasjon det dreier seg om. Loven understreker at straffen gjelder for handlinger begått både i og utenfor landet. Det iranske parlamentet vedtok i 2021 nye lovtillegg til artikkel 499 og 500, som trådte i kraft samme år. Tilleggene utvider hjemmelen for å straffe personer som «fornærmer islam» og driver «avvikende pedagogisk eller misjonerende aktivitet» (USCIRF 2021, s. 1; 2022b, s. 1). Mer spesifikt kriminaliserer også tilleggene aktivitet utført på internett (Article 18 2021). I tillegg har strafferammen økt (Amendments to articles 499 and 500 IPC 2021). [13]

Kapittel 2 i straffelovens bok 5 (artikkel 513 – 515) regulerer straffeutmåling for de som har fornærmet øverste leder, den utøvende, dømmende eller lovgivende makt, samt religiøse ledere. Straffeutmålingen er i spennet fra seks måneder til to år. De som angriper eller kritiserer Øverste leder, dømmes fra tre til ti års fengsel med mindre forbrytelsen er å anse som *moharebeh* (Penal Code 1996/2013).

Presseloven (Press Law 1988) regulerer grensene for hva som kan publiseres innenfor den islamske republikkens rammer, og hvor den «røde linjen» går. «Undermining the political system» eller forsøk på «infiltrating the pillars of the Islamic Republic» aksepteres ikke, heller ikke ytringer som kan stimulere til «sexual freedom and indecency» (Simin & Rauchfleisch 2019, s. 4).

I 2009 ble loven Computer Crimes Law vedtatt. Lovens kapittel 4 er viet til «Forbrytelser mot offentlig moral og kyskhet». Artikkel 14 regulerer produksjon, publisering, lagring, handel og distribuering av uanstendig materiale på nett (Article 19 2012, s. 17, 29-32). Handlinger som beskrevet i artikkel 14, kan medføre anklager om «spreading corruption on Earth» og straffes med døden (FIDH 2020, s. 19). Det er Computer Crimes Law av 2009 som regulerer hvilket innhold som skal blokkeres; det utgjør et bredt spekter – fra pornografisk materiale til fornærmelse av religiøse figurer og offentlige tjenestemenn.

[13] Landinfo omtaler disse lovendringene og eksempler på saker i rapporten *Arrestasjon og straffeforfølgelse av kristne konvertitter – en oppdatering* (Landinfo 2022).

Vurderingen av om vilkårene for sensur er oppfylt kan synes vilkårlige, og det er lite informasjon tilgjengelig om beslutningsprosessene (Freedom House 2021).

Det finnes ingen lov som beskytter grunnleggende personvernhensyn, eller gir anvisning om hvordan opplysninger innhentet om den enkelte borger skal behandles. Det foreligger med andre ord ikke lovgivning eller juridiske garantier mot misbruk av data (Freedom House 2021).

8.2 Personer som straffeforfølges som følge av aktivitet på internett

Som tidligere nevnt (se kap. 2.2) hevder myndighetene at flere titalls tusen har blitt arrestert som følge av nettaktivitet de siste årene. Det foreligger lite informasjon om hvilke konkrete forhold som er bakgrunnen for arrestasjonene, og hva som har blitt endelig utfall i sakene; hvor stor andel som blir domfelt og på hvilket grunnlag. Sakene som det her vises til, er ikke representative. De er inkludert i notatet fordi det foreligger tilgjengelig informasjon om sakene fra åpne kilder, og de illustrerer bredden i type saker.

Journalisten Abdollah Zam bodde i eksil i Frankrike. Han drev en kryptert nyhetskanal, AmadNews, på plattformen Telegram. AmadNews var uttalt kritisk til iranske myndigheter, og hadde om lag 1,4 millioner abonnenter. Zam ble pågrepet under mystiske omstendigheter av iransk etterretning da han var på besøk i Nord-Irak høsten 2019. Anklagen lød «corruption on earth». Sommeren 2020 ble Zam dømt til døden av en revolusjonsdomstol, og i desember samme år ble han henrettet. Dette medførte sterke protester mot Iran fra flere vestlige land (BBC News 2020; Radio Free Europe 2020).

Også religionskritikk har medført strenge straffer og dødsstraff. I 2017 opprettholdt Høyesterett dødsstraffen mot Sina Dehghan og Mohammad Noori. De hadde lagt ut informasjon om islam på sosiale medier og ble funnet skyldige i anklager om «cursing the Prophet» (FIDH 2020, s. 12).

Menneskerettighetsaktivisten Narges Mohammadi har de siste to årene blitt dømt til mer enn elleve års fengsel for ulike forhold. Blant annet ble hun i 2021 dømt til 36 måneders fengsel, 80 piskeslag og bøter for «anti-government propaganda by means of the publication of false information» and «insulting government officials». Narges uttaler seg ofte på internett og sosiale medier om menneskerettighetsbrudd i Iran (Freedom House 2022; Frontline Defenders 2022).

En sak, som riktignok ligger noen år tilbake i tid, er interessant fordi dommen åpenbart hadde en allmennpreventiv hensikt, og skulle avskrekke brukere av internett mot å gå utenfor den strenge statlige kontrollen. I dommen av 2013 går dommeren i Revolusjonsdomstolen i Teheran utover strafferammen i loven, og dømte åtte internettbrukere til fengsel i 123 år. En av de dømte, en kvinne, hevdet

at de ikke publiserte egenprodusert stoff, men videreformidlet allerede eksisterende materiale på ulike Facebook-sider. Det dreide seg blant annet om informasjon om fengselsforhold og karikaturtegninger (CHRI 2014, 2015).

Etter revolusjonen i 1979 har kvinner vært pålagt å dekke til håret og bære hodeplagg. En aktivist i USA har oppfordret iranske kvinner til å legge ut bilder av seg selv uten hijab i en kampanje som bærer navnet «White Wednesdays». Ifølge et iransk nyhetsbyrå (som gjengitt av Radio Free Europe 2019) skal Revolusjonsdomstolen ha truet med at kvinner som deltar i kampanjen kan idømmes fengsel med en strafferamme på inntil ti år. Landinfo er ikke kjent med om noen faktisk har blitt straffet på dette grunnlaget i forbindelse med denne spesifikke kampanjen.

Sommeren 2022 annonserte iranske myndigheter en strengere implementering av landets offisielle kleskode. Lederen av Headquarters for the Office of Enjoining Right and Forbidding Evil, Mohammad Saleh Hashemi Golpayegani, skal i august 2022 ha sagt at kvinner som publiserer bilde av seg selv uten hijab, kan miste «noen sosiale rettigheter» i en periode på seks måneder til et år. Statsansatte kan miste jobben dersom profilbilde på sosiale media ikke samsvarer med islamsk lov. Golpayegani har også sagt i et intervju at myndighetene vil bruke ansikts-gjenkjenning for å slå ned på ukorrekt hijabbruk i offentlige rom (Filterwatch 2022b; RFE/RL 2022; Strzyżyńska 2022).

The Guardian har rapportert om kvinner som har blitt identifisert og arrestert etter at videoer av dem ble spredt på nettet. Artist og forfatter Sepideh Rashno ble arrestert i juli 2022 (Strzyżyńska 2022). Videoen av henne viste at Rashno ble trakassert av en annen passasjer på grunn av ukorrekt bruk av hijab. Menneske-rettighetsorganisasjoner mener hun ble tvunget til å tilstå på statlig tv. Rashno er anklaget for flere forhold og ble løslatt mot kausjon i slutten av august 2022 (USCIRF 2022a).

Da 22 år gamle Mahsa Amini døde etter å ha blitt arrestert av moralpolitiet for feil bruk av hijab i september 2022, brøt det ut store protester i hele landet. Blant de mange journalistene som har blitt arrestert, er Mojtaba Rahimi. Han ble arrestert etter at han la ut tweets om drepte demonstranter i hjembyen Qazvin (The New Arab 2022). Sangeren Shervin Hajipour ble arrestert etter at sangen hans «Baraye» ble delt på sosiale medier i forbindelse med protestene og fikk mer enn 40 millioner visninger. Myndighetene skal ha tvunget Hajipour til å fjerne sangen fra Instagram og han skal senere ha blitt løslatt mot kausjon (Berger & Mahoozi 2022).

Det foreligger rapporterte tilfeller av at aktivister har blitt arrestert på grunn av nettaktivisme mot tvungen bruk av hijab. I april 2019 ble Mojgan Keshavarz, Monireh Arabshahi og sistnevntes datter Yasaman Ariyani arrestert for å ha delt en video på ulike sosiale medier på kvinnedagen. Videoen viser at kvinnene deler

ut blomster, og samtidig argumenterer for at bruk av hijab ikke skal være påbudt, men et frivillig valg. En revolusjonsdomstol i Teheran dømte aktivistene til lange fengselsstraffer. Den lengste straffen ble idømt Keshavarz, og var på over 20 år. En ankedomstol reduserte antall år fengselsstraff noe. Sakene har fått internasjonal oppmerksomhet, blant annet fra Human Rights Watch og FN (Radio Farda 2020; U.S. Department of State 2020, s. 25).

En tidligere verdensmester i kickboksing, kjent som Picasso Moin, ble sammen med sin kone dømt til 16 års fengsel, 74 piskeslag og bot av en revolusjons-domstol på grunn av deres aktivitet på sosiale medier. Anklagene handlet om offentlig moral og moralsk korrupsjon. Paret, som flyktet til Tyrkia i september 2019, har nærmere 1,5 millioner følgere på Instagram (Sinaiee 2020).

Menneskerettighetsaktivisten Payam Shakiba ble i september 2021 dømt til 13 måneders fengsel, samt et forbud mot å forlate landet og bli medlem i politiske og sosiale grupper. Han ble funnet skyldig i å støtte politiske fanger og å oppfordre til boikott av valget på internett (UN Special Rapporteur 2022, s. 10).

LGBT-aktivistene Zahra Sadighi Hamedani and Elham Choubdar ble i september 2022 dømt til døden for «corruption on earth» av en revolusjonsdomstol. Gjennom populære kontoer på Instagram og Telegram skal kvinnene ha hatt fokus på rettighetene til LGBT-personer, noe Amnesty og FN-eksperter mener er en del av grunnlaget for domfellelsen (Amnesty International 2022; Office of the High Commissioner for Human Rights 2022).

Fire bahá'íere ble ifølge CHRI (2021a) dømt til fem års fengsel for «acting against national security through the Baha'i cult organization and posting falsehoods online». Kritiske innlegg på nett om statens behandling av bahá'íere og tilknytning til et nettbasert bahá'í-universitet ble nevnt i dommene.

Det finnes også eksempel på at kristne konvertitter skal ha blitt presset av iransk etterretning til å avstå fra kontakt, både fysisk og på internett (Article 18 2021).

Konvertitten Ismaeil Maghrebinejad ble arrestert i 2019, blant annet for «insulting Islamic sacred beliefs in the cyberspace». Dette skyldtes at han hadde reagert med en smiley-emoji på en SMS som gjorde narr av prestestyret. Tiltalen må sees i sammenheng med at mannen er konvertitt, samt flere andre tiltaler mot ham, mener Article 18. Ankedomstolen opphevet akkurat denne dommen, som var på 2 år (Article 18 2022).

9 Referanser

Skriftlige kilder

Al-Monitor (2021a, 10. desember). BBC calls for Iran to stop 'campaign of harassment' against staff. *Al-Monitor*. Tilgjengelig fra https://www.al-monitor.com/originals/2021/12/bbc-calls-iran-stop-campaign-harassment-against-staff [lastet ned 12. juli 2022].

Al-Monitor (2021b, 13. oktober). Iran's president calls for tighter internet control. *Al-Monitor*. Tilgjengelig fra https://www.al-monitor.com/originals/2021/10/irans-president-calls-tighter-internet-control [lastet ned 15. juli 2022].

Al Jazeera (2022, 22. september). Iran restricts WhatsApp, Instagram as Mahsa Amini protests grow. *Al Jazeera*. Tilgjengelig fra https://www.aljazeera.com/news/2022/9/22/iran-restricts-whatsapp-instagram-as-mahsa-amini-protests-grow [lastet ned 29. september 2022].

Amendments to articles 499 and 500 IPC (2021). قانون الحاق دو ماده به کتاب پنجم قانون مجازات اسلامی (تعزیرات و مجازات های بازدارنده) *[The law on the accession of two articles to the fifth book of the Islamic Penal Code (ta'zir and deterrent punishments)]*. Tilgjengelig fra https://web.archive.org/web/20210824111950/https://rc.majlis.ir/fa/law/show/1643402 [lastet ned 14. september 2022]. Nettsiden er tilgjengelig via Wayback Machine.

Amnesty International (2020, 18. februar). *Human Rights in Iran: Review of 2019*. London: Amnesty International. Tilgjengelig fra https://www.amnesty.org/en/documents/mde13/1829/2020/en/ [lastet ned 12. juli 2022].

Amnesty International (2022, 15. september). *Iran: Iranian LGBTI defender sentenced to death: Zahra Sedighi-Hamadani & Elham Choubdar*. London: Amnesty International. Tilgjengelig fra https://www.amnesty.org/en/documents/mde13/6035/2022/en/ [lastet ned 7. oktober 2022].

Anderson, Collin & Sadjapour, Karim (2018). *Iran's Cyber Threat*. Washington D.C.: Carnegie Endowment for International Peace. Tilgjengelig fra https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf [lastet ned 7. juli 2022].

Arouzi, Ali & Luce, Dan De (2019, 21. august). Tech-savvy Iranians stay connected on social media despite regime restrictions. *NBC News*. Tilgjengelig fra https://www.nbcnews.com/news/world/tech-savvy-iranians-stay-connected-social-media-despite-regime-restrictions-n1044016 [lastet ned 11. juli 2022].

Article 18 (2020, 23. september 2020). *Iranian minorities and activists targeted in 'large-scale' hacking operation*. London: Article 18. Tilgjengelig fra https://articleeighteen.com/news/6866/ [lastet ned 5. oktober 2022].

Article 18 (2021, 3. februar). *Iranian Christians ordered not to meet – in person or online*. London: Article 18. Tilgjengelig fra https://articleeighteen.com/news/7762/ [lastet ned 13. juli 2022].

Article 18 (2022, 16. juli). *Ismaeil Maghrebinejad*. London: Article 18. Tilgjengelig fra https://articleeighteen.com/reports/case-studies/6137/ [lastet ned 10. oktober 202].

Article 18; Open Doors; CSW, dvs. Christian Solidarity Worldwide & MEC, dvs. Middle East Concern (2021, januar). *Rights Violations Against Christians in Iran. Annual Report 2020*. London: Article 18, Open Doors, CSW & MEC. Tilgjengelig fra https://articleeighteen.com/wp-content/uploads/2021/02/2020-Report-Edited-1.pdf [lastet ned 14. juli 2022].

Article 19 (2012). *Islamic Republic of Iran: Computer Crimes Law*. London: Article 19. Tilgjengelig fra https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5b4%5d.pdf [lastet ned 12. juli 2022].

Article 19 (2017). *Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran*. London: Article 19. Tilgjengelig fra https://www.article19.org/data/files/medialibrary/38619/Iran_report_part_2-FINAL.pdf [lastet ned 1. oktober 2021].

Article 19 (2020, september). *Iran: Tightening the Net 2020 After Blood and Shutdowns*. London: Article 19. Tilgjengelig fra https://www.article19.org/wp-content/uploads/2020/09/TTN-report-2020.pdf [lastet ned 30. juni 2022].

Article 19 (2021). *Iran: Parliament's "Protection Bill" will hand over complete control of the Internet to authorities*. London: Article 19. Tilgjengelig fra https://www.article19.org/resources/iran-parliaments-protection-bill-will-hand-over-complete-control-of-the-internet-to-authorities/ [lastet ned 6. juli 2022].

Article 19 (2022, 9. september). *Iran: Cyberspace authorities 'silently' usher in draconian internet bill*. London: Article 19. Tilgjengelig fra https://www.article19.org/resources/iran-draconian-internet-bill/ [lastet ned 2. november 2022].

Ayatollah Seyed Ali Khamenei, @khamenei_ir (u.å.), *Ayatollah Seyed Ali Khamenei*. Twitter. Tilgjengelig fra https://www.instagram.com/khamenei_ir/?utm_source=ig_embed [lastet ned 11. juli 2022].

Azarhoosh, Kaveh (2022, 29. juni). *Policy Monitor - April 2022*. S.l.: FilterWatch. Tilgjengelig fra https://filter.watch/en/2022/06/29/policy-monitor-april-2022/ [lastet ned 7. juli 2022].

Badiei, Farzaneh (2020). *The Tale of Telegram Governance: When the Rule of Thumb Fails*. New Haven: Yale's Justice Collaboratory. Tilgjengelig fra https://law.yale.edu/sites/default/files/area/center/justice/document/telegram-governance-publish.pdf [lastet ned 7. juli 2022].

BBC News (2020, 13. desember). Ruhollah Zam: EU powers boycott Iran forum over execution. *BBC News*. Tilgjengelig fra https://www.bbc.com/news/world-middle-east-55296434?xtor=AL-72-%5Bpartner%5D-%5Binforadio%5D-%5Bheadline%5D-%5Bnews%5D-%5Bbizdev%5D-%5Bisapi%5D [lastet ned 12. juli 2022].

Bekkevang, Marius Andreas (2017). *Cyberangrep. En risiko for Norge*. Oslo: Krigsskolen. Tilgjengelig fra https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2452303/2017-04-03%20%28U%29%20Bekkevang%2C%20Kull%20Krebs%2C%20Bacheloroppgave.pdf?sequence=1&isAllowed=y [lastet ned 30. juni 2022].

Berger, Miriam (2021, 7. august). Bill to restrict Internet in Iran could threaten pandemic-era Instagram commerce boom. *The Washington Post*. Tilgjengelig fra https://www.washingtonpost.com/world/2021/08/07/iran-instagram-pandemic-economy-ban/ [lastet ned 8. juli 2022].

Berger, Miriam & Mahoozi, Sanam (2022, 5. oktober). How a viral song became the unofficial anthem of Iran's protests. *The Washington Post*. Tilgjengelig fra https://www.washingtonpost.com/world/2022/10/04/iran-protests-song-shervin-hajipour-arrested/ [lastet ned 11. oktober 2022].

Berger, Miriam & Taylor, Adam (2021, 2. februar). Will Twitter ban Iran's supreme leader next? *The Washington Post*. Tilgjengelig fra

https://www.washingtonpost.com/world/2021/02/02/will-twitter-ban-irans-supreme-leader-next/ [lastet ned 11. juli].

Bergman, Ronen & Fassihi, Farnaz (2020, 2020-09-18). Iranian Hackers Found Way Into Encrypted Apps, Researchers Say. *The New York Times*. Tilgjengelig fra https://www.nytimes.com/2020/09/18/world/middleeast/iran-hacking-encryption.html [lastet ned 05.02.2021].

Beste VPN Norge (u.å.). Hva er VPN og hvordan kan det hjelpe deg? *Beste VPN Norge*. Tilgjengelig fra https://bestevpnnorge.no/hva-er-vpn [lastet ned 8. juli 2022].

Biddle, Sam & Hussain, Murtaza (2022, 28. oktober 2022). *Hacked documents: How Iran can track and control protesters' phones*. S.l.: The Intercept. Tilgjengelig fra https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/ [lastet ned 3. november 2022].

Bratberg, Kathinka Louise Rinvik & Raake, Hannah (2021, 2. februar). Atomavtalen og håpet som brast. *Folk og Forsvar*. Artikkelen er ikke lenger tilgjengelig på nett [lastet ned 16. mars 2021]. Den kan leses via Wayback Machine: https://web.archive.org/web/20210203024602/https://folkogforsvar.no/usa-og-iran-pa-randen-av-krig/.

Cedoca (2020). *COI Focus Iran. Treatment of returnees by their national authorities*. Brussel: Cedoca. Tilgjengelig fra https://www.cgrs.be/sites/default/files/rapporten/coi_focus_iran_treatment_of_returnees_by_their_national_authorities_20200330.pdf [lastet ned 12. juli 2022].

Check Point Research (2020). *Rampant Kitten – An Iranian Espionage Campaign*. Tel Aviv & San Carlos, CA: Check Point Research. Tilgjengelig fra https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign/ [lastet ned 5. oktober 2022].

CHRI, dvs. Center for Human Rights in Iran (2014, 27. mai). *Eight Facebook Users Sentenced to Decades in Prison*. New York: CHRI. Tilgjengelig fra https://iranhumanrights.org/2014/05/facebook-sentence/ [lastet ned 12. juli 2022].

CHRI, dvs. Center for Human Rights in Iran (2015, 4. august). *Facebook Activist Details How She Received a Seven-Year Prison Sentence in Iran*. New York: CHRI. Tilgjengelig fra https://iranhumanrights.org/2015/08/shahsavandi-facebook-sentenced/ [lastet ned 12. juli 2022].

CHRI, dvs. Center for Human Rights in Iran (2018a, juni). *Closing of the Gates. Implications of Iran's Ban on the Telegram Messaging App*. New York: CHRI. Tilgjengelig fra https://www.iranhumanrights.org/wp-content/uploads/Closing-the-gates-3-online.pdf [lastet ned 11. juli 2022].

CHRI, dvs. Center for Human Rights in Iran (2018b). *Guards at the Gate: The Expanding State Control Over the Internet in Iran*. New York. Tilgjengelig fra https://www.iranhumanrights.org/wp-content/uploads/EN-Guards-at-the-gate-High-quality.pdf [lastet ned 30. juni 2022].

CHRI, dvs. Center for Human Rights in Iran (2021a, 14. oktober). *Four Baha'is Sentenced to Five Years in Prison for Trying to Access Higher Education*. New York: CHRI. Tilgjengelig fra https://iranhumanrights.org/2021/10/four-bahais-sentenced-to-five-years-in-prison-for-trying-to-access-higher-education/ [lastet ned 13. juli 2022].

CHRI, dvs. Center for Human Rights in Iran (2021b, 17. mars). *U.S. Government, Companies Can Do More to Promote Internet Freedom in Iran*. New York: CHRI. Tilgjengelig fra https://iranhumanrights.org/2021/03/u-sgovernment-companies-can-do-more-to-promote-internet-freedom-in-iran/ [[lastet ned 6. juli 2022].

CHRI, dvs. Center for Human Rights in Iran (2022a, 26. september). *Joint Statement: U.S. Treasury's New General License D2 Advances Internet Freedom in Iran*. New York: CHRI. Tilgjengelig fra https://iranhumanrights.org/2022/09/joint-statement-u-s-treasurys-new-general-license-d2-a-step-forward-for-internet-freedom-in-iran/ [lastet ned 5. oktober 2022].

CHRI, dvs. Center for Human Rights in Iran (2022b). *Rights Groups Call on Meta to Fix Persian Content Moderation for Instagram*. New York: CHRI. Tilgjengelig fra https://iranhumanrights.org/2022/06/rights-groups-call-on-meta-to-fix-persian-content-moderation-for-instagram/ [lastet ned 7. oktober 2022].

Constitution of Iran (1979). *The Constitution of the Islamic Republic of Iran*. Tilgjengelig fra http://www.refworld.org/docid/3ae6b56710.html [lastet ned 5. juli 2022].

CPJ, dvs. Committee to Protect Journalists (2021). *Iran's parliament moves forward with troubling bill to further restrict internet*. Wahington D.C.: CPJ. Tilgjengelig fra https://cpj.org/2021/11/iran-parliament-bill-restrict-internet/ [lastet ned 8. juli 2022].

Dagres, Holly (2022, januar). *Iranians on #SocialMedia*. Washington D.C.: Atlantic Council. Tilgjengelig fra https://www.atlanticcouncil.org/in-depth-research-reports/report/iranians-on-socialmedia/ [lastet ned 8. juli 2022].

Danish Immigration Service (2020, juli). *November 19 Protests*. København: Danish Immigration Service. Tilgjengelig fra https://www.ecoi.net/en/file/local/2033026/COI_brief_report_iran_nov_2019_protest_july_2020.pdf [lastet ned 5. juli 2022].

Deutsche Welle (2019, 5. desember). Iranian journalists in Europe face threats and harassment from regime in Tehran. *Deutsche Welle*. Tilgjengelig fra https://www.dw.com/en/iranian-journalists-in-europe-face-threats-and-harassment-from-regime-in-tehran/a-51547687 [lastet ned 23. august 2021].

DFAT, dvs. Department of Foreign Affairs and Trade (Australia) (2020, 14. april). *DFAT Country Information Report Iran*. Canberra: DFAT. Tilgjengelig fra https://www.dfat.gov.au/sites/default/files/country-information-report-iran.pdf [lastet ned 30. juni 2022].

DIS, dvs. Danish Immigration Service (2020, februar). *Iranian Kurds. Consequences of political activities in Iran and KRI*. København: Danish Immigration Servce. Tilgjengelig fra https://www.ecoi.net/en/file/local/2024578/Report+on+Iranian+Kurds+Feb+2020.pdf [lastet ned 25. juni 2021].

DIS, dvs. Danish Immigration Service & DRC, dvs. Danish Refugee Council (2013, 30. september). *Iranian Kurds*. København: DIS & DRC. Tilgjengelig fra https://www.ecoi.net/en/file/local/1133789/1226_1380796700_fact-finding-iranian-kurds-2013.pdf [lastet ned 8. juli 2022].

DIS, dvs. Danish Immigration Service & DRC, dvs. Danish Refugee Council (2018, februar). *Iran: House Churches and Converts*. København: DIS & DRC. Tilgjengelig fra https://us.dk/publikationer/2018/februar/iran-house-churches-and-converts/ [lastet ned 11. juli 2022].

Ehlson, Sara Beth; Yeung, Douglas; Roshan, Parisa; Bohandy, S.R. & Nader, Alireza (2012). Background on Social Media Use in Iran and Events Surrounding the 2009. I: *Using Social Media to Gauge Iranian Public Opinion and Mood After the 2009 Election*. California: RAND corporation. Tilgjengelig fra https://www.jstor.org/stable/10.7249/tr1161rc.10 [lastet ned 30. juni 2022].

Elezi, Elona & Gholami, Niloofar (2022, 16. september). Albania once again the target of cyberattacks after cutting diplomatic ties with Iran and expelling diplomats. *Deutsche Welle*. Tilgjengelig fra https://www.dw.com/en/albania-once-again-the-target-of-cyberattacks-after-cutting-diplomatic-ties-with-iran-and-expelling-diplomats/a-63146285 [lastet ned 12. oktober 2022].

Erdbrink, Thomas (2018). Vår mann i Teheran [Our man in Tehran] [TV-serie]. Serien var tidligere mulig å se via NRK TV, men er per 11. juli 2022 ikke lenger tilgjengelig.

Ershad, Alijani (2020, 21. april). In Iran, poverty and lack of internet make distance learning impossible. *The Observers*. Tilgjengelig fra https://observers.france24.com/en/20200421-iran-internet-covid19-distance-learning-poverty [lastet ned 5. juli 2022].

Esfandiari, Golnaz (2022, 9. september). Iran Accused Of Secretly Implementing Controversial Draft Internet Bill. *RFE/RL, dvs. Radio Free Europe/Radio Liberty*. Tilgjengelig fra https://www.rferl.org/a/iran-internet-bill-controversy-secretly-implementing/32026313.html [lastet ned 12. oktober 2022].

FIDH, dvs. International Federation for Human Rights (2020). *No one is spared. The widespread use of the death penalty in Iran*. Paris: FIDH. Tilgjengelig fra https://www.fidh.org/IMG/pdf/iranpdm758ang.pdf [lastet ned 12. juli 2022].

Filterwatch (2021, 19. juli). *[Updated 26/7] Shutdown Monitor: Local Internet Disruptions Target Escalating Water Protests in Khuzestan*. S.l.: Filterwatch. Tilgjengelig fra https://filter.watch/en/2021/07/19/shutdown-monitor-local-internet-disruptions-target-escalating-water-protests-in-khuzestan/ [lastet ned 3. august 2022].

Filterwatch (2022a, 25. oktober). *Iran's Domestic Messaging Apps: Abandoned Rafts Floating on the Ocean of Internet Restriction Policies* S.l.: Filterwatch. Tilgjengelig fra https://filter.watch/en/2022/10/25/irans-domestic-messaging-apps-abandoned-rafts-floating-on-the-ocean-of-internet-restriction-policies/ [lastet ned 3. november 2022].

Filterwatch (2022b, 28. september). *Policy Monitor: Government Use of AI-enabled Facial Recognition Systems*. S.l.: Filterwatch. Tilgjengelig fra https://filter.watch/en/2022/09/28/policy-monitor-august-2022/ [lastet ned 4. oktober 2022].

Filterwatch (2022c, 2. november). *A Summary of The Intercept's Report: "How Iran Can Track and Control Protesters' Phones"*. S.l.: Filterwatch. Tilgjengelig fra https://filter.watch/en/2022/11/02/a-summary-of-the-intercepts-reporthow-iran-can-track-and-control-protesters-phones/ [lastet ned 3. november 2022].

Finsveen, Jesper Nordahl (2020, 17. januar). Det massive angrepet «ingen» merket. *Dagbladet*. Tilgjengelig fra https://www.dagbladet.no/nyheter/det-massive-angrepet-ingen-merket/72029080 [lastet ned 7. juli 2022].

Freedom House (2020). *Freedom on the Net 2020. Iran*. Washington D.C.: Freedom House. Tilgjengelig fra https://freedomhouse.org/country/iran/freedom-net/2020 [lastet ned 5. juli 2022].

Freedom House (2021, 21. september). *Freedom on the Net 2021: Iran*. Washington D.C.: Freedom House. Tilgjengelig fra https://freedomhouse.org/country/iran/freedom-net/2021 [lastet ned 12. oktober 2021].

Freedom House (2022). *Freedom on the Net 2022: Iran*. Washington D.C.: Freedom House. Tilgjengelig fra https://freedomhouse.org/country/iran/freedom-net/2022 [lastet ned 2. november 2022].

Frenkel, Sheera (2018, 2. januar). Iranian Authorities Block Access to Social Media Tools. *The New York Times*. Tilgjengelig fra https://www.nytimes.com/2018/01/02/technology/iran-protests-social-media.html [lastet ned 5. juli 2022].

Frontline Defenders (2022, 11. oktober). Narges Mohammadi sentenced to additional 15 months in prison. *Frontline Defenders*. Tilgjengelig fra https://www.frontlinedefenders.org/en/case/narges-mohammadi-sentenced-additional-15-months-prison [lastet ned 8. november 2022].

Ghobadi, Parham (2022, 27. mai). Instagram moderators say Iran offered them bribes to remove accounts. *BBC*. Tilgjengelig fra https://www.bbc.com/news/world-middle-east-61516126 [lastet ned 7. oktober 2022].

Gilbrant, Jørgen M. (2010, 15. desember). «Stuxnet» har satt Iran to år tilbake. *Dagbladet*. Tilgjengelig fra https://www.dagbladet.no/nyheter/stuxnet-har-satt-iran-to-ar-tilbake/64353609 [lastet ned 30. juni 2022].

Gjevori, Elis (2022, 23. september). Mahsa Amini: Activists accuse Iranian authorities of using Telegram 'snitch line' to track protesters. *Middle East Eye*. Tilgjengelig fra https://www.middleeasteye.net/news/mahsa-amini-iran-protests-authorities-accused-telegram-snitch-line-track-protesters [lastet ned 10. oktober 2022].

Honari, Ali (2018, juli-september). "We Will Either Find a Way, or Make One": How Iranian Green Movement Online Activists Perceive and Respond to Repression. *Social Media + Society*, *4*(3). Tilgjengelig fra https://journals.sagepub.com/doi/10.1177/2056305118803886 [lastet ned 8. juli 2022].

HRW, dvs, Human Rights Watch (2022, 17. mars). *Iran: Human Rights Groups Sound Alarm Against Draconian Internet Bill*. New York: HRW. Tilgjengelig fra https://www.hrw.org/news/2022/03/17/iran-human-rights-groups-sound-alarm-against-draconian-internet-bill [lastet ned 7. oktober 2022].

Isfahani, Sayeh (2021, 4. november). *Tightening the net: Alarming moves to enforce the "User Protection Bill"*. London: Article 19. Tilgjengelig fra https://www.article19.org/resources/tightening-the-net-is-the-dangerous-user-protection-bill-still-imminent/ [lastet ned 8. juli].

ITU, dvs. International Telecommunication Union (2020). *Percentage of individuals using the internet*. Genève: ITU. Tilgjengelig fra https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2021/December/PercentIndividualsUsingInternet.xlsx [lenken går direkte til Excel-skjemaet] [lastet ned 14. juli 2022].

Jedina, Mehdi (2020, 25. mars). Iran Uses Arrests, Censorship to Silence Critical COVID-19 Coverage. *Voice of America*. Tilgjengelig fra https://www.voanews.com/a/extremism-watch_iran-uses-arrests-censorship-silence-critical-covid-19-coverage/6186407.html [lastet ned 6. juli 2022].

Kazemi, Melody (2021, 30. november). *The Role of Domestic Messaging Apps in Iran's Information Controls*. S.l.: Filterwatch. Tilgjengelig fra https://filter.watch/en/2021/11/30/the-role-of-domestic-messaging-apps-in-irans-information-controls/ [lastet ned 8. juli 2022].

Kazemi, Melody (2022, 29. mars). *Policy Monitor - February 2022*. S.l.: FilterWatch. Tilgjengelig fra https://filter.watch/en/2022/03/29/policy-monitory-february-2022/ [lastet ned 7. juli 2022].

Landinfo (2017, 29. november). *Iran: Kristne konvertitter og hjemmekirker (2) - arrestasjoner og straffeforfølgelse*. Oslo: Landinfo. Tilgjengelig fra https://landinfo.no/wp-content/uploads/2018/04/Iran-temanotat-Kristne-konvertitter-og-hjemmekirker-del-2-Arrestasjoner-og-straffeforf%C3%B8lgelse-29112017.pdf [lastet ned 11. juli 2022].

Landinfo (2020, 12. august). *The Iranian Welfare System*. Oslo: Landinfo. Tilgjengelig fra https://landinfo.no/wp-content/uploads/2020/08/Report-Iran-Welfare-system-12082020.pdf [lastet ned 5. juli 2022].

Landinfo (2021a, 5. januar). *Pass, ID- og sivilstatusdokumenter*. Oslo: Landinfo. Tilgjengelig fra https://landinfo.no/wp-content/uploads/2021/01/Iran-temanotat-Pass-ID-og-sivilstatusdokumenter-NIP-AHOV-05012021.pdf [lastet ned 8. desember].

Landinfo (2021b, 23. november). *Reaksjoner mot regimekritiske eksiliraneres familiemedlemmer i Iran*. Oslo: Landinfo. Tilgjengelig fra https://landinfo.no/wp-content/uploads/2021/11/Temanotat-Iran-Reaksjoner-mot-regimekritiske-eksilborgeres-familiemedlemmer-23112021.pdf [lastet ned 12. juli 2022].

Landinfo (2022, 20. juni). *Arrestasjon og straffeforfølgelse av kristne konvertitter – en oppdatering*. Oslo: Landinfo. Tilgjengelig fra https://landinfo.no/wp-content/uploads/2022/06/Temantoat-Iran-Arrestasjon-og-straffeforfolgelse-av-kristne-konvertitter-en-oppdatering-20062022-utenENDNOTE.pdf [lastet ned 13. juli 2022].

Landinfo; CGRS, dvs. The Office of the Commissioner General for Refugees and Stateless Persons & SEM, dvs. State Secretariat for Migration (2021). *Iran. Criminal procedures and documents*. Oslo, Brussel og Bern: Landinfo, CGRS & SEM. Tilgjengelig fra https://landinfo.no/wp-content/uploads/2021/12/Iran-report-criminal-procedures-and-documents-122021-4.pdf [lastet ned 3. august 2022].

MacLellan, Stephanie (2018, 9. januar 2018). What You Need to Know about Internet Censorship in Iran. *Centre for International Governance Innovation*. Tilgjengelig fra https://www.cigionline.org/articles/what-you-need-know-about-internet-censorship-iran/ [lastet ned 5. juli 2022].

Malekian, Somayeh (2019, 7. oktober). Iranian social media influencer arrested for 'encouraging youths to corruption'. *ABC news*. Tilgjengelig fra https://abcnews.go.com/US/iranian-social-media-influencer-arrested-encouraging-youth-corruption/story?id=66114640 [lastet ned 12. juli].

Marchant, James (2019, 20. mai). *FATAwatch//01 — Iranian Cyber Police Monitoring*. S.l.: FilterWatch. Tilgjengelig fra https://medium.com/filterwatch/fatawatch-01-iranian-cyber-police-monitoring-767c22a023fb [lastet ned 11. juli 2022].

Meta (2022, 11. oktober). *September 2021 Coordinated Inauthentic Behavior Report*. S.l. Tilgjengelig fra https://about.fb.com/news/2021/10/september-2021-coordinated-inauthentic-behavior-report/ [lastet ned 8. november 2022].

Miaan Group (2020). *Spiraling Attacks: Iranian Hacking Campaign*. S.l.: Miaan Group. Tilgjengelig fra https://www.miaan.org/publication/spiraling-attacks/ [lastet ned 5. oktober 2022].

Michaelsen, Marcus (2017). Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran. *Surveillance & Society, 15*(3/4), 465-470. Tilgjengelig fra https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6635/6436 [lastet ned 12. juli 2022].

Michaelson, Marcus (2018). Exit and voice in a digital age: Iran's exiled activists and the authoritarian state. *Globalizations, 15*(2), 248-264. Tilgjengelig fra https://www.tandfonline.com/doi/full/10.1080/14747731.2016.1263078?scroll=top&needAccess=true [lastet ned 19. juni 2021].

Migrationsanalys (2020, 8. juni). *Iran – Situationen för konvertiter och regimens övervakning av internet och sociala medier*. Norrköping: Migrationsanalys. Tilgjengelig fra https://lifos.migrationsverket.se/dokument?documentSummaryId=44432 [lastet ned 6. juli 2022].

Miresmaeili, Amir Hossein (2022, 5. januar). Are These the Dying Days of Iran's Open Internet? *IranWire*. Tilgjengelig fra https://iranwire.com/en/features/11054 [lastet ned 8. juli 2022].

Motamedi, Maziar (2022a). Iran's internet bill expected to progress despite overturned vote. *Al Jazeera*. Tilgjengelig fra https://www.aljazeera.com/news/2022/2/23/irans-internet-bill-expected-to-progress-despite-overturned-vote [lastet ned 8. juli 2022].

Motamedi, Maziar (2022b, 26. september). Why Elon Musk's Starlink will not affect protests in Iran. *Al Jazeera*. Tilgjengelig fra https://www.aljazeera.com/news/2022/9/26/why-elon-musks-starlink-wont-impact-protests-in-iran [lastet ned 5. oktober 2022].

NetBlocks (2019, 15. november). Internet disrupted in Iran amid fuel protests in multiple cities. *NetBlocks*. Tilgjengelig fra https://netblocks.org/reports/internet-disrupted-in-iran-amid-fuel-protests-in-multiple-cities-pA25L18b [lastet ned 5. juli 2022].

The New Arab (2022, 6. oktober). Iran has arrested 35 journalists since start of Mahsa Amini protests, CPJ says. *The New Arab*. Tilgjengelig fra https://english.alaraby.co.uk/news/iran-has-arrested-35-journalists-amid-mahsa-amini-protests [lastet ned 11. oktober 2022].

Newman, Lily Hay (2022, 30. september). The Challenge of Cracking Iran's Internet Blockade. *Wired*. Tilgjengelig fra https://www.wired.com/story/subvert-iran-internet-blackout/ [lastet ned 5. oktober 2022].

Norton (2021, 14. januar). What is a VPN? *Norton*. Tilgjengelig fra https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html [lastet ned 8. juli 2022].

Office of the High Commissioner for Human Rights (2022, 28. september). *Iran: UN experts demand stay of execution for two women, including LGBT activist*. Genève: OHCHR. Tilgjengelig fra https://www.ohchr.org/en/press-releases/2022/09/iran-un-experts-demand-stay-execution-two-women-including-lgbt-activist [lastet ned 7. oktober 2022].

Open Doors (2022, januar). *Iran: Full Country Dossier*. Santa Ana: Open Doors. Tilgjengelig fra https://odusa-media.com/2017/12/Full-Country-Dossier-Iran-2022.pdf [lastet ned 15. september 2022].

Penal Code (1996/2013). *Islamic Penal Code of the Islamic Republic of Iran – Book Five*. Tilgjengelig fra https://iranhrdc.org/islamic-penal-code-of-the-islamic-republic-of-iran-book-five/ [lastet ned 12. juli 2022].

Penal Code (2013). *Islamic Penal Code of the Islamic Republic of Iran*. Tilgjengelig fra https://iranhrdc.org/english-translation-of-books-i-ii-of-the-new-islamic-penal-code/ [lastet ned 12. juli 2022].

PJAK (u.å.). *PJAK*. Tilgjengelig fra https://pjak.eu/en/ [lastet ned 8. juli 2022].

Radio Farda (2019, 11. april). Iranians Return To Banned Telegram As It Proves Effective In Flood Relief. *Radio Farda*. Tilgjengelig fra https://en.radiofarda.com/a/iranians-return-to-banned-telegram-as-it-proves-effective-in-flood-relief/29874542.html [lastet ned 11. juli 2022].

Radio Farda (2020, 6. februar). Iran Court Upholds Long Prison Sentences Of Anti-Hijab Women Activists. *Radio Farda*. Tilgjengelig fra https://en.radiofarda.com/a/iran-court-upholds-long-prison-sentences-of-anti-hijab-women-activists/30420949.html [lastet ned 4. august 2022].

Radio Free Europe (2019). Iran. Iranians Sending Photos Without Hijab To Activist In U.S. Face Prison. *Radio Free Europe*. Tilgjengelig fra https://www.rferl.org/a/iranians-sending-photos-without-hijab-to-activist-in-u-s-face-prison/30082107.html [lastet ned 12. juli 2022].

Radio Free Europe (2020, 30. juni). Iranian Journalist Sentenced to Death for Role in Protests. *Radio Free Europe*. Tilgjengelig fra https://www.rferl.org/a/iranian-journalist-sentenced-to-death-for-role-in-protests/30698329.html [lastet ned 12. juli 2022].

Rashidi, Amir (2022a). *Internet Shutdown in Khuzestan and Nationwide Throttling in Response to Protests*. S.l.: Filterwatch. Tilgjengelig fra https://filter.watch/en/2022/05/09/internet-shutdown-in-khuzestan-and-nationwide-throttling-in-response-to-bread-protests/ [lastet ned 3. august 2022].

Rashidi, Amir (2022b, 17. oktober). *Women, Life, and Internet Shutdowns: Network Monitor, September 2022*. S.l.: Filterwatch. Tilgjengelig fra https://filter.watch/en/2022/10/17/women-life-and-internet-shutdowns-network-monitor-september-2022/ [lastet ned 3. november 2022].

Rashidi, Amir & Mostofi, Mani (2021, 3. november 2021). Throwing gas on the fire of Iranian internet suppression. *Atlantic Council*. Tilgjengelig fra https://www.atlanticcouncil.org/blogs/iransource/throwing-gas-on-the-fire-of-iranian-internet-suppression/ [lastet ned 8. juli 2022].

Reporters Without Borders (2017, 6. desember). *How Iran tries to control news coverage by foreign-based journalists*. Paris: Reporters without Borders. Tilgjengelig fra https://rsf.org/en/news/how-iran-tries-control-news-coverage-foreign-based-journalists [lastet ned 12. juli 2022].

Reporters Without Borders (2020, 22. januar). *Open letter about threats to Iranian journalists in six EU countries and US*. Paris: Reporters Without Borders. Tilgjengelig fra https://rsf.org/en/news/open-letter-about-threats-iranian-journalists-six-eu-countries-and-us [lastet ned 12. juli 2022].

RFE/RL, dvs. Radio Free Europe/Radio Liberty (2022, 15. august). Iranian President Signs Decree Further Restricting How Women Can Dress. *RFE/RL*. Tilgjengelig fra https://www.rferl.org/a/iran-women-dress-restrictions-raisi/31989759.html [lastet ned 11. oktober 2022].

Schwirtz, Michael (2021, 26. januar). Telegram, Pro-Democracy Tool, Struggles Over New Fans From Far Right. *The New York Times*. Tilgjengelig fra https://www.nytimes.com/2021/01/26/world/europe/telegram-app-far-right.html [lastet ned 12. juli 2022].

Simin, Kargar & Rauchfleisch, Adrian (2019). State-aligned trolling in Iran and the double-edged affordances of Instagram. *New Media & Society, 21*(7), 1506-1527. Tilgjengelig fra https://www.researchgate.net/publication/330608334_State-aligned_trolling_in_Iran_and_the_double-edged_affordances_of_Instagram [lastet ned 12. juli 2022].

Sinaiee, Maryam (2020, 30. april). Iran Sentences A Popular Instagram Couple In Self-Exile To Jail, Lashes. *Radio Farda*. Tilgjengelig fra https://en.radiofarda.com/a/iran-sentences-a-popular-instagram-couple-in-self-exile-to-jail-lashes/30585994.html.

Small Media (2017). *#IranVotes2017. Analysing the 2017 Iranian Presidential Elections through Telegram, Twitter and Instagram*. London: Small Media. Tilgjengelig fra https://smallmedia.org.uk/media/projects/files/IranVotes2017.pdf [lastet ned 30. juni 2022].

Small Media (u.å.). *Iran's Cyber Police— 'Society-Based Policing' and the Rise of Peer Surveillance*. London: Small Media. Tilgjengelig fra https://smallmedia.org.uk/news/irans-cyber-police-society-based-policing-and-the [lastet ned 30. juni 2022].

Spence, Thomas (2018, 8. september). PST: «Sannsynlig» at Sandbergs sikkerhetsbrudd er blitt misbrukt av Kina og Iran. *Aftenposten*. Tilgjengelig fra https://www.aftenposten.no/norge/politikk/i/5VgpoX/pst-sannsynlig-at-sandbergs-sikkerhetsbrudd-er-blitt-misbrukt-av-kina-og-iran [lastet ned 6. juli 2022].

Strzyżyńska, Weronika (2022, 5. september). Iranian authorities plan to use facial recognition to enforce new hijab law. *The Guardian*. Tilgjengelig fra https://www.theguardian.com/global-development/2022/sep/05/iran-government-facial-recognition-technology-hijab-law-crackdown [lastet ned 11. oktober 2022].

U.S. Department of State (2020). *Iran 2019 International Religious Freedom Report*. Washington D.C.: U.S. Department of State. Tilgjengelig fra https://www.state.gov/wp-content/uploads/2020/06/IRAN-2019-INTERNATIONAL-RELIGIOUS-FREEDOM-REPORT.pdf [lastet ned 13. juli 2022].

U.S. Department of State (2021, 30. mars). *2020 Country Reports on Human Rights Practices: Islamic Republic of Iran*. Washington D.C.: U.S. Department of State,. Tilgjengelig fra https://www.state.gov/reports/2020-country-reports-on-human-rights-practices/iran/ [lastet ned 12. juli 2022].

U.S. Department of State (2022, 12. april). *2021 Country Reports on Human Rights Practices: Iran*. Washington D.C.: U.S. Department of State. Tilgjengelig fra https://www.state.gov/wp-content/uploads/2022/03/313615_IRAN-2021-HUMAN-RIGHTS-REPORT.pdf [lastet ned 30. juni 2022].

U.S. Department of the Treasury (2022, 23. september). *U.S. Treasury Issues Iran General License D-2 to Increase Support for Internet Freedom*. Washington D.C.: U.S. Department of the Treasury. Tilgjengelig fra https://home.treasury.gov/news/press-releases/jy0974 [lastet ned 5. oktober 2022].

UN Special Rapporteur, dvs. UN Special Rapporteur on the situation of human rights in the Islamic Republic of Iran (2021, 11. januar). *Situation of human rights in the Islamic Republic of Iran. Report of the Special Rapporteur on the situation of human rights in the Islamic Republic of Iran*. New York: UN Human Rights Council. Tilgjengelig fra https://www.ecoi.net/en/file/local/2045194/A_HRC_46_50_E.pdf [lastet ned 30. juni 2022].

UN Special Rapporteur, dvs. UN Special Rapporteur on the situation of human rights in the Islamic Republic of Iran (2022). *Situation of human rights in the Islamic Republic of Iran. Report of the Special Rapporteur on the situation of human rights in the Islamic Republic of Iran, Javaid Rehman*. New York: UN Human Rights Council. Tilgjengelig fra https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/005/44/PDF/G2200544.pdf?OpenElement [lastet ned 15. juli 2022].

USCIRF, dvs. U.S. Commission on International Religious Freedom (2021, august). *Country Update Iran: Religious Freedom Conditions in Iran*. Washington D.C.: USCIRF. Tilgjengelig fra https://www.uscirf.gov/sites/default/files/2021-08/2021%20Iran%20Country%20Update.pdf [lastet ned 31. juli 2022].

USCIRF, dvs. U.S. Commission on International Religious Freedom (2022a). *Sepideh Rashnu*. Washington D.C.: USCIRF. Tilgjengelig fra https://www.uscirf.gov/religious-prisoners-conscience/forb-victims-database/sepideh-rashnu [lastet ned 12. oktober 2022].

USCIRF, dvs. U.S. Commission on International Religious Freedom (2022b, 25. april). *USCIRF Annual Report 2022: Iran*. Washington D.C.: USCIRF. Tilgjengelig fra https://www.uscirf.gov/annual-reports?country=49 [lastet ned 13. juli 2022].

WHO, dvs. World Health Organization (2022, 5. juli). *Iran (Islamic Republic of)*. Genève: WHO. Tilgjengelig fra https://www.who.int/countries/irn/ [lastet ned 6. juli 2022].

Muntlige kilder

Bjørn Svenungsen, tidligere høgskolelektor, telefonsamtale 4. mai 2021.

Censored Planet, e-post september 2021.

Diplomatkilde, e-post oktober 2021.

Diplomatkilde, e-post november 2021.

Diplomatkilde, e-post januar 2022.

Diplomatkilde, e-post mai 2022.

Diplomatkilde, e-post november 2022.

Iransk jurist, e-post februar 2021.

Iransk jurist, digitalt møte (Teams) februar 2021.

Komala-CPI, samtale med partiets ledelse i Sergwes, Sulaymaniya, oktober 2019.

Nasjonalt ID-senter, e-post april 2021.

OONI, dvs. Open Observatory for Network Interference. E-post, august 2021.

PJAK, samtale med representanter for partiet, Sulaymaniya, oktober 2019.