LANDINFO

Utlendingsforvaltningens fagenhet for landinformasjon

Temanotat

Iran

Internett og sosiale medier

31. mai 2021

Alle henvendelser om Landinfos rapporter kan rettes til:

Landinfo
Utlendingsforvaltningens fagenhet for landinformasjon

Storgata 33 A
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, about 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 developed a local, state-controlled network, National Information Network (NIN).

Social media platforms such as Telegram, Twitter, Facebook and YouTube 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 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, om lag 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 utarbeidet et lokalt, statskontrollert nettverk, National Information Network (NIN).

Sosiale medieplattformer som Telegram, Twitter, Facebook og YouTube 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

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, 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. Oppbygging 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.

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 2020, s. 1).

FNs spesialrapportør for menneskerettigheter i Iran (2021, s. 7) 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. Mange brukte også smarttelefon, hele to tredjedeler av befolkningen. 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 (Small Media 2017, s. 8; Ehlson et al. 2012).

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 (Gilbrant 2010; Bekkevang 2017, s. 14).

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 2018a, s. 18).

Informasjons- og kommunikasjonsteknologien (IKT) er kontrollert av myndighetene, både gjennom direkte eierskap og politisk kontroll (Freedom House 2020, s. 2; Article 19 2020, s. 23). 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 2018a, 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 2018a, s. 18) innebærer dette at presidenten og representanter for hans kabinett bare spiller en beskjeden rolle. Under valgkampen forut for presidentvalget i 2017 lovet president Hassan Rouhani å beskytte iranernes tilgang til det globale internettet. Rouhani har ikke vært 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 2018a, s. 8; Freedom House 2020, s. 10).

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, som kommuniseres til relevante myndigheter for implementering (Article 19 2017, s. 19). Freedom House (2020, s. 14) understreker at slike beslutninger ofte er vilkårlige, og at det foreligger lite informasjon om beslutninger og prosesser i komiteen. Det er flere myndighetsorgan som kan beslutte blokkering eller filtrering uten at CCDOC har vært involvert (Article 19 2017, s. 19, 20).

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 (U.S. Department of State 2020a, s. 23; DFAT 2020, s. 44).

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

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 datakriminalitet – Iranian Cyber Police (FATA) (Article 19 2020, s. 9). Det er relativt lite tilgjengelig informasjon om FATA; både hvordan de opererer, og hvilke metoder de benytter.

Ifølge Small Media (2019) 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 i løpet av de siste åtte årene. 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 2019).

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 eventuell straff som idømmes (Small Media 2019).

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 IRCG 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 IRCGs 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 2019). 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 (2019) 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).

Høgskolelektor 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». Tanken er å styrke lokale plattformer, utarbeide gode tekniske løsninger, og på den måten legge til rette for at iranerne velger det lokale nettet. Den formelle lanseringen var 28. august 2016. NIN er et statskontrollert nettverk med søkemotor og epost-tjenester. 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 2018a, s. 26, 27).

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. 24, 23, 25; CHRI 2018a, s. 20, 27).

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 betydelig. 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 2018a, s. 27).

Ifølge en rapport fra IKT-minsteriet[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 (Freedom House 2020; Article 19 2020, s. 23).

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 2018, 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. Ifølge tall fra Article 19 brukte 57,4 millioner av en befolkning på 82 millioner internett i 2020, hvilket utgjør en andel på om lag 70 prosent (Article 19 2020, s. 13).

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 internett, og at fire av fem iranere skulle ha tilgang gjennom bredbånd (Freedom House 2020).

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 2020).

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

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

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).

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, fingeravtrykk og signatur. Kortet utleveres med PIN-koder som gir innehaveren tilgang til offentlige tjenester via internett (Landinfo 2021, 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, epost 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, epost 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, øke hastigheten og senke prisene. 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)[3] 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 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 2020a, 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[4] – 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, med påfølgende nedstengning fra myndighetene. 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).

Myndighetene oppnår flere ting med å stenge ned 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.

[3] 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 1979).

[4] Såkalte ISP; Internet Service Providers.

- 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 (Svenungsen, mai 2021; Article 19 2020, s. 14).

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).

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 (Rinvik Bratberg & Raake 2021).

Ifølge ekspert på IKT og sikkerhet Amir Rashidi (som gjengitt i CHRI 2021) 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 (CHRI 2021; Article 19 2020, s. 26).

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 2021).

Blokkering og filtrering kan omgås ved bruk av tekniske løsninger (se 4.2.). 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 Github, Amazon Cloud og Google Cloud (Article 19 2020 s. 26).

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. Lederen av FATA, Vahid Majid, kunngjorde at det var opprettet en arbeidsgruppe som skulle bekjempe rykter om spredning av viruset på nett (Freedom House 2020). 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).

Iran har blitt hardt rammet av covid 19, og pr. mars 2021 var mer enn 60 000 registrert døde i pandemien (diplomatkilde, mars 2021).

3.2.1 Blokkering og filtrering

En strategi som myndighetene benytter, er å blokkere eller filtrere enkelte nettsteder – enten i en periode eller permanent. Twitter, Facebook og YouTube er blokkert og ikke tilgjengelig, i likhet med Blogspot, Blogger og WordPress (Freedom House 2020, s. 10). Article 19 (2017, s. 16) forklarer forskjellen mellom blokkering og filtrering slik: Ved blokkering hindres tilgang totalt, mens ved filtrering er det elementer som fanges opp av filteret.

I 2017 hadde Iran blokkert eller filtrert en fjerdedel av alt tilgjengelig materiale på internett. Tilgangen til tusenvis av nettsteder begrenses, herunder blant annet tilgangen til internasjonale nyhetsmedier og menneskerettighetsorganisasjoner, nettsteder med tilknytning til den politiske opposisjonen, etniske og religiøse minoriteter, og andre regimekritiske nettsteder. 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, s. 10).

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, s. 10-12). En annen metode som har blitt benyttet, eksempelvis under presidentvalget i 2013, er å redusere hastigheten på nettet betydelig, og på den måten påvirke befolkningen til ønsket adferd (Article 19 2020, s. 14).

3.2.2 Cyberangrep og overvåking på internett

Ifølge CHRI (2018a, 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 IRCG, og i mindre grad Ministeriet for etterretning, som står bak nett-angrepene (CHRI 2018a, 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.

3.2.2.1 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 2018a, s. 48).

En utbredt strategi er å innhente informasjon på individnivå og infiltrere ulike digitale nettverk. Ifølge Article 19 (som gjengitt i Migrationsverket 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. 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 (2018a, 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 epost, 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 epost-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 kvinne-aktivister og den politiske opposisjonen.

Ifølge Miaan Group (gjengitt i Bergman & Fassihi 2020) har myndighetsaffilierte iranske hackere kommet inn på krypterte applikasjoner som Telegram og WhatsApp. De har også kommet inn på tidligere antatt sikre mobiltelefoner og datamaskiner. Det dreier seg blant annet om phishing-angrep der de har utarbeidet falske Android-applikasjoner, og på den måten forledet brukere til å oppgi brukernavn og passord.

- **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. Dersom kodene kommer på 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 skal ha 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 programmet som gjør at angriperne får tilgang til all informasjon på enheten (Bergman & Fassihi 2020).

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 & Sadjadpour 2018, s. 5).

Ifølge flere kilder som svenske Migrationsverket (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).

Ifølge Bjørn Svenungsen, høgskolelektor i cybersikkerhet ved Institutt for forsvarsstudier (IFS) (som gjengitt i Finsveen 2020) er ikke Iran helt på nivå med USA, Kina og Russland. Iranske cyberangrep synes å være «godt organisert», ifølge høgskolelektoren.

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 Strategier for å unngå sensur og blokkeringer

På tross av den omfattende sensuren, blokkeringen/filtreringen og de ulike cyberangrepene, 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.

4.1 Selvsensur

Sosiologen Ali Honari (2018, 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, 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).

Ifølge Freedom House (2020, s. 16) ble situasjonen noe bedre for reformvennlige journalister etter at Rouhani overtok presidentvervet i 2013. Kritikk av regimet, øverste leder, profeten og fundamentet for det islamske styresettet slås fortsatt hardt ned på.

4.2 Bruk av omgåelsesverktøy som VPN

På tross av myndighetenes forsøk på å kontrollere befolkningens bruk av internett, kan forbudte 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, s. 7).

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.

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.

Det har lenge vært uklart om iranske myndigheter har teknisk kompetanse til å overvåke kommunikasjon sendt kryptert i utenlandske sosiale nettverk. Svenske Migrationsverket hevder i en rapport av 2020 (s. 21) at mye tyder på at slike nettverk er tryggere enn lokale kommunikasjonsplattformer, som ikke beskytter brukerdata i samme grad.

Svenungsen (mai 2021) uttalte til Landinfo at det ikke er holdepunkter for at iranske myndigheter får tilgang til godt kryptert materiale. 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 ulike VPN-løsninger som også er tilgjengelig i Iran.

5 Den regimekritiske aktiviteten og debatten foregår i stor grad på internett

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 og tilknytning til de kurdiske partiene. Spørsmålene dreier seg ofte om kommunikasjonsmønster samt bruk av internett og sosiale medier.

5.1 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 (Danish Immigration Service 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 Danish Immigration Service 2020b, 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 opplyste i samtale med Landinfo (oktober 2019) at internett har gjort det lettere enn tidligere å spre partiets budskap blant iranske kurdere. Også PJAK[5]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.).

5.2 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 (Migrationsverket 2020, s. 23; Landinfo 2017, s. 9). Bibelen på persisk kan gratis lastes ned fra nettet, og mye annet kristent materiell er også tilgjengelig.

En kilde som danske Udlændigestyrelsen (Danish Immigration Service & Danish Refugee Council 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.

Article 18, en kristen menneskerettighetsorganisasjon som arbeider for religionsfrihet i Iran (som gjengitt i Migrationsverket 2020, s. 21) 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.

[5] 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.

5.3 Bruk av sosiale medier

På 2000-tallet begynte det som Article 19 (2017, s. 23) beskriver som «blogging fever». De senere årene har sosiale medier blitt viktige plattformer, men Facebook, Twitter, Telegram og YouTube er blokkert. Den 25. januar 2021 ble den krypterte meldingstjenesten Signal blokkert (Rashidi 2021). I tillegg er blogger-plattformer som Blogspot og Blogger blokkert (Freedom House 2020, s. 10). Det er imidlertid et paradoks at Irans lederskap, herunder øverste leder Ali Khamenei og president Rouhani, er aktive brukere av Twitter, blant annet som ledd i utenrikspolitikken og retorikken mot USA og tidligere president Trump (Arouzi & De Luce 2019).

Instagram er en av få sosiale medier som er tillatt. Instagram er populært og har mange bruker. 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 kommunikasjonskanalen i landet (Erdbrink 2018).

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 2017; Small Media 2019)

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 av grunnene til at Instagram ikke forbys, kan være fordi plattformen brukes aktivt av det iranske regimet og deres tjenestemenn. President Rouhani har mer enn to millioner følgere og Instagram spilte en betydelig rolle under presidentvalget i 2017. Øverste leder Khamenei hadde i 2017 om lag 1,6 millioner følgere. Han legger daglig ut oppdateringer, eksempelvis taler, bilder, fordømming av andre land og liknende (Erdbrink 2018).

5.3.1 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 følgere, 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. President Rouhani var uttalt motstander av forbudet, men var ikke i stand til å stoppe det. Ifølge CHRI (2018b, s. 11) illustrerer dette hvor irrelevant og marginalisert president Rouhani er, 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 (Radio Farda 2019; Marchant 2019; Article 19 2020, s. 24).

Ifølge en artikkel i New York Times (Schwirtz 2021) har forbudet utgjort liten forskjell. Telegram er fortsatt den foretrukne kanalen for å holde seg informert, og iranere bruker VPN-nettverk for å omgå myndighetenes forbud og blokkering. «Alle» bruker Telegram, selv besteforeldre som vanligvis ikke beveger seg på digitale plattformer, ifølge journalisten.

6 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 (Migrationsverket 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 (2020a, s. 27) 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).

6.1 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 de følges tett av iranske sikkerhetsmyndigheter. Kanaler og medier med mange følgere, som eksempelvis Telegram, blir som tidligere nevnt fulgt ekstra godt med på (Migrationsverket 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).

6.2 Iranere i utlandet

Iranere i utlandet er underlagt iransk lov, og kan ifølge straffeloven (Islamic Penal Code 2013, artikkel 7) straffeforfølges i Iran for lovbrudd begått i utlandet. En iransk jurist (digitalt møte 2021) nyanserte bildet, og forklarte at det primært er sikkerhetsrelaterte lovbrudd – av både intern og ekstern karakter – som straffeforfølges i Iran selv om de 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, det åpner mulighet for å utøve makt rettet mot egne borgere utenfor landets grenser. 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 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.

Ifølge en diplomatkilde (2020) er arrestasjoner og dødsdommer mot iranere med oppholdstillatelse eller statsborgerskap i vestlige land blitt mer utbredt. I desember 2020 var om lag 40 personer med doble statsborgerskap i iransk rettsvesen sin varetekt. Diplomatkilden mener at motivet kan være å samle forhandlingskort overfor vestlige land. I en del av sakene gjelder tiltalen ulike former for spionasje.

6.2.1 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 (Reporteres without Borders 2020).

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,[6] Voice of America, Deutsche Welle og Radio France Internationale er også utsatt, ifølge Reporters without Borders (2017; 2020).

6.2.2 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. 5)?

7 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).

7.1 Lovgivning som kan komme til anvendelse

Straffeloven inneholder flere vagt formulerte straffebud med svært vide strafferammer. 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

[6] 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, epost 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 år. 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. Kapittel 2 (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. Vurderingen av om vilkårene for sensur er oppfylt kan synes vilkårlige, og det er lite informasjon tilgjengelig om beslutningsprosessene (Freedom House 2020, s. 14).

På den andre siden er det 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 2020, s. 17).

7.2 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 2020; RFE 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).

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 (CHRI 2014; CHRI 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 RFL 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.

Det foreligger imidlertid andre rapporterte tilfeller av at aktivister som kjemper mot tvungen bruk av hijab har blitt arrestert. 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 har dømt aktivistene til lange fengselsstraffer. Den lengste straffen ble idømt Keshavarz, og var på over 20 år. Sakene har fått internasjonal oppmerksomhet, blant annet fra Human Rights Watch og FN (U.S. Department of State 2020b, 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 revolusjonsdomstol 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).

8 Referanser

Skriftlige kilder

Anderson, C. & Sadjadpour, K. (2018). *Iran's cyber threat.* Carnegie Endowment for International Peace. Washington D.C.: CEIP. Tilgjengelig fra Iran_Cyber_Final_Full_v2.pdf (carnegieendowment.org) [lastet ned 3. mars 2021]

Amnesty International (2020, 18. februar). *Human Rights in Iran: Review of 2019.* London: Amnesty International. Tilgjengelig fra Amnesty Public Statement [lastet ned 18. mai 2021]

Article 19 (2012). *Islamic Republic of Iran: Computer Crimes Law*. London: Article 19. Tilgjengelig fra 12-01-30-FINAL-iran-WEB[4].pdf (article19.org) [lastet ned 20. mai 2021]

Article 19 (2017, 3. februar). *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 26. februar 2021]

Article 19 (2020, september). *Iran: Tightening the Net 2020 After Blood and Shutdowns.* London: Article 19. Tilgjengelig fra TTN-report-2020.pdf (article19.org) [lastet ned 15. februar 2021]

Arouzi, A. & De Luce, D. (2019, 21. august). Tech-savvy Iranians stay connected on social media despite regime restrictions. *NBC News.* Tilgjengelig fra Tech-savvy Iranians stay connected on social media despite regime restrictions (nbcnews.com) [lastet ned 11. februar 2021]

Badiei, F. (2020). *The Tale of Telegram Governance: When the Rule of Thumb Fails.* New Haven: Yale's Justice Collaboratory. Tilgjengelig fra telegram-governance-publish.pdf (yale.edu) [lastet ned 22. februar 2021]

BBC News (2020, 13. desember). Ruhollah Zam: EU powers boycott Iran forum over execution. *BBC News.* Tilgjengelig fra Ruhollah Zam: EU powers boycott Iran forum over execution - BBC News [lastet ned 4. februar 2021]

Bekkevang, M. A. (2017). *Cyberangrep. En risiko for Norge.* Oslo: Krigsskolen. Tilgjengelig fra 2017-04-03 (U) Bekkevang, Kull Krebs, Bacheloroppgave.pdf (unit.no) [lastet ned 5. mai 2021]

Bergman, R. & Fassihi, F. (2020, 18. september). Iranian Hackers Found Way Into Encrypted Apps, Researchers Say. *The New York Times.* Tilgjengelig fra Iranian Hackers Can Beat Encrypted Apps like Telegram, Researchers Say - The New York Times (nytimes.com) [lastet ned 11. mars 2021]

Beste VPN Norge (u.å.). Hva er VPN og hvordan kan det hjelpe deg? *Beste VPN Norge.* Tilgjengelig fra Hva er en VPN tjeneste? - Enkel forklaring og veiledning (bestevpnnorge.no) [lastet ned 11. februar 2021]

Cedoca (2020, 30. mars). *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 11. mars 2021]

CHRI, dvs. Center for Human Rights in Iran (2014, 27. mai). *Eight Facebook Users Sentenced to Decades in Prison.* New York: CHRI. Tilgjengelig fra Eight Facebook Users Sentenced to Decades in Prison – Center for Human Rights in Iran (iranhumanrights.org) [lastet ned 28. april 2021]

CHRI (2015, 4. august). *Facebook Activist Details How She Received a Seven-Year Prison Sentence in Iran.* New York: CHRI. Tilgjengelig fra Facebook Activist Details How She Received a Seven-Year Prison Sentence in Iran – Center for Human Rights in Iran (iranhumanrights.org) [lastet ned 18. mai 2021]

CHRI (2018a, januar). *Guards at the Gate: The Expanding State Control Over the Internet in Iran*. New York: CHRI. Tilgjengelig fra https://www.iranhumanrights.org/wp-content/uploads/EN-Guards-at-the-gate-High-quality.pdf [lastet ned 2. mars 2021]

CHRI (2018b, juni). *Closing of the Gates. Implications of Iran's Ban on the Telegram Messaging App.* New York: CHRI. Tilgjengelig fra Closing-the-gates-3-online.pdf (iranhumanrights.org) [lastet ned 25. mars 2021]

CHRI (2021, 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-s-government-companies-can-do-more-to-promote-internet-freedom-in-iran/ [lastet ned 18. mars 2021]

[Constitution] (1979, 24. oktober). The Constitution of the Islamic Republic of Iran. Tilgjengelig via Refworld http://www.refworld.org/docid/3ae6b56710.html [lastet ned 15. mars 2021]

Danish Immigration Service (2020a, juli). *November 2019 Protests.* København: Danish Immigration Service. Tilgjengelig fra K:\Kontoret for Landedokumentation\OSINT-Team\Analyseprodukter\Iran - analyse\Endelige rapport\Forside forslag 2 (ecoi.net) [lastet ned 28. april 2021]

Danish Immigration Service (2020b, februar). *Iranian Kurds Consequences of political activities in Iran and KRI.* København: Danish Immigration Service. Tilgjengelig fra Report on Iranian Kurds Feb 2020 (4).pdf [lastet ned 22. februar 2021]

Danish Immigration Service & Danish Refugee Council (2018, februar). *Iran: House Churches and Converts*. København: Udlændigestyrelsen & Dansk Flygtningehjælp. Tilgjengelig fra https://www.nyidanmark.dk/da/Words%20and%20Concepts%20Front%20Page/US/Asylum/landerapporter [lastet ned 25. februar 2021]

Danish Immigration Service (2013). *Iranian Kurds.* København: Danish Immigration Service. Tilgjengelig fra 1226_1380796700_fact-finding-iranian-kurds-2013.pdf (ecoi.net) [lastet ned 19. mars 2021]

Deutsche Welle (2019, 5. desember). Iranian journalists in Europe face threats and harassment from regime in Tehran. *Deutsche Welle.* Tilgjengelig fra Iranian journalists in Europe face threats and harassment from regime in Tehran | Asia| An in-depth look at news from across the continent | DW | 05.12.2019 [lastet ned 25. februar 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 4. mars 2021]

Ehlson, S. B., Yeung, D., Roshan, P., Bohandy, S. R. & Nader, A. (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 Background on Social Media Use in Iran and Events Surrounding the 2009 Election (jstor.org) [lastet ned 4. februar 2021]

Erdbrink, T. (2018). Vår mann i Teheran. *NRK*. Tilgjengelig på NRK.TV Vår mann i Teheran – 1. episode (Sesong 2) – NRK TV [lastet ned 12. februar 2021]

Ershad, A. (2020, 22. april). 8 In Iran, poverty and lack of internet make distance learning impossible. *The Observers.* Tilgjengelig fra In Iran, poverty and lack of internet make distance learning impossible (france24.com) [lastet ned 16. mars 2021]

FIDH, dvs. International Federation for Human Rights (2020, oktober). *No one is spared. The widespread use of the death penalty in Iran.* Paris: FIDH. Tilgjengelig fra iranpdm758ang.pdf (fidh.org) [lastet ned 23. februar 2021]

Finsveen, J. N. (2020, 17. januar). Det massive angrepet «ingen» merket. *Dagbladet.* Tilgjengelig fra https://www.dagbladet.no/nyheter/det-massive-angrepet-ingen-merket/72029080 [lastet ned 28. april 2021]

Freedom House (2020). *Freedom on the net 2020. Iran.* Washington D.C.: Freedom House. Tilgjengelig fra Iran | Freedom House [lastet ned 4. februar 2021]

Frenkel, S. (2018, 2. januar). Iranian Authorities Block Access to Social Media Tools. *The New York Times.* Tilgjengelig fra Iranian Authorities Block Access to Social Media Tools - The New York Times (nytimes.com) [lastet ned 18. mars 2021]

Gilbrant, J. (2010, 15. desember). «Stuxnet» har satt Iran to år tilbake. *Dagbladet.* Tilgjengelig fra - «Stuxnet» har satt Iran to år tilbake (dagbladet.no) [lastet ned 5. mai 2021]

Honari, A. (2018). "We Will Either Find a Way, or Make One": How Iranian Green Movement Online Activists Perceive and Respond to Repression. *Social Media + Society*. Tilgjengelig fra https://journals.sagepub.com/doi/10.1177/2056305118803886 [lastet ned 25. februar 2021]

Jedina, M. (2020, 25. mars). Iran Uses Arrests, Censorship to Silence Critical COVID-19 Coverage. *Voice of America.* Tilgjengelig fra Iran Uses Arrests, Censorship to Silence Critical COVID-19 Coverage | Voice of America - English (voanews.com) [lastet ned 16. mars 2021]

Landinfo (2021, 5. januar). *Pass, ID- og sivilstatusdokumenter.* Oslo: Landinfo. Tilgjengelig fra Iran: Pass, ID- og sivilstatusdokumenter og pass (landinfo.no) [lastet ned 28. april 2021]

Landinfo (2020, 12. august). *The Iranian Welfare System.* Oslo: Landinfo. Tilgjengelig fra Report-Iran-Welfare-system-12082020.pdf (landinfo.no) [lastet ned 3. mars 2021]

Landinfo (2017, 27. november). *Iran: Kristne konvertitter og hjemmekirker (1) – utbredelse og vilkår for trosutøvelse.* Oslo: Landinfo. Tilgjengelig fra Iran: Kristne konvertitter og hjemmekirker (1) - utbredelse og vilkår for trosutøvelse (landinfo.no) [lastet ned 16. februar 2021]

MacLellan, S. (2018, 9. januar). What you need to know about Internet Censorship in Iran. *Centre for International Governance Innovation*. Tilgjengelig fra What You Need to Know about Internet Censorship in Iran | Centre for International Governance Innovation (cigionline.org) [lastet ned 11. februar 2021]

Malekian, S. (2019, 7. oktober). Iranian social media influencer arrested for 'encouraging youths to corruption'. *ABC News.* Tilgjengelig fra Iranian social media influencer arrested for 'encouraging youths to corruption' - ABC News (go.com) [lastet ned 24. mars 2021]

Marchant, J. (2019, 20. mai). FATA watch/01 – Iranian Cyber Police Monitoring. *Filterwatch.* Tilgjengelig fra FATAwatch//01 — Iranian Cyber Police Monitoring | by James Marchant | Filterwatch | Medium [lastet ned 11. februar 2021]

Michaelsen, M. (2018). Exit and voice in a digital age: Iran's exiled activists and the authoritarian state. *Globalizations 15*(2), 248-264. Tilgjengelig fra Exit and voice in a digital age: Iran's exiled activists and the authoritarian state (tandfonline.com) [lastet ned 18. mars 2021]

Michaelsen, M. (2017). Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran. *Surveillance and Society 15*(3/4), 465-470. Tilgjengelig fra https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6635/6436 [lastet ned 18. mars 2021]

Migrationsverket (2020). *Situationen för konvertiter och regimens övervakning av internet och sociala medier.* Norrkøping: Migrationsverket. Tilgjengelig fra Dokument - Lifos extern (migrationsverket.se) [lastet ned 22. februar 2021]

NetBlocks (2019, 15. november). Internet disrupted in Iran amid fuel protests in multiple cities. *NetBlocks.* Tilgjengelig fra Internet disrupted in Iran amid fuel protests in multiple cities - NetBlocks [lastet ned 18. mai 2021]

Norton (2021, 14. januar). What is a VPN? *Norton*. Tilgjengelig fra What is a VPN? | Virtual Private Networks Explained | Norton [lastet ned 19. mai 2021]

[Penal Code] (2013). The Islamic Penal Code of Iran. Tilgjengelig fra English Translation of Books I & II of the New Islamic Penal Code - Iran Human Rights Documentation Center (iranhrdc.org) [lastet ned 4. mars 2021]

[Penal Code, Book 5] (1996/2013). Islamic Penal Code of the Islamic Republic of Iran – Book Five. Tilgjengelig fra Islamic Penal Code of the Islamic Republic of Iran – Book Five - Iran Human Rights Documentation Center (iranhrdc.org) [lastet ned 19. mai 2021]

Peltier, E (2021, 13. februar). Academic Fcing Jail in Iran escapes to U.K. *The New York Times.* Tilgjengelig fra Academic Facing Jail in Iran Escapes to U.K. - The New York Times (nytimes.com) [lastet ned 3. mars 2021]

PJAK (u.å.). PJAK. *PJAK.* Tilgjengelig fra https://pjak.eu/en [lastet ned 19. mars 2021]

Radio Farda (2019, 11. april). Iranians Return To Banned Telegram As It Proves Effective In Flood Relief. *Radio Farda.* Tilgjengelig fra Iranians Return To Banned Telegram As It Proves Effective In Flood Relief (radiofarda.com) [lastet ned 15. februar 2021]

Rashidi, A. (2021, 9. februar). Network Monitor – January 2021. *Filterwatch.* Tilgjengelig fra Network Monitor – January 2021 - Filterwatch [lastet ned 22. februar 2021]

RFE, dvs. Radio Free Europe (2020, 30. Juni). Iranian Journalist Sentenced to Death for Role in Protests. *RFE.* Tilgjengelig fra Iranian Journalist Sentenced To Death For Role In Protests (rferl.org) [lastet ned 4. februar 2021]

RFE (2019, 29. juli). IRAN. Iranians Sending Photos Without Hijab To Activist In U.S. Face Prison. *RFE.* Tilgjengelig fra Iranians Sending Photos Without Hijab To Activist In U.S. Face Prison (rferl.org) [lastet ned 23. februar 2021]

Reporters without Borders (2017, 6. september). How Iran tries to control news coverage by foreign-based journalists. *Reporters without Borders.*Tilgjengelig fra How Iran tries to control news coverage by foreign-based journalists | RSF [lastet ned 19. mars 2021]

Reporters without Borders (2020, 22. januar). Open letter about threats to Iranian journalists in six EU countries and US. *Reporters without Borders.*Tilgjengelig fra Open letter about threats to Iranian journalists in six EU countries and US | RSF [lastet ned 23. mars 2021]

Rinvik Bratberg, K. L. & Raake, H. (sist endret 2. februar 2021). *Atomavtalen og håpet som brast.* Oslo: Folk og Forsvar. Tilgjengelig fra Atomavtalen og håpet som brast - Folk og Forsvar [lastet ned 18. mars 2021]

Schwirtz, M. (2021, 26. januar). Telegram, Pro-Democracy Tool, Struggles Over New Fans From Far Right. *The New York Times.* Tilgjengelig fra Telegram Messaging App Struggles Over New Fans From Far Right - The New York Times (nytimes.com) [lastet ned 22. februar 2021]

Simin, K. & Rauchfleisch, A. (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 25. februar 2021]

Sinaiee, M. (2020, 30. april). Iran Sentences A Popular Instagram Couple In Self-Exile To Jail, Lashes. *Radio Farda.* Tilgjengelig fra Iran Sentences A Popular Instagram Couple In Self-Exile To Jail, Lashes (radiofarda.com) [lastet ned 4. mars 2021]

Small Media ([2019], 20. februar). *Iran's Cyber Police—'Society-Based Policing' and the Rise of Peer Surveillance.* London: Small Media.Tilgjengelig fra Iran's Cyber Police—'Society-Based Policing' and the Rise of Peer Surveillance – Small Media Foundation [lastet ned 18. mai 2021]

Spence, T. (2018, 8. september). PST: «Sannsynlig» at Sandbergs sikkerhetsbrudd er blitt misbrukt av Kina og Iran. *Aftenposten.* Tilgjengelig fra PST: «Sannsynlig» at Sandbergs sikkerhetsbrudd er blitt misbrukt av Kina og Iran (aftenposten.no) [lastet ned 19. mars 2021]

York, J. C. (2012, 2. oktober). Is Iran's halal internet possible? *Al Jazeera*. Tilgjengelig fra Is Iran's halal internet possible? | Science and Technology News | Al Jazeera [lastet ned 3. februar 2021]

UN Special Rapporteur (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 OHCHR. Tilgjengelig fra A_HRC_46_50_E.pdf (ecoi.net) [lastet ned 16. februar 2021]

U.S. Department of State (2020a). *Iran 2019. Human Rights Report.* Washington D.C.: U.S. Department of State. Tilgjengelig fra IRAN 2019 HUMAN RIGHTS REPORT (state.gov) [lastet ned 1. mars 2021]

U.S. Department of State (2020b). *Report on International Religious Freedom: Iran.* Washington D.C.: U.S. Department of State. Tilgjengelig fra IRAN 2019 INTERNATIONAL RELIGIOUS FREEDOM REPORT (state.gov) [lastet ned 1. mars 2021]

Muntlige kilder

Diplomatkilde, epost desember 2020.

Diplomatkilde, epost mars 2021.

Europeisk utlendingsenhet, seminar i Landinfo 2017.

Høgskolelektor Bjørn Svenungsen, telefonsamtale 4. mai 2021.

Iransk jurist, epost februar 2021.

Iransk jurist, digitalt møte (Teams) februar 2021.

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

Nasjonalt ID-senter, epost april 2021.

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