Faktanotat

Til: NBIM v/ Carine Smith Ihenacho, leder for eierskapsavdelingen

Fra: Amnesty International

Dato: 27.11.2017

Ang investeringen til Statens pensjonsfond Utland i Saudi Telecom Company

NBIM foretok den første investeringen på det saudiske markedet i 2. kvartal 2015. Blant de 34 saudiske selskapene fondet kjøpte aksjer i, er Saudi Telecom Company (STC). Investeringen i STC har gjort oljefondet til medeier i det største telekom-selskapet i Saudi-Arabia som er kontrollert av den saudiske staten.

1. Problemstilling

Amnesty International vil med dette faktadokumentet redegjøre for den dokumentasjon vi har kunnet fremskaffe om STC, det statlige overvåkningsregimet i Saudi-Arabia samt rollen til STC og andre telekom-operatører på det saudiske markedet. Dokumentasjonen tilsier at det er en kobling mellom STC, direkte og indirekte gjennom selskapets majoritetseier, den saudiske staten, og overvåkning av saudiske mobil- og nettkunder som fører til straffeforfølgelse, inkludert bruk av dødsstraff, mot saudiske menneskerettighetsforkjempere.

Norge har definert arbeid for menneskerettighetsforkjempere som en utenrikspolitisk topp-prioritet, og, i tillegg til de etiske retiningslinjene NBIM er pålagt å følge, har NBIM et eget forventningsdokument på menneskerettigheter som skal følges.

Amnesty International mener oljefondet bør foreta en gjennomgang av hvorvidt fondets investering i STC er i samsvar med fondets etiske retningslinjer. Vi anbefaler videre at en tilsvarende gjennomgang gjøres for de øvrige investeringene i statskontrollerte saudiske selskaper.

2. Bakgrunn

2.1. Oljefondets investeringer i Saudi-Arabia

Såvidt Amnesty International forstår, investerte Norges Bank Investment Management (NBIM) for første gang i selskaper på det saudiske markedet 2. kvartal 2015. I juni 2015 annonserte Saudi-Arabia at de ville åpne for at internasjonale investorer for første gang kunne investere i aksjemarkedet gjennom tildelte kvoter. Fondet investerte i saudiske deltakelsessertifikater. I praksis betyr det at fondet kjøpte aksjeposter i 34 saudiske selskaper for en verdi av totalt 3500 mil NOK. Selskapene er fordelt på de fleste bransjer. Den samlede verdien av de saudiske aksjepostene hadde ifølge NBIMs nettsider økt til 3933 mil NOK pr 2016. NBIM kjøpte bl.a. en aksjepost i Saudi Telecom Company (STC) på 0,04 % som

tilsvarte en investering på 55 mil NOK. Verdien av denne investeringen hadde i 2016 steget til 121 mil NOK.

2.2. Menneskerettighetssituasjonen i Saudi-Arabia

Saudi-Arabia er et absolutt enevelde som ikke respekterer de etablerte internasjonale rettsstatsprinsipper. Lovverk og rettssystem er ikke i overensstemmelse med menneskerettighetene.

Saudi-Arabia krenker menneskerettighetene på en rekke områder. Menneskerettighetsorganisasjoner som Amnesty International og Human Rights Watch, foruten FN-organer, har i en årrekke rapportert om omfattende og tildels systematiske brudd. Det omfatter alt fra ytringsfrihet, forsamlingsfrihet og trosfrihet; til kravet om rettsstatsprinsipper som rettferdig rettergang; forbudet mot vilkårlige fengslinger og forsvinninger, tortur og annen mishandling, og forbudet mot diskriminering. Myndighetene har lang tradisjon for å arrestere og straffeforfølge mennesker som på fredelig vis gir uttrykk for meninger som anses støtende eller kritiske. Antallet samvittighetsfanger er likevel umulig å fastslå siden myndighetene ikke praktiserer åpenhet i styringen av landet og heller ikke står ansvarlig for noen siden borgerne er nektet politisk medbestemmelse.

Et ministerråd er i sin helhet utnevnt blant medlemmer av kongefamilien som er etterkommere etter Ibn Saud, Saudi-Arabias grunnlegger. Ministerrådet fungerer som en slags regjering, men kongen har som statsoverhode og regjeringssjef kontroll over alle viktige politiske beslutninger.

Saudi-Arabia har ikke et parlament, men kongen utnevner et rådgivende organ, *shura*, med 150 medlemmer, hvorav 30 siden 2015 har vært kvinner. Landet har heller ikke en grunnlov, men baserer seg på islamsk rett, sharia. Så sent som i 1992 ble den saudiske eneveldige styreformen stadfestet i en lov, Basic Law. Kongen har utstedt ny lovgivning på de områder der en moderne stat er avhengig av fastlagte regler, som finanslovgivning og lovgivning som regulerer næringsliv og handelsvirksomhet. Lover utstedes i form av kongelige dekreter.

I dag har kong Salman gitt sin sønn, kronprins Muhammad bin Salman, tilnærmet total kontroll over alle viktige statsfunksjoner; alle sikkerhetsapparater, inkludert militæret, og den økonomiske politikken. Av relevans for denne drøftingen er at kronprinsen også leder det statlige investeringsfondet, Public Investment Fund (PIF) som holder i statens 70% aksjemajoritet i STC. Styreleder i STC representerer PIF.

2.2.1. Forfølgelse av menneskerettighetsforkjempere etter den arabiske våren

Saudiske myndigheter håndterte den arabiske våren i 2011 som en eksistensiell trussel mot sitt eget regime. Det ble satt i gang en massiv undertrykkelse: Militære intervensjoner for å slå ned uro i andre land i regionen og omfattende trusler mot egen befolkning, kombinert med kjøp av lojalitet gjennom direkte pengegaver, jobber og andre offentlige ytelser. Likevel fortsatte grupper, særlig den sjiamuslimske minoriteten, å gi uttrykk for protest i 2012. I 2013 satte myndighetene inn en offensiv mot enhver ytring som de anså kritisk, og de startet en systematisk bølge av arrestasjoner mot menneskerettighetsforkjempere. Denne offensiven har fortsatt til dags dato. I tillegg har det nye saudiske lederskapet med kong Salman i spissen fra 2015 og kronprins Muhammad bin Salman fra 2017, økt bruken av dødsstraff, bl.a. mot de som tok til gatene i 2011-2012.

2.2.2. Loven mot nettkriminalitet og loven om terrorbekjempelse som redskap til forfølgelse

Saudiske myndigheter bruker særlig to lover som redskaper til å kneble kritikere og menneskerettighetsforkjempere.

Loven mot nettkriminalitet ble innført i 2007. Loven kriminaliserer ærekrenkelser på internett. I artikkel 6, 1. ledd heter det at enhver person som forbryter seg mot lovens bestemmelser skal straffes i inntil fem år og inntil tre millioner riyaler, eller begge deler dersom de gjør seg skyldig i «produksjon, forberedelse, overføring eller lagring av materiale som påvirker offentlig orden, religiøse verdier, offentlig moral og privatliv, gjennom informasjonsnettverk eller datamaskiner». Denne lovbestemmelsen gir ingen klar definisjon av grensen for tillatte ytringer eller andre aktiviteter på nettet, men gir myndighetene mulighet til å slå ned på enhver nettbruker som de mener bryter offentlig moral eller verdier. En rekke bloggere og andre skribenter har blitt dømt til lange fengselsstraffer og pisking for å ha gitt uttrykk for meninger som skal ha vært i strid med denne loven.

En ny terrorlov, «straffelov mot terrorkriminalitet og dens finansiering», ble innført 1. februar 2014. Den gir myndighetene utvidede fullmakter til å straffeforfølge saudiske borgere for kritisk virksomhet siden loven ikke klart definerer og avgrenser hva terrorvirksomhet er. Ifølge loven er terrorisme «enhver handling[...]som har til hensikt å forstyrre offentlig orden[...]eller fornærme statens anseelse eller posisjon.» En rekke saudiske menneskerettighetsforkjempere har siden blitt dømt til fengselsstraffer på 10-15 år for å «fornærme staten» gjennom sitt ikke-voldelige forsvar av menneskerettighetene. I tillegg har folk som demonstrerte under den arabiske våren i 2011 og 2012 blitt dømt til lange fengselsstraffer, inkludert dødsstraff under denne terrorlovgivningen. De særlige domstolene som har ansvar for terror-relaterte saker, Specialized Criminal Court, er underlagt Innenriksdepartementet og følger ikke internasjonale prinsipper for rettferdig rettergang[1]. 1. november 2017 trådte en ny terrorlov i kraft. Den utvider de strafferettslige bestemmelsene, og er like problematisk i menneskerettslig forstand som den foregående loven. Den nye loven definerer eksplisitt det «å portrettere kongen eller kronprinsen på en måte som bringer religion eller rettssystem i vanry» til en terrorhandling[2].

2.2.3. Mangel på rettssikkerhet, bruken av tortur og dødsstraff

Over en årrekke er det dokumentert at det foregår vilkårlig arrestasjoner og folk blir holdt i administrativ forvaring i lengre perioder uten å bli stilt for en kompetent domstol. Fanger ble ofte holdt i isolasjon under avhør og nektes tilgang til juridisk bistand. Rettsprosesser respekterer ikke internasjonale prinsipper for rettferdig rettergang. Gjentatte anklager om bruk av tortur under avhør og mishandling av fanger i regi av sikkerhetstjenesten blir ikke gransket. I praksis hersker det total straffefrihet for bruk av tortur og mishandling. 'Tilståelser' som blir fremtvunget gjennom tortur, blir brukt som bevis i retten. Tiltalte mangler ofte tilgang til advokat og oversettelse i retten dersom tiltalte ikke forstår arabisk.

[1] Se bl.a. en juridisk analyse av loven og terrordomstolene ved prof Michael Newton, Vanderbilt Univ School of Law, 2015 http://www.esohr.org/en/wp-content/uploads/2015/11/A-Legal-Assessment-of-the-Saudi-Penal-Law-for-Terrorism-and-its-Financing.pdf

[2] Se bl.a. https://alqst.org/eng/new-saudi-terrorism-law-still-deeply-flawed-wide-open-abuse/

Saudiske myndigheter benytter fremdeles korporlig avstraffelse som pisking i strid med forbudet mot tortur og annen mishandling.

Bruken av dødsstraff har økt. Både i 2015 og 2016 ble over 150 mennesker henrettet, de fleste ved offentlig halshugging. Per 1 november 2017 er 110 mennesker henrettet i Saudi-Arabia. Domstolene idømmer dødsstraff for en rekke forbrytelser, inkludert ikke-voldelige narkotikaforbrytelser som ifølge folkeretten ikke må føre til dødsstraff. Mange tiltalte ble dømt til døden etter urettferdige rettssaker der eneste bevis er 'tilståelser' som er signert under tortur.

2.3. Overvåkning i Saudi-Arabia

Statlig overvåkning er per definisjon ikke en virksomhet som myndighetene ønsker åpenhet om. I demokratiske land sørger offentlig oppnevnte kontroll-instanser for tilsyn med denne typen virksomhet og sikrer at den utføres innenfor lovlige rammer. I autoritære land, og i særdeleshet i et absolutt enevelde som det saudiske, er det verken åpenhet om, eller kontroll over, overvåkningen. Et forsøk på å få innsyn i hvilken type overvåkning som foregår, må derfor ta utgangspunkt i tilgjengelig informasjon om salg av overvåkningsteknologi til landet.

2.3.1. Salg av overvåkningsteknologi til Saudi-Arabia

Gravejournalistikk og lekkasjer fra involverte selskaper har vist at flere vestlige og israelske selskaper har solgt overvåkningsteknologi til saudiske myndigheter. Senest har BBC og den danske avisen Dagbladet Information i juni 2017 avslørt at det danske firmaet **BAE Systems Applied Intelligence A/S**, som er et datterselskap av den britiske våpengiganten BAE Systems, gjennom en årrekke har solgt teknologiske løsninger for masseovervåkning. Salget har vært godkjent av danske eksportmyndigheter til tross for EU-regler som skal hindre at europeisk overvåkningsteknologi bidrar til undertrykkelse i diktaturstater. I 2017 ble en eksporttillatelse til Saudi-Arabia, til en verdi av 70 millioner DKK, godkjent. Tillatelsen omfatter teknologi til «IP-overvåkning og dataanalyse til bruk for nasjonal sikkerhet og etterforskning av alvorlige forbrytelser». Tilsvarende tillatelser er også gitt til eksport til Qatar og Oman[3].

Forskere fra Citizen Lab ved Universty of Toronto har tidligere avslørt at saudiske sjiaer i den østlige provinsen i Saudi-Arabia har blitt overvåket med spionprogramvare gjemt i en nyhets-app. I motsetning til denne formen for målrettet overvåkningsteknologi, etterlater det danske systemet ingen spor på ofrenes datamaskiner og mobiltelefoner. Det danske overvåkningssystemet kan snappe opp data ved hjelp av «prober» som enkelt sagt klipses på kablene som utgjør internettets infrastruktur. Hvis man ikke har tilgang til kilder innenfor i overvåkningsapparatet, vil man ikke kunne fastslå med sikkerhet om overvåkningsutstyret har blitt brukt mot en gitt person.

Wikileaks har offentliggjort dokumenter fra det danske firmaet som viser at systemet kan brukes til å samle overvåkning av både telefoni og alle former for nettkommunikasjon i et system som gjør det lett for myndighetene å få oversikt. Man kan bruke alt fra epostadresser, telefonnumre eller søkeord for å finne frem til mistenkte som deretter kan overvåkes i realtid og kartlegge hvem de kommuniserer med

[3] https://www.information.dk/indland/2017/06/danmark-tillod-salg-teknologi-kan-overvaage-hel-befolkning-verdens-mest-undertrykkende-regimer-saudi-arabien?lst_rel

og når. På denne måten kan myndighetene bl.a. finne ut om vedkommende sender epost til internasjonale menneskerettighetsorganisasjoner som Amnesty International.

Wikileaks avslørte at det danske selskapet reklamerte med at produktene deres gjorde det mulig å «følge et måls bevegelser ved å spore hans/hennes mobiltelefon-aktivitet» og at deres verktøy kan samle opp og visualisere alle opplysninger om en mistenkts sosiale nettverk. En tidligere ansatt i selskapet har bekreftet overfor BBC/Information at disse opplysningene er dekkende for selskapets teknologi.

Lekkasje fra selskaper som selger overvåkningsteknologi avslører at vestlige selskaper har solgt spionprogramvare (intrusion software) til regjeringer i Gulfen som kan brukes til å krenke borgers rett til privatliv. Citizen Lab har funnet bevis på at spion-programvare fra det italienske selskapet **Hacking Team** har blitt brukt av myndighetene i Saudi-Arabia, Oman og De forente arabiske emirater, mens Emiratene, Bahrain, Oman, Qatar og Saudi-Arabia kan ha kjøpt annen type spionprogramvare fra **FinFisher/Gamma International**[4]. Hackere fikk tilgang til de to selskapenes interne epost-kommunikasjon og dokumenter, og gjorde dem tilgjengelig på nettet i 2014 og 2015. De avslørte dokumentene bygget opp under mange av funnene til Citizen Lab[5]. De to selskapene markedsfører seg med at de bare selger sin teknologi til regjeringer. Teknologien gjør det mulig for myndighetene å hacke seg inn på PCer og mobiler og installere spionprogramvaren som gir dem tilgang til eposter, tekstmeldinger, anropslogg, kontaktlister, filer og potensielt også passord. Programvaren gjør det også mulig å skru på PCens kamera og mikrofon for å ta bilder, video eller lyd uten eierens viten.

Citizen Lab illustrerte sine funn med et eksempel der den prominente menneskerettighetsforkjemperen Ahmed Mansoor fra De forente arabiske emiratene mottok mistenkelige tekstmeldinger på sin mobil som ga inntrykk av at han ville få informasjon om tortur i emiratiske fengsler dersom han klikket på en lenke som det viste seg ville ha installert spionprogramvare på hans iPhone og gitt en ekstern operatør mulighet til å kontrollere hans telefon og kamera, og overvåke hans chatte-applikasjoner og spore bevegelsene hans. Flere saudiske aktivister har fortalt om hacking av sine PCer og at deres kamera har skrudd seg på av seg selv og andre tegn på ekstern kontroll over deres kommunikasjons-enheter[6]. Citizen Lab har ikke kunnet bekrefte at saudiske myndigheter har tatt i bruk Hacking Teams spionprogramvare, men de har offentliggjort beviser på at servere knyttet til Hacking Team opererer i Saudi-Arabia og derved sannsynliggjort at deres teknologi er i bruk i landet[7].

STC er den største teleoperatøren på det saudiske markedet etterfulgt av **Mobily**. Lekket epost-kommunikasjon mellom en navngitt representant for Mobily, Yasser Alruhaily, Executive Manager of the Network & Information Security Department i Mobily, og en amerikansk forsker innen IT-sikkerhet og tidligere leder av Twitters sikkerhetsteam og grunnlegger av Open Whisper Systems med kallenavnet Moxie Marlinspike[8], viste at selskapet i mai 2013 henvendte seg til IT-spesialisten med forespørsel om

[4] Citizen Lab, «Pay no attention to the server behind the proxy: Mapping FinFisher's Continuing Proliferation», 15.10.2015 https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/ https://citizenlab.ca/2014/06/backdoor-hacking-teams-tradecraft-android-implant/

[5] Human Rights Watch, «140 Characters» https://features.hrw.org/features/HRW_2016_report/140_Characters/index.html#_ftnref4

[6] Bloggeren Raif Badawi, i Haidar, Ensaf: *Raif Badawi. My husband. Our Story*, 2016 og kvinneaktivisten Manal al-Sharif til Ina Tin, mai 2016

[7] HRW, ibid

[8] https://www.popsci.com/moxie-marlinspike-makes-encryption-for-everyone#page-2

et oppdrag. Selskapet var på utkikk etter kompetanse til å utvikle et overvåkningsprogram. Ifølge den lekkede kommunikasjonen var prosjektets kravspesifikasjoner et pålegg fra «regulatoren», som er den statlige Kommisjonen for kommunikasjon og informasjonsteknologi (CITC). Ifølge denne kravspekken måtte programmet både kunne overvåke og blokkere mobil datakommunikasjon. Ordrett skal Yasser Alruhaily ha forklart Moxie Marlinspike følgende:

"Vi forsøker å finne en måte å håndtere alle slike krav fra regulatoren, og det handler ikke bare om Whatsapp, men om Whatsapp, Line, Viber, Twitter osv. Så det vi trenger din hjelp til er følgende:

- Finnes det en teknisk løsning som gjør det mulig å overvåke denne trafikken?
- Finnes det et selskap eller en selger som kan hjelpe oss med det?
- Finnes det en teleoperatør som har installert en slik løsning eller funnet en måte å håndtere det på?"

"I et av dokumentene jeg mottok uttrykte de et spesifikt ønske om å forplikte en leverandør av SSL-sertifikater under jurisdiksjonen til De forente arabiske emirater eller Saudi-Arabia til å lage et SSL-sertifikat som kunne brukes til å fange opp informasjon. I tillegg var en stor del av dokumentet viet til en drøfting av eventuelt kjøp av [informasjon om] sårbarheter i SSL-sertifikater eller andre bragder."[9]

Den amerikanske IT-spesialisten tok ikke oppdraget, men offentliggjorde kommunikasjonen med Mobily i 2013. Bloggen førte til stor diskusjon i sosiale medier og Mobily hevdet at opplysningene var falske. De hevdet at de aldri samarbeidet med hackere og at deres oppgave ikke var å spionere på kundene sine.[10] Med det forbeholdet at hele kommunikasjonen kan være et falsum, gir denne epostutvekslingen en indikasjon på at «regulatoren», dvs den statlige saudiske Kommisjonen for kommunikasjon og informasjonsteknologi (CITC) gir teleoperatørene på det saudiske markedet pålegg om å utvikle og drifte systemer for overvåkning av kommunikasjonen til selskapets kunder. Det vil i så fall også omfatte den største operatøren, nemlig STC.

Saudiske embetsmenn knyttet til kronprins Muhammed bin Salman skal så sent som sommeren 2017 ha kjøpt inn spionprogramvare til online overvåkning, ifølge The Wall Street Journal.[11]

2.3.2. Dommer mot menneskerettighetsforkjempere som er basert på informasjon fra overvåkning

Saudiske borgere har blitt arrestert, tiltalt og dømt på grunnlag av informasjon fra overvåkning. En av dem er Abdulaziz al-Shubaily, en av grunnleggerne av den viktigste saudiske menneskerettighetsorganisasjonen Saudi Civil and Political Rights Assosiation, ACPRA. Han ble tatt inn til avhør i november 2013 og konfrontert med telefonsamtaler der han skulle ha diskutert en demonstrasjon. I mai 2016 ble han tiltalt og dømt for terrorvirksomhet. En av tiltalepunktene var at han

[9] https://moxie.org/blog/saudi-surveillance/
[10] http://www.reuters.com/article/saudi-telecoms-spying/saudis-mobily-denies-asking-for-help-to-spy-on-customers-idUSL6N0DW33M20130515
[11] The Wall Street Journal, 02.07.2017 https://www.wsj.com/articles/saudi-arabia-moves-to-silence-deposed-prince-dissidents-1499034642 sitert i HRW Arab Gulf States: Assault on Online Activists, 12.07.2017 https://www.hrw.org/news/2017/07/12/arab-gulf-states-assault-online-activists

hadde gjort seg skyldig i kommunikasjon med Amnesty International og å ha gitt feilaktig informasjon til to uspesifiserte rapporter[12]. Et annet eksempel er slektninger til fire dødsdømte brødre som fikk en advarende telefon fra Innenriksdepartementet få timer etter at de hadde kontaktet Amnesty International fordi de fryktet henrettelsene var nært forestående. De fire brødrene ble henrettet noen dager senere[13].

2.3.3. Overvåkningsregimet til saudiske myndigheter

I Saudi-Arabia er det ingen åpenhet rundt politiske beslutningsprosesser eller statlig forvaltning. Ministerrådet, departementene og andre offentlige organer står til ansvar for kongen, ingen andre. Dette setter klare begrensninger for muligheten til å få klarhet i ansvarsfordeling og kommandolinjer i overvåkningsvirksomhet knyttet til den offentlige forvaltningen.

Det følgende gir en oversikt over instanser som er involvert i håndhevelsen av lov og orden generelt og digital sikkerhet spesielt.

Håndhevelsen av lov og orden er underlagt kongen direkte i tillegg til Forsvarsdepartementet, Innenriksdepartementet og Departementet for nasjonalgarden. Departementene med ansvar for informasjon (Departementet for informasjons og kommunikasjonsteknologi og Departementet for kultur og informasjon) har et spesifikt ansvar for å overse sektoren for telekommunikasjon.

2.3.3.1. Innenriksdepartementet

Innenriksdepartementet har kontroll over intern sikkerhet, inkludert sikkerhetsstyrker og politistyrker. Politiet og sikkerhetsstyrkene har myndighet til å arrestere og fengsle individer. Det er sikkerhetstjenesten, *mabahith*, som gjennomfører arrestasjoner og avhør av saudiere mistenkt for kritisk virksomhet. Det er *mabahiths* etterforskningsorgan, General Investigations Directorate, som oftest anklages for å utføre tortur for å presse frem informasjon og tilståelser under avhør.

Innenriksdepartementet har i alle år blitt oppfattet som en stat i staten som ustraffet har kunnet forfølge enhver saudisk borger med avvikende ytringer og presse frem tilståelser ved hjelp av tortur. Et ukjent antall ansatte i Innenriksdepartementet arbeider med intern sikkerhet. En indikasjon på omfanget fremkommer ved at det ble opprettet 60.000 nye stillinger i Innenriksdepartementet knyttet til sikkerhet som en av kongens grep under den arabiske våren i 2011 for å hindre protester og uroligheter. Fra 2014 fikk Innenriksdepartementet utvidede fullmakter til å straffeforfølge kritisk

[12] https://www.amnesty.org/en/latest/news/2016/05/saudi-arabia-counter-terror-court-sentences-activist-for-exposing-systematic-human-rights-violations/

[13] https://www.amnesty.org/en/latest/news/2014/08/saudi-arabia-four-family-members-executed-hashish-possession-amid-disturbing-surge-executions/

virksomhet gjennom den nevnte terrorloven som trådte i kraft. De særlige domstolene som har ansvar for terror-relaterte saker, Specialized Criminal Court, er underlagt Innenriksdepartementet.

Ifølge en rapport fra Freedom House i 2015 var brukerne av sosiale medier stadig mer forsiktig med hva de postet, delte eller "likte" på nettet, spesielt etter at terrorloven ble innført i 2014.

2.3.3.2. Departementet for informasjons og kommunikasjonsteknologi og Departementet for kultur og informasjon

Departementet for kultur og informasjon må godkjenne alle nettsider som er registrert og driftet i landet. Kommisjonen for audiovisuelle medier har ansvar for å regulere alt lyd- og video-innhold i landet, inkludert satelittkanaler, film, musikk, internett og mobile applikasjoner.

Presse- og publikasjonsloven kriminaliserer publisering eller nedlasting av støtende nettsteder, og myndighetene blokkerer rutinemessig nettsteder som inneholder materiale som oppfattes som skadelig, ulovlig, støtende eller anti-islamsk.

Loven mot nettkriminalitet kriminaliserer ærekrenkelser på internett. Sikkerhetsmyndighetene overvåker aktivt internettaktivitet, både for å håndheve lover, forskrifter og samfunnsnormer, og for å overvåke rekruttering til såkalte terrororganisasjoner.[14] I denne sammenhengen er det viktig å nevne at en menneskerettighetsorganisasjon som Amnesty International blir betraktet som en terrororganisasjon i Saudi-Arabia. Lovparagraf 6, 1. ledd har blitt brukt en rekke ganger for å straffeforfølge individer som myndighetene har identifisert gjennom overvåkning og monitorering av nettaktivitet.

Tilgang til internett er lovlig tilgjengelig bare gjennom autoriserte nett-leverandører. Myndighetene forlanger at nett-leverandører overvåker kunder og pålegger nettkafeer å installere skjulte kameraer og ID-registrere kunder. Myndighetene samler informasjon om identiteten til mennesker som på fredelig vis gir uttrykk for politiske, religiøse eller ideologiske meninger på nettet og tiltaler de som bruker internett for å uttrykke kritikk av tjenestemenn eller religiøse myndigheter med terrorisme, blasfemi og frafall.[15]

2.3.3.3. CITC

Den statlige Kommisjonen for kommunikasjon og informasjonsteknologi (CITC) er opprettet av ministerrådet som i den daglige driften opererer selvstendig, men som tar imot ordrer fra flere departementer. Kommisjonen har et styre som består av ni ministre og regjeringsoppnevnte medlemmer. Minister for kommunikasjon og informasjonsteknologi er styreleder. CITC er ansvarlig for å utstede lisenser til selskaper som vil tilby IT- og telekommunikasjonstjenester i landet. Kommisjonen har også ansvar for å administrere tariffer, føre kvalitetskontroll og filtrere innhold og blokkere tilgang til

[14] US Dep of State: Report on Human Rights Practices for 2016 Saudi-Arabia: https://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/#wrapper
[15] Ibid

nettsider som kommisjonen anser som støtende. Nettsider som tar til orde for politiske, sosiale eller økonomiske reformer eller menneskerettigheter er blant de nettsidene som anses som støtende.

CITC gjennomfører filtreringen og sensuren gjennom å hoste brannmurer som blokkerer tilgangen til nettsider som anses problematiske ifølge det strenge sensur-regimet.[16] Spørsmålet er om CITC setter ut hele eller deler av denne overvåkningsvirksomheten til tele og nett-leverandørene og ber dem overvåke kundene sine.

Alle aktører på telekommunikasjonsmarkedet er regulert av CITC og underlagt Innenriksdepartementet i politiske saker.

Loven om telekommunikasjon krever at nettleverandører blokkerer forbudte nettsider. Pornosider er forbudt, men det er som nevnt også nettsider som tar til orde for reformer eller menneskerettigheter, i tillegg til lokale og internasjonale rettighetsorganisasjoner og sidene til eksil-saudiere.[17]

I oktober 2016 annonserte CITC at kommisjonen hadde blokkert 2.6 millioner «pornografiske» nettsider i 2015 og 3.5 millioner i perioden 2010-2015. Bortsett fra beslutninger om blokkering av phishing-sider (sider som forsøker å stjele personlig eller finansiell informasjon), gir myndighetene ansvaret for beslutning om blokkering av nettsider til en interdepartemental komite som ledes av Innenriksdepartementet. Ifølge telekommunikasjonsloven kan nettleverandører som unnlater å blokkere forbudte nettsider, ilegges bøter på 4-5 millioner riyaler.

CITC hevdet i 2016 at Facebook fjernet materiale som CITC anså støtende, men at Twitter ignorerte alle CITC-forespørsler. Facebook, Messenger og Whatsapp var delvis tilgjengelige: Tekstmeldingsfunksjoner var tilgjengelig, mens tale- og videofunksjoner var blokkert. Brukere av Snapchat, FaceTime og andre video-apps rapporterte i 2016 at slike tjenester ble blokkert. I 2013 annonserte CITC at tale-appen Viber ble blokkert, og at den ville "ta passende tiltak" mot apper eller tjenester, inkludert Skype og WhatsApp, hvis leverandørene ikke tillot myndighetene "lovlig tilgang" for overvåkingsformål.[18]

CITC oppfordrer publikum til å sende inn forespørsler om å blokkere eller fjerne blokkering av bestemte nettsteder og skjemaer ligger lett tilgjengelig på statlige nettsider.[19] I 2010 oppga CITC at den mottok mer enn 300.000 forespørsler om å blokkere nettsteder årlig. I tillegg etablerte Innenriksdepartementet i 2016 en app der allmenheten lett kan anmelde sine medborgere for sikkerhetsrelaterte lovbrudd. Appen heter «Kulna amn», «Vi er alle sikkerhet», med betydningen «vi har alle et ansvar for sikkerhet». Mao har myndighetene gitt befolkningen digital tilgang til å drive angiveri. Appen var inspirert av en tilsvarende app utviklet i 2012 av Transportdepartementet for anmeldelse av trafikkforseelser.

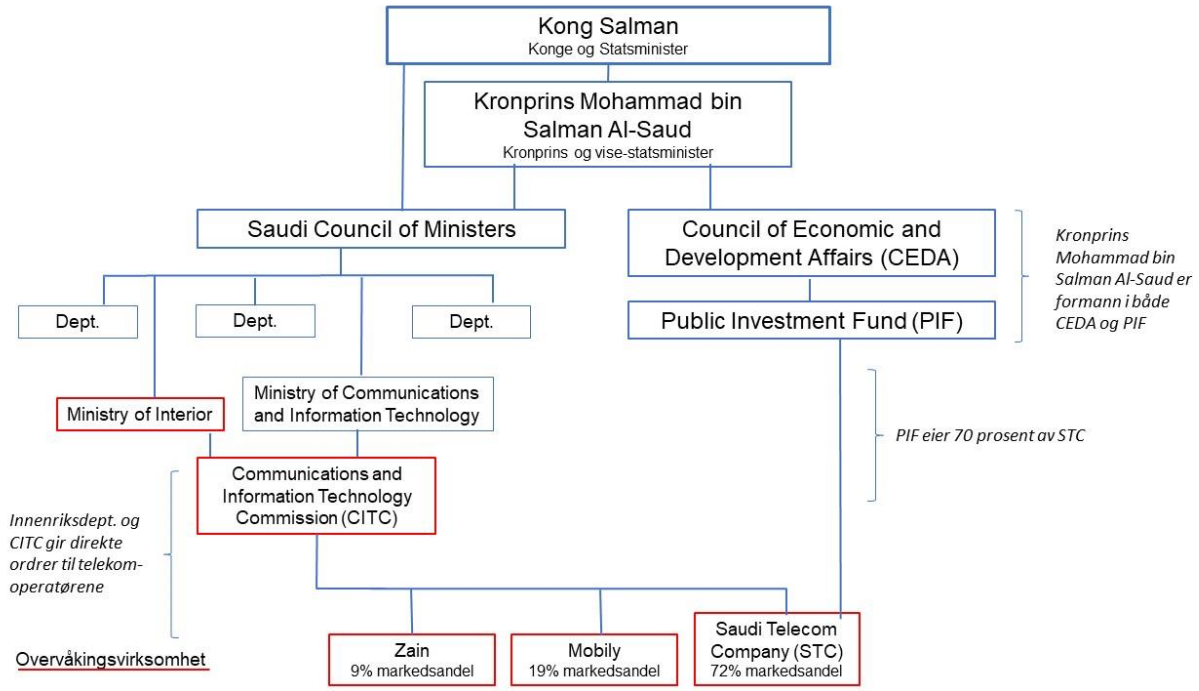
Regjeringen kan kontrollere telekommunikasjonsmarkedet gjennom CITC som tar imot ordrer fra Innenriksdepartementet om hva som skal sensureres og overvåkes, oppsummerer Steffen Hertog, professor i sammenliknende politikk ved London School of Economics (LSE).[20] Alle telekomm-

[16] Shearman & Sterling LLP: Telecoms in the Kingdom of Saudi Arabia – An Overview, Sept 2016 http://www.shearman.com/~/media/Files/NewsInsights/Publications/2016/09/Saudi-Arabia-Publications/Telecoms-in-the-Kingdom-of-Saudi-Arabia--An-Overview.pdf
[17] US Dep of State: Report on Human Rights Practices for 2016 Saudi-Arabia: https://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/#wrapper
[18] Ibid
[19] https://www.saudi.gov.sa/wps/portal/snp/individuals
[20] Epost-kommunikasjon med undertegnede, nov 2016.

leverandører er underlagt CITCs kontroll og som nevnt kan de ilegges bøter hvis de unnlater å drive overvåkning for å kunne blokkere forbudte nettsider.

2.3.4. Grafisk fremstilling av aktørene i overvåkningsvirksomheten

Dette er en enkel og ufullstendig fremstilling av forbindelsene mellom øverste ledelse av kongehuset og STC, og en oversikt over de organene som spiller en rolle i overvåkningsvirksomheten. Vi utelukker ikke at det finnes flere organer som er involvert i denne virksomheten.



2.4. Saudi Telecom Company

2.4.1. Nøkkelinformasjon om STC

Saudi Telecom Company (STC) Group er det største telekommunikasjonsselskapet i Midtøsten. Selskapets kjernevirksomhet er i Saudi-Arabia, i tillegg har STC 19 datterselskaper som opererer i Midtøsten og Sørøst-Asia.[21] STC leverer mobil og fasttelefon-tjenester, internett-abonnementer og ulike nettrelaterte tjenester som undersjøiske kabelnettverk.

[21] https://english.mubasher.info/markets/TDWL/stocks/7010/profile

Selskapets omsetning var i 2015 50.65 mia SAR (116.5 mia NOK, kurs: 2,30) med et overskudd på 9.25 mia SAR (21.3 mia NOK), mens tilsvarende tall i 2016 var hhv 51.83 mia SAR (119 mia NOK) og 8.53 mia SAR (19.6 mia NOK).[22]

Selskapet ble etablert ved kongelig saudisk dekret i 1998 som et 100% statseid selskap med hovedkvarter i Riyadh. I 2002 valgte myndighetene å selge 30% av selskapets aksjeportefølje. Selskapet gikk på den saudiske børsen Tadawul i januar 2013. Staten kontrollerer fortsatt 70% av aksjene gjennom Public Investment Fund (PIF). Som nevnt er PIF et statlig fond som ledes direkte av kronprins Muhammad bin Salman. Styreformann i STC, Abdullah bin Hassan Al Abdulkader, representerer PIF. Andre store aksjeeiere er General Organization for Social Insurance - Saudi Arabia med 7% eierandel og Public Pension Agency med 6.77%. Oljefondets eierandel tilsvarer 0.04% av selskapet.

2.4.2. STCs posisjon på telekommunikasjonsmarkedet i Saudi-Arabia

Mobiltelefoni: STC er den klart største mobiloperatøren i Saudi-Arabia med en *estimert* markedsandel på 72%.[23] Mobil-sektoren er den viktigste komponenten i Saudi-Arabias telekom-industri og bidrar med 75% av sektorens inntekter. Saudi-Arabia har en befolkning på 32 millioner (hvorav ca 10 millioner migrantarbeidere) som totalt i 2016 innehadde 48 millioner mobilabonnementer, dvs en mobilutbredelse på 153%. Den høyeste mobilutbredelsen var i 2011 (under den arabiske våren) med totalt 53,7 millioner abonnementer, dvs 181%. Nedgangen antas bl.a. å være knyttet til at Innenriksdepartementet i starten av 2016 innførte en lov om biometrisk fingeravtrykk som innebærer at kunder som kjøper SIM-kort må avgi fingeravtrykk som lagres i et nasjonalt informasjonssenter. Loven førte til en markert nedgang i antallet mobil-abonnenter i 2016, inkludert bredbånd-abonnementer.[24] Ni av ti saudiere eier en smarttelefon, ifølge en Google-studie.

Internett-tjenester: STC er også markedsledende som nett-leverandør på det saudiske markedet (ADSL fra 2001, FttP -fibre-to-the-premises fra 2010). Anslag over unike internett-brukere i Saudi-Arabia varierer, men The International Telecommunication Union estimerer at det i 2016 var 23.2. millioner nett-abonnenter i landet, som tilsvarer 70% av befolkningen.

Mobily er den neststørste telekom-leverandøren på det saudiske markedet med en estimert andel av mobilmarkedet på 19%, tilsvarende 10 millioner abonnenter. **Zain** er nummer tre på dette markedet med en andel på 9%.

[22] Buddecomm Report: Saudi Arabia Telecoms - Mobile and Broadband – Statistics and Analyses, 2017 https://www.budde.com.au/Research/Saudi-Arabia-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses

[23] Selskapet oppgir ikke egne tall på markedsandel. Buddecomm Report: Saudi Arabia Telecoms - Mobile and Broadband – Statistics and Analyses, 2017 https://www.budde.com.au/Research/Saudi-Arabia-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses

[24] Ibid

3. Drøfting

Problemstillingen er om NBIM kan sannsynliggjøre at investeringen til oljefondet i STC ikke er i strid med oljefondets etiske retningslinjer og forventningsdokument om menneskerettigheter.

Investeringen i STC har gjort oljefondet til medeier i det største telekom-selskapet i Saudi-Arabia som er kontrollert av den saudiske staten. Amnesty International mener med dette notatet å sannsynliggjøre, så langt det er mulig når det handler om et absolutt enevelde, at STC er involvert i overvåkningsvirksomhet i landet: Selskapet er pålagt å drive overvåkning av nettet og det er sannsynlighet for at det også er involvert i målrettet overvåkning av sine kunders mobilbruk. Uansett står selskapets majoritetseier ansvarlig for overvåkning av mobil- og nettbruk i Saudi-Arabia som fører til straffeforfølgelse, inkludert bruk av dødsstraff, mot saudiske menneskerettighetsforkjempere.

3.1. Lovlig og ulovlig overvåkning

Det foregår overvåkning av nettet i en rekke land i den hensikt å stanse ulovlig virksomhet, f.eks. for å straffeforfølge bakmenn som misbruker barn i pornoindustrien. Overvåkning er først ulovlig hvis den er i strid med internasjonal rett og menneskerettighetene.

En diskusjon av den saudiske overvåkningen må derfor ta utgangspunkt i at saudisk lovgivning gjør det straffbart å opprette og drive nettsider eller kommunisere gjennom mobile og digitale plattformer om bl.a. menneskerettighetsspørsmål, utveksle meninger om religion eller politikk, eller gi uttrykk for regimekritikk. Den saudiske lovgivningen representerer derfor i seg selv et brudd på ytringsfriheten, religionsfriheten og privatlivets fred. Overvåkning som et redskap for å håndheve en lovgivning som krenker menneskerettighetene, er derfor ulovlig og vil gjøre overvåkeren selv ansvarlig for krenkelsen i kraft av å være den som utøver krenkelsen.

Det er ytterligere skjerpende momenter at det saudiske rettssystemet ikke yter den tiltalte rettferdighet, og at myndighetene tillater at tortur benyttes for å presse frem «tilståelser» som brukes som bevis i retten. I tillegg risikerer den tiltalte å bli dømt til døden etter rettsprosesser som ikke respekterer internasjonale prinsipper for rettferdig rettergang. Både loven mot nettkriminalitet og terrorloven har beviselig gjentatte ganger blitt brukt til å kneble kritikere og dømme menneskerettighetsforkjempere til lange fengselsstraffer som terrorister.

3.2. STC som et redskap i overvåkningen

Som den største mobil- og nettleverandøren i Saudi-Arabia er STC underlagt statlig kontroll og er pålagt å forholde seg til det overvåkningsregimet som saudiske myndigheter har etablert gjennom lovgivning og opprettelsen av CITC som regulator av telekom-markedet. STC risikerer bøter for å unnlate å følge CITCs pålegg om overvåkning, filtrering og blokkering av nettsider som anses problematiske. STC må derfor anses som en aktør som utøver/fasiliterer overvåking og sensur av nettet.

Overvåkningen av nettet har ført til etterforskning, arrest, tiltaler og dommer mot en rekke menneskerettighetsforkjempere, bloggere og skribenter fra 2011 til i dag. De 11 grunnleggerne av den viktigste saudiske menneskerettighetsorganisasjonen, Saudi Civil and Political Rights Assosiation, ACPRA,

og en av deres advokater og støttespillere, Waleed Abu al-Khair, er bare noen få slike eksempler. Bloggerne Hamza Kashgari og Raif Badawi er to andre, så vel som journalisten Alaa Brinji og poeten Ashraf Fayadh.

Når det gjelder mobil-overvåkning, er det problematisk direkte å fastslå hvilke instanser som faktisk utøver virksomheten: STC som teleoperatør, CITC som regulator av telekommarkedet og/eller i regi av Innenriksdepartementet som CITCs overordnede i sikkerhetsspørsmål. Det som kan fastslås er at myndighetene i Saudi-Arabia i en årrekke har kjøpt inn avansert teknologi både til å drive massovervåkning i den hensikt å overvåke særlige personer, grupper eller miljøer, eller finne frem til mennesker som kommuniserer om bestemte temaer og overvåke dem i realtid. Myndighetene har også kjøpt inn spionprogramvare som kan brukes til hacking av utpekte individers digitale enheter for å installere overvåkning på deres mobiltelefoner og PCer.

Det som kan fastslås gjennom disse avsløringene, er at saudiske myndigheter har tatt i bruk alle tenkelige redskaper for å identifisere individer som de anser gjør seg skyldig i undergravende virksomhet. Det som ikke kan fastslås, er hvor i systemet selve mobil-overvåkningen foregår. Henvendelsen fra STCs konkurrent på mobilmarkedet, Mobily, til en amerikansk IT-spesialist, er likevel en indikasjon på at mobil-leverandørene selv er pålagt å utføre overvåkningen av kundenes mobiltrafikk. Med det forbehold at den lekkede kommunikasjonen kan være et falsum, er det derfor sannsynlighet for at STC på samme måten som Mobily er pålagt å finne frem til metoder for å tilfredsstille CITCs krav om overvåkning og rapportering.

3.3. Delansvaret til oljefondet som aksjeeier i STC

Oljefondet ble deleier i STC i 2015. Denne drøftingen har vist at oljefondet gjennom aksjekjøpet i Saudi-Arabias største telekom-selskap, STC, for to år siden har fått et medansvar for utøvelsen av den nett-overvåkningen som saudiske myndigheter pålegger nett-leverandører på det saudiske markedet å utføre. Overvåkning av nettet har beviselig ført til straffeforfølgelse av menneskerettighetsforkjempere i Saudi-Arabia. Denne overvåkningen gjør derfor oljefondet delaktig i en virksomhet som er i strid med en rekke menneskerettigheter. I tillegg er det sannsynliggjort at STC også driver overvåkning av sine mobilkunder i strid med menneskerettighetene. Det er hevet over tvil at det foregår statlig overvåkning av mobiltrafikk i Saudi-Arabia, så enten utføres den av den største eieren til STC, staten, eller av selskapet selv.

3.4. Praktiseringen av oljefondets etiske retningslinjer

Oljefondet er pålagt å foreta investeringer som gir maksimal avkastning på sikt for å sikre pensjonene til fremtidige generasjoner i Norge. Fondets investeringsvirksomhet skal likevel foregå i overensstemmelse med etiske retningslinjer vedtatt av Stortinget.

Fondet velger å investere i nye markeder og fremvoksende økonomier for å spre risiko mest mulig. Samtidig er det ofte slike markeder som representerer til dels store etiske risikoer. Når NBIM velger å gå inn i nye markeder, foretas det i henhold til fondets retningslinjer for investeringsunivers, «en helhetsvurdering av konfliktsituasjon, politisk terror, beskyttelse av eierskapsrettigheter og korrupsjon»,

og det skal foretas i henhold til de etiske retningslinjene.Det er vanskelig å forstå at en slik "helhetsvurdering" har tatt hensyn til de etiske risikoer som er forbundet med å gå inn på det saudiske markedet, og i særdeleshet i statlig kontrollerte saudiske selskaper. Fondet må ha valgt å se bort fra risiko forbundet med mangel på åpenhet og transparens, ulovlig overvåkning, et rettssystem som bryter menneskerettighetene og andre omfattende krenkelser av menneskerettighetene som den saudiske staten står ansvarlig for. Vi ser derfor frem til å høre fondets redegjørelse for den vurderingen som er gjort av det saudiske markedet og de etiske risikoene som er forbundet med investeringer på dette markedet generelt, og investeringen i STC spesielt

Som ledd i NBIMs risikohåndtering, formulerer fondet forventninger til selskaper som fondet vurderer å investere i: «Som finansiell investor forventer NBIM at selskaper respekterer menneskerettighetene og tar hensyn til menneskerettigheter i sin virksomhet. Våre forventninger retter seg først og fremst mot selskapenes styrer og er et utgangspunkt for vår dialog med selskapene om menneskerettigheter."[25] Vi kan ikke se at fondets investering i STC kan være i samsvar med fondets nevnte forventninger eller de etiske retningslinjene.

I tilfellet STC vil en eventuell aktiv eierskapsdialog i så fall føres med styret i STC som ledes av en representant for det statlige investeringsfondet, PIF, som er kontrollert direkte av kronprins Mohammed bin Salman. I en evt dialog med styret i STC må NBIM derfor forvente å møte en styreleder som representerer det saudiske kongehuset. Vi ser derfor også frem til NBIMs vurdering av mulighetene som ligger i å påvirke STC til respekt for menneskerettighetene gjennom å benytte en aktiv eierskapsdialog.

3.5. NBIMs argumentasjon

Ifølge kommunikasjonssjef i NBIM, Thomas Sevang, er alle fondets investeringer i Saudi-Arabia gjort av eksterne forvaltere i Dubai og Riyadh. «Disse forvalterne investerer i aksjer etter en grundig fundamental analyse av selskapene. Hensyn til selskapenes miljø, sosiale faktorer og eierstyring (ESG) er for alle forvaltere en integrert del av denne fundamentale analysen»[26]. Sevang har ikke villet svare på spørsmål om menneskerettighetsdimensjonen var inkludert i NBIMs risikoanalyse i forbindelse med investeringene i Saudi-Arabia og har følgelig heller ikke svart på om NBIM ikke anså at det var en risiko for at fondet gjennom sine investeringer kunne få et delansvar for brudd på menneskerettighetene. Han har avvist å kommentere fondets vurdering og analyser for enkeltinvesteringer eller enkeltmarkeder eller gå i detalj om definisjoner: «I henhold til våre retningslinjer avstår vi fra å kommentere enkeltselskaper og problemstillinger som kan settes i en utenrikspolitisk sammenheng»[27]Med dette notatet ønsker Amnesty International derfor å løfte dialogen om investeringen i STC opp til fagavdelingen i NBIM. Vi ser frem til en drøfting av vurderingene knyttet til denne konkrete investeringen. Vi mener en slik drøfting har prinsipiell verdi og kan bidra til å øke forståelsen av hvordan de etiske retningslinjenes menneskerettslige dimensjon kan praktiseres i NBIMs investeringsvirksomhet.

[25] www.nbim.no
[26] Epost fra Thomas Sevang til Ina Tin, 14.10.2016