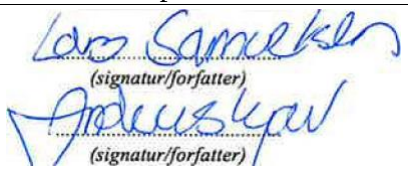
Universitetet
i Stavanger
DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i samfunnssikkerhet	Vårsemesteret, 2021 Åpen
Forfattere: Lars Samuelsen Andreas Kjær	 (signatur/forfatter) (signatur/forfatter)
Fagansvarlig: Odd Einar Falnes Olsen **Veileder:** Odd Einar Falnes Olsen	
Tittel på masteroppgaven: Digitalisering og sårbarhet i kommunal sektor **Engelsk tittel:** Digitalization and vulnerability in the municipal sector	
Studiepoeng: 30	
Emneord: Digitalisering, kommunal sektor, risiko, sårbarhet, risikostyring, informasjonssikkerhet, digitale fellesløsninger, trusselbildet, organisatoriske faktorer og utilsiktede hendelser	Sidetall: 92 + vedlegg/annet: 110 Stavanger, 14.06.2021

Forside for masteroppgaven

Digitalisering og sårbarhet i kommunal sektor

Andreas Kjær
Lars Samuelsen

Master i Samfunnssikkerhet
Universitetet i Stavanger
Det Teknisk-Naturvitenskapelige Fakultetet
Våren 2021

Forord

Med innlevering av denne masteroppgaven avsluttes en spennende og lærerik studietid ved universitetet i Stavanger. Arbeidet med masteroppgaven har vært en omfattende prosess og krevd at to svært skriveglade studenter har måttet holde tungen bent i munnen for å redusere både innhold og sidetall. Resultatet av denne prosessen er at vi sitter igjen med et produkt vi begge kan være stolte av, samtidig som at undersøkelsen har bidratt til økt fordypning og kunnskap innenfor et fagområdet som representerer utfordringer i hele samfunnet.

Vi vil rette en stor takk til studiens informanter som på tross av en allerede hektisk hverdag har stilt opp og vært villig til å dele av sin erfaring og kunnskap. Takk til Digitaliseringsdirektoratet for samtaler og faglige innspill underveis. Tusen takk til vår veileder, Odd Einar Falnes Olsen, for svært gode og oppmuntrende tilbakemeldinger gjennom hele prosessen. Takk for at du har bevart troen på oss. En stor takk til Kamilla Amundsen, venner og familie for korrekturlesing og oppmuntrende ord gjennom hele halvåret.

Sist men ikke minst vil vi takke hverandre for et produktivt og godt samarbeid. Et samarbeid vi ikke ville vært foruten.

Andreas Kjær & Lars Samuelsen, 14.06.2021

Sammendrag

Norske kommuner står ovenfor et omfattende digitaliseringsarbeid som endrer hvordan kommunene kommuniserer med, og tilbyr tjenester til både innbyggere og næringsliv innenfor sitt ansvarsområde. Digitaliseringen skjer som følge av økte krav fra innbyggere om gode og lett tilgjengelige tjenester, samt sektorens egne behov for effektivisering og gevinstrealisering, hvor økt bruk av digitale fellesløsninger fremgår som en viktig satsing for å oppnå dette. Selv om digitaliseringen har positive innvirkninger på mange områder, vil også den økte bruken av IKT i kommunesektoren medføre endringer i risiko- og sårbarhetsbildet.

I denne studien undersøker vi hvordan bruken av digitale fellesløsninger endrer kommunenes arbeid med informasjonssikkerhet. Dette gjøres ved å foreta en dokumentanalyse i kombinasjon med intervjuer av ansatte i kommunene for å få en god dybdeforståelse av utfordringsbildet, samt hvordan kommunene tilpasser seg disse utfordringene i arbeidet med informasjonssikkerhet. Ved å bruke teori om informasjonssikkerhet, regulering, MMD og HRO belyser vi hvorfor bruk av fellesløsninger kan føre til sikkerhetsutfordringer, samt hvordan kommunene arbeider for å ivareta sikkerheten i egne digitale løsninger. Undersøkelsen viser at kommunene står ovenfor en rekke utfordringer, og at bruken av fellesløsninger stiller nye krav til hvordan kommunene arbeider for å ivareta informasjonssikkerheten. Årsakene til disse utfordringene og kravene er sammensatte, hvor funnene våre viser at:

- Digitale avhengigheter og lengre verdikjeder i kombinasjon med manglende digital kompetanse medfører økt konsekvenspotensiale, ettersom feil kan spre seg på nye og uventede måter når systemer er tettere sammenkoblet og avhengighetene øker.
- Flere kommuner opplever utfordringer med det risikobaserte regelverket. Kommunene står også ovenfor utfordringer ved involveringen av ledelsen i informasjonssikkerhetsarbeidet.
- Den desentraliserte organiseringen i kommunene utfordrer mulighetene for å oppnå en god helhetsforståelse av det samlede risiko og sårbarhetsbilde kommunene står ovenfor.
- Målkonflikter, informasjonsvansker og manglende intern kompetanse og ressurser er sentrale utfordringer for risikostyringsarbeidet
- Funnene våre viser at kommunene står ovenfor økte krav til mer proaktiv risikostyring, ivaretakelse av et helhetsbilde av risiko- og sårbarhetsforhold, uformelle

samarbeid, og et tettere samarbeid med eksterne aktører for å ivareta god informasjonssikkerhet.

Ett overraskende funn er at kommunene i mange tilfeller er bevisste på hvilke utfordringer de selv står ovenfor, og at det i mange tilfeller er mangelen på kompetanse og interne ressurser som setter begrensninger for kommunenes sikkerhetsarbeid fremfor kompleksiteten av trussel og sårbarhetsbilde.

Innholdsfortegnelse

Figurer:

Tabeller:

1.0 Innledning

1.1 Bakgrunn

Digitalisering blir ofte brukt som en samlebetegnelse for å beskrive overgangen fra analoge, mekaniske eller papirbaserte løsninger og systemer, til elektroniske og digitale motparter. Digitalisering kan videre beskrives som en omstillingsprosess hvor man introduserer ny teknologi i organisasjoner (Kommunal- og moderniseringsdepartementet, 2014a). Digitaliseringen baner vei for både innovasjon og effektivisering i form av at nye forretningsmodeller og næringsveier kan utvikles, og mindre effektive løsninger kan fases ut. Behovet for en økt digital offentlig sektor ble særlig aktualisert etter lanseringen av stortingsmeldingen *Digital agenda for Norge* der regjeringen presenterte sine ambisiøse mål med den nasjonale IKT-politikken, som fremhevet ulike målsetninger for digitaliseringen av offentlig sektor (Kommunal- og moderniseringsdepartementet, 2016).

På tross av sine mange fordeler medfører digitaliseringsarbeidet en endring i samfunnets risiko og sårbarhetsbilde der uønskede hendelser kan ramme virksomheter og sektorer på nye og uventede måter (NOU 2015: 13, 2015). Flere studier har belyst temaene digitalisering og den økte utnyttelsen av IKT i offentlig sektor. Dawes (2008) undersøkte utviklingen av IKT i offentlig sektor og hvordan implementeringen av IKT har ført til bekymringer for nye trusler relatert til sikkerhet, personvern, stabilitet og forvaltning. Guo (2010) fremhever fordelene, potensialet og risikoene forbundet med at myndighetene bruker innovative former for IKT for å forbedre tilgangen på, og øke kvaliteten på offentlige tjenester og prosesser til fordel for innbyggerne og virksomheter. Singh & Karulia (2011) tar for seg hvilke informasjonssikkerhetsutfordringer offentlig sektor står ovenfor ved økt utnyttelse av IKT og beskriver strategier for å forbedre sikkerheten i digitaliserte offentlige tjenester. Ejdys, Ginevicius, Rozsa og Janoskova (2019) undersøkte i hvilken grad risikooppfatning og opplevd sikkerhet fra et brukerperspektiv påvirket tilliten til myndighetenes IKT-løsninger og bruken av disse. Mark, Tømte, Næss og Røsdal (2019) gjennomførte en studie med formål å frambringe oppdatert kunnskap om utvikling av IKT-sikkerhetskompetanse med tanke på fremtidige behov. I sin komparative analyse undersøker Thompson, Mullins og Chongsutakawewong (2020) hvorvidt en økt andel IKT-løsninger i offentlig sektor gir bedre digital sikkerhet eller ikke.

Ifølge Nasjonal sikkerhetsmyndighet (NSM) vil digitalisering alltid innebære risiko, og selv om stadig flere ser ut til å prioritere IKT-sikkerhetsarbeid utfordres dette arbeidet av et stadig mer komplekst IKT-risikobilde (Nasjonal sikkerhetsmyndighet, 2020). Digitaliseringen i kommunal sektor skaper ifølge Politiets sikkerhetstjeneste (PST) nye avhengigheter og bidrar til at det utvikles sensitiv informasjon innenfor stadig nye samfunnsområder (Politiets sikkerhetstjeneste, 2021). Overgangen til en stadig mer digital offentlig sektor har medført at flere verdier legges inn i det digitale domenet og i nettverkene, noe som stiller kommunene ovenfor økte krav til kapasitet og sikkerhet (Kommunal- og moderniseringsdepartementet, 2021b). Kommunale virksomheter har som følge av den økte digitaliseringen, og de store informasjonsmengdene sektoren forvalter, fått et betydelig større ansvar for å sikre egne informasjonsverdier og personopplysninger. God informasjonssikkerhet blir dermed ansett som en viktig forutsetning for en vellykket digitalisering og for å ivareta tilliten befolkningen har til offentlige IT-systemer og digitale tjenester (Kommunal- og moderniseringsdepartementet, 2021a). Dette forutsetter at kommunale virksomheter arbeider systematisk og målrettet for å styre risiko slik at krav til sikkerhet og personvern blir ivaretatt på en god måte.

1.2 Problemstilling og forskningsspørsmål

Tilnærmingen i denne studien er å undersøke digitaliseringen i kommunal sektor med utgangspunkt i et sikkerhetsfaglig perspektiv. For å gjøre dette har vi valgt å se på et av utviklingstrekkene i digitaliseringen, som i denne undersøkelsen tar for seg både felleskomponenter og digitale fellestjenester. Vi har valgt å bruke *digitale fellesløsninger* som en samlebetegnelse hvor begge disse begrepene inngår. Det har ikke tidligere blitt gjort undersøkelser som spesifikt tar for seg hvordan den økte utnyttelsen og bruken av digitale fellesløsninger påvirker norske kommunenes informasjonssikkerhetsarbeid. På bakgrunn av dette har vi derfor utarbeidet følgende problemstilling:

«Hvordan endrer bruk av digitale fellesløsninger kommunenes arbeid med informasjonssikkerhet i egen virksomhet?»

For å besvare denne problemstillingen har vi valgt å utforme tre forskningsspørsmål (FS) som på hver sin måte skal belyse ulike momenter som er viktige å undersøke for å besvare problemstillingen.

FS1: *Hvordan fører bruk av digitale fellesløsninger til sikkerhetsutfordringer?*

For å forstå hvordan bruken av digitale fellesløsninger endrer kommunenes arbeid med informasjonssikkerhet er forskningsspørsmålet utarbeidet med den hensikt å belyse hvorvidt den økte bruken av digitale fellesløsninger representerer noen særegne organisatoriske- og digitale sikkerhetsutfordringer for kommunene.

FS2: *Hvilke utfordringer opplever kommunene i forbindelse med regelverket og intern organisering på informasjonssikkerhetsområdet?*

Formålet med dette forskningsspørsmålet er å opparbeide oss en forståelse av hvordan lovverket på informasjonssikkerhetsarbeidet kan påvirke og skape utfordring for hvordan kommunene arbeider for å ivareta informasjonssikkerheten i egen virksomhet. Vi ønsker også å belyse hvordan den interne organiseringen samt ledelsens rolle i informasjonssikkerhetsarbeidet kan utfordre evnen kommunene har til å ivareta god informasjonssikkerhet i de digitale fellesløsningene. Sistnevnte ses i sammenheng med at kommunene har stor frihet til å velge egen organisering, noe som legger til rette for at kommunene kan ha store variasjoner på den interne organiseringen. Ettersom vi ser på deltakelsen i det interkommunale samarbeidet «Digi Rogaland» som et organiseringsvalg, har forskningsspørsmålet videre til hensikt å undersøke hvordan deltakelsen i samarbeidet kan påvirke informasjonssikkerhetsarbeidet i de enkelte kommunene.

FS3: *På hvilken måte utfordrer bruken av digitale fellesløsninger risikostyringsarbeidet i kommunene?*

Det siste forskningsspørsmålets hensikt er å undersøke hvorvidt den økte bruken av digitale fellesløsninger kan utfordre måten kommunale virksomheter tradisjonelt har drevet sine risikostyrende aktiviteter. Vi tenker her at det vil være naturlig at eventuelle endringer i risiko- og sårbarhetsbilde som følge av felles løsningene vil kunne påvirke kommunenes risikostyringsarbeid. Forskningsspørsmålet er basert på en antakelse om at den økte bruken av digitale løsninger kan medføre fragmenterte ansvarsforhold mellom kommunene og leverandørene av løsningene.

1.3 Avgrensning

I denne undersøkelsen har vi valgt å undersøke hvordan bruk av digitale fellesløsninger kan utfordre og endre kommunenes arbeid med informasjonssikkerhet med særlig fokus på kommunenes helsesektor. Begrepet digitale fellesløsninger blir brukt på en lite konsekvent måte av forskjellige aktører, og man finner ulike varianter av begrepet som delvis overlapper. I denne undersøkelsen bruker vi begrepet digitale fellesløsninger som en samlebetegnelse for ferdigutviklede digitale tjenester (fellestjenester/løsninger) som eksempelvis digi helse og digisos, samt det som noen steder blir omtalt som nasjonale felleskomponenter. Sistnevnte er gjenbrukbare komponenter for eksempelvis innlogging, autentisering eller registre som virksomheter kan bruke for å utvikle egne digitale tjenester som eksempelvis ID-porten. Hovedfokuset i denne undersøkelsen er ikke å undersøke de tekniske aspektene ved løsningene. Vi kommer heller til å undersøke hvordan bruken av disse løsningene kan representere organisatoriske utfordringer med henvisning til risikostyring, ledelse og intern organisering. Videre har vi valgt å avgrense oss slik at vi utelukkende tar for oss utilsiktede hendelser. Vi vil derfor ikke ta for oss hendelser som går inn under cyber-domenet.

1.4 Tidligere Forskning

Cram, Proudfoot og D'Arcy (2017) har gjennomført en studie som oppsummerer den eksisterende kunnskapen innenfor forskning på informasjonssikkerhetspolitikk i organisasjoner. Studien har tatt for seg 114 artikler fra 34 forskjellige journaler som omhandler policyer for informasjonssikkerhet i organisasjoner, og har identifisert fem hovedområder forskningen har fokusert spesielt på. Det første hovedområdet forskningen har vært interessert i er hvilke faktorer som påvirker utviklingen og implementeringen av informasjonssikkerhetspolicyer. Her har forskningen vært rettet mot tre hovedfaktorer. Den første er forskning som ser på hvordan standarder, veiledere og regulering påvirker hvordan retningslinjer for informasjonssikkerhet blir innført i organisasjoner. Den andre faktoren som er blitt indentifisert i forskningen er spørsmål om hvilken struktur og format som benyttes. Her har forskerne vært interessert i hvordan beslutninger om lengde, grad av detaljering og lignende påvirker implementeringen av retningslinjene. Den siste faktoren som er blitt identifisert handler om interne og eksterne karakteristikker som påvirker valg av design på informasjonssikkerhetsretningslinjene, dette kan være type organisasjon, størrelse på organisasjonen, IT-infrastruktur, interne og eksterne trusler og lignende.

Det andre hovedområdet som forskerne har fokusert på er hvordan informasjonssikkerhetsretningslinjene påvirker organisasjonen og ansatte. Innenfor dette forskningsområdet har det blitt rettet søkelys på to faktorer, informasjonssikkerhetskultur og bevissthet og sosioemosjonelle konsekvenser for ansatte. Førstnevnte handler om forskning som undersøker hvordan implementeringen av retningslinjer for informasjonssikkerhet påvirker felles verdier, holdninger og forståelse av sikkerhet i organisasjonen. Den sosioemosjonelle faktoren handler om forskning på hvordan informasjonssikkerhetsretningslinjer påvirker de ansattes følelser, som eksempelvis tillit og motivasjon.

Det tredje hovedområdet omhandler organisatoriske og individuelle faktorer som påvirker etterlevelse av retningslinjene. Dette forskningsområdet utgjør omtrent 70 prosent av studiene som omtales i denne litteraturgjennomgangen, og består av forskning som ser på hvilke faktorer som fører til økt grad av etterlevelse og forskning som ser på det motsatte. Her har forskerne vært interessert i hvordan karakteristikker som organisatoriske verdier, normer og miljø, de sosioemosjonelle konsekvensene av retningslinjene (stress, trivsel, motivasjon etc), personlige normer og moralitet hos enkeltansatte har innvirkning på etterlevelsen av retningslinjer. Videre ser de på i hvilken grad de ansatte opplever informasjonssikkerhetsretningslinjene som legitime, rettferdige og nødvendige påvirker etterlevelsen av retningslinjene i organisasjonen. Det fjerde hovedområdet handler om forskning som ser på informasjonssikkerhetsstyringen påvirker måloppnåelse i organisasjonene, eksempelvis reduksjon i sikkerhetsbrudd. Noe av forskningen på dette feltet har sett på sammenhengen mellom innføring av retningslinjer og antall sikkerhetshendelser og alvorlighetsgraden av disse. Det femte, og siste, hovedområdet for forskning på informasjonssikkerhetsstyring i organisasjoner omhandler endring og oppdatering av informasjonssikkerhetsretningslinjene. Mye av forskningen på dette feltet fokuserer på å kartlegge hyppigheten av oppdateringer og endringer, hvorfor organisasjonene velger å endre eller oppdatere retningslinjene sine, samt om dette påvirker sikkerheten i form av antall sikkerhetsbrudd. Andre forskere har en mer konseptuell tilnærming ved å modellere trinnene som burde være på plass for å foreta justeringer, eksempelvis med å starte med risikovurderinger etterfulgt av utvikling av retningslinjer og til slutt evaluering.

I sin litteraturgjennomgang belyser Soomro, Shah og Ahmed (2016) at mye av forskningen på informasjonssikkerhet har tidligere blitt gjennomført med en teknologisk vinkling. Den

senere tiden har det derimot blitt rettet mer oppmerksomhet rundt betydningen av ledere i informasjonssikkerhetsstyringsarbeidet. Den eksisterende litteraturen tar for seg mange ulike ledelsesaspekter som har betydning for informasjonssikkerhetsstyringen og artikkelen kategoriserer disse i fem grupper. Den første gruppen kalles *«informasjonssikkerhet og ledelse»,* litteraturen viser til at teknologiske løsninger på informasjonssikkerhetsutfordringer er avhengig av interne informasjonssikkerhetsretningslinjer og andre organisatoriske strategier i virksomhetene, og derfor bør ses i relasjon til virksomhetens ledelse. Litteraturen peker på viktigheten av at ansvaret for informasjonssikkerhet ikke bare blir lagt på tekniske avdelinger, men at toppledelsen i virksomhetene er involvert. Litteraturen viser til at det ikke er nok å bare utarbeide informasjonssikkerhetsstrategier og informasjonssikkerhetssystemer i seg selv, disse må kontinuerlig evalueres og endres for å tilpasses til nye trusler, noe som forutsetter engasjement fra toppledelsen. Den andre gruppen av ledelsesaspekter er *«informasjonssikkerhetsretningslinjer, opplæring og bevissthet»*. Flere av studiene innenfor denne gruppen fokuserer på betydningen av trening, opplæring og bevisstgjøring rettet mot organisasjonens informasjonssikkerhetspolitikk.

«Informasjonssikkerhet og integrasjon av ledelsesaktiviteter og tekniske aktiviteter» handler om at informasjonssikkerhetsstyring kan deles i en teknisk del og en ledelsesdel, hvor ledelsen blant annet har ansvar for utvikling av strategier, innkjøp av utstyr, bevisstgjøringsaktiviteter, internkontroll etc, mens den tekniske delen håndteres av IT og sikkerhetsspesialister. Uten teknisk kompetanse vil ikke ledelsen kunne styre informasjonssikkerheten, samtidig viser også litteraturen at IT og sikkerhetsspesialister ikke klarer å ivareta informasjonssikkerheten uten støtte og engasjement fra ledelsens side. Litteraturen viser derfor til et behov for å integrere tekniske aktiviteter og ledelsesaktiviteter. *«Informasjonssikkerhet og det menneskelige aspektet»* er den fjerde gruppen av ledelsesaspekter, her viser forskningen at mennesker er det mest kritiske elementet i informasjonssikkerhetsstyring, og kan ha både positiv og negativ innvirkning på informasjonssikkerheten i en virksomhet. *«Informasjonssikkerhet som et overordnet forretningsspørsmål»* er den siste gruppen av ledelsesaspekter, innenfor dette feltet argumenterer flere forskere for at informasjonssikkerhet burde ses i en bredere kontekst og bli behandlet som et forretningsspørsmål på lik linje med andre aktiviteter som har samme innvirkning på markedsposisjon. Dersom informasjonssikkerhet blir diskutert på høyeste nivå i virksomhetene vil informasjonssikkerhetsarbeidet bli sammenflettet med den overordnede virksomhetsplanleggingen og derfor også få nødvendig oppmerksomhet og engasjement.

Bekkevik, Holm, Vassilakopoulou og Hustad (2018) har undersøkt hvilke hovedutfordringer som preger organisasjoners informasjonssikkerhetsarbeid og hvordan disse imøtekommes gjennom ulike organisatoriske tiltak og initiativer. Førstnevnte av disse hovedutfordringene viser til problemene i tilknytning til at det ikke er uvanlig at de ansatte i organisasjoner verken har lest eller har kjennskap til de interne retningslinjene for informasjonssikkerhet, noe som igjen kan ha innvirkning på de ansattes beslutninger og risikoatferd i forbindelse med arbeidet som utføres. «*Individuell and personal risks*» viser til at individuelle og personlige faktorer kan ha en innvirkning på hvorvidt interne regler og prosedyrer overholdes. På samme måte som at de ansatte kan bidra til å forbedre informasjonssikkerhetsnivået i organisasjonene kan nivået på en annen side stagnere og påvirkes av variasjoner mellom de ansattes personligheter, intensjoner, holdninger og atferd. «*Culture and security awareness*» tar for seg hvordan informasjonssikkerhet kan anses som et aspekt av en organisasjonskultur. Utfordringene med å implementere en adekvat sikkerhetskultur i organisasjoner kan relateres til variasjoner omkring hva som anses som relevante sikkerhetsspørsmål mellom ulike grupper i organisasjonen og avstanden mellom ledelsen og øvrige hierarkiske nivåer. En mangelfull sikkerhetskultur kan gjøre organisasjonen sårbare for digitale angrep og for alvorlige sikkerhetsbrudd fordi ansatte i virksomheten kan bryte regler for informasjonssikkerhet uten å ha kjennskap til disse. «*Organizational and power relations*» vektlegger utfordringer relatert til ulike maktforhold og målsettinger som eksisterer i organisasjoner. Fordi organisasjoner kan ha strategier og målsetninger om effektivitet, produksjon og sikkerhet, kan utfordringer oppstå med å tilpasse informasjonssikkerhet til øvrige organisasjonsmål.

1.5. Undersøkelsens struktur

I dette kapittelet har vi redegjort for bakgrunnen for undersøkelsen, samt problemstilling og forskningsspørsmål denne studien har til hensikt å undersøke og besvare. I delkapittelet som tar for seg studiens avgrensning har vi hatt som formål å belyse hvilke valg og avgrensinger som har blitt gjort for å beskrive nærmere hvilke områder denne undersøkelsen vil legge særlig vekt på. I kapittel 2 redegjøres det for studiens kontekst, som går inn på selve rammene rundt studien. Her vil vi gå nærmere inn på digitaliseringen i kommunal sektor og gjøre rede for hvilke målsetninger og prioriteringer som ligger til grunn for utviklingen fremover. Her gir vi også en beskrivelse av relevant lovverk på informasjonssikkerhetsområdet. Kapittel 3 beskriver det teoretiske rammeverket som senere vil brukes i studiens diskusjonskapittel.

Kapittel 4 beskriver de metodiske valgene som har blitt gjort i gjennomføringen av studien med en nærmere utdypning av selve forskningsprosessen. Denne delen vil også diskutere kvalitetskriteriene opp mot det innsamlede datamaterialet. I kapittel 5 presenteres empiriske funn innhentet fra vår dokumentanalyse og intervjuer med informanter i ulike kommuner. Disse funnene vil i kapittel 6 diskuteres i lys av det teoretiske rammeverket. Studiens konklusjon og besvarelse av problemstilling vil bli belyst i kapittel 7. I sistnevnte kapittel vil vi også komme med forslag til videre forskning.

2.0 Kontekst

Regjeringen har en ambisjon om at Norge skal være ledende internasjonalt i digitaliseringen av forvaltningen. Digitalisering beskrives som et sentralt verktøy i arbeidet med å effektivisere prosesser, for eksempel ved å automatisere tidligere manuelle arbeidsoppgaver eller ved å tilpasse tjenester slik at man kan oppnå raskere og mer presis saksbehandling. Digitalisering er derfor et innsatsområde for å sikre økonomisk vekst samt en velfungerende velferdsstat for fremtiden. For kommunene vil digitalisering representere et viktig virkemiddel for å målsetningen om mer brukerrettede og sammenhengende tjenester (Statistisk sentralbyrå, 2019). Kommunale virksomheter har en bred og omfattende oppgaveportefølje hvorav oppgavene som utføres og tjenestene som tilbys av disse virksomhetene er av stor betydning for innbyggernes liv så vel som for næringslivet. Siden kommuner er ansvarlige for å drifte og forvalte store deler av velferdstjenestene i Norge inngår også informasjonsbehandling som en naturlig del av sektorens oppgaver.

2.1 Digitalisering i offentlig sektor

Regjeringens prioriteringsområder knyttet til IKT beskrevet i *digital agenda* har fått stor betydning for digitaliseringsarbeidet i kommunal sektor, der det pågående digitaliseringsarbeidet i landets kommuner gjenspeiler disse. Kommunesektorens organisasjon (KS) utarbeidet i 2017 en digitaliseringsstrategi for kommuner og fylkeskommuner der strategien vekta hvordan de nasjonale målsetningene kunne overføres til digitaliseringsarbeidet i kommunal sektor (Kommunesektorens organisasjon, 2017). I tillegg har også Kommunal- og moderniseringsdepartementet utarbeidet en digitaliseringsstrategi for årene 2019-2025 for offentlig sektor som er en videreføring av det arbeidet som ble gjort i digital agenda for Norge. Vi vil hovedsakelig ta utgangspunkt i KS digitaliseringsstrategi for 2017-2020 som spesifikt omhandler kommunal sektor, men vil supplere denne med det som kommer frem i Kommunal- og moderniseringsdepartementets digitaliseringsstrategi for 2019-2025 for å kunne si noe om den planlagte utviklingen av offentlig sektor i årene fremover.

Brukeren i sentrum er en målsetning som handler om at kommunale tjenester skal være sammenhengende og bidra til helhetlige tjenester utviklet på bakgrunn av en grundig forståelse av brukernes behov. Brukere er i denne sammenheng innbyggere, ansatte, frivillige organisasjoner og det private næringsliv. En metode som kan benyttes for å utvikle tjenester

som har brukernes behov i sentrum er tjenestedesign, hvor man systematisk kartlegger behovene til de som bruker tjenesten ved å samle inn tilbakemeldinger. De tilbakemeldingene man samler inn vil igjen kunne fungere som grunnlag for forbedring ved oppdatering av tjenester, eller i arbeidet med å utvikle nye tjenester (Kommunesektorens organisasjon, 2017). I tillegg fremhever Kommunal- og moderniseringsdepartementet (2019) at et prioriteringsområde frem mot 2025 er å sørge for at brukerne skal kunne oppleve offentlig sektor og de tjenestene som tilbys som sammenhengene og effektive, som én digital offentlig sektor. Med sammenhengende tjenester menes det at de digitale løsningene skal være utviklet på en slik måte at brukeren skal få enkelt tilgang til relevant informasjon, sine data og hjelp uavhengig om vedkommende er pålogget en kommunal, fylkeskommunal eller statlig nettside eller løsning.

Digitalisering er en vesentlig innsatsfaktor for innovasjon og økt produktivitet er det andre satsingsområdet som handler om hvordan digitalisering kan bidra til innovasjon, effektivisering og bedre tjenester som krever færre ressurser. Blant annet nevnes innovative anskaffelser som et viktig verktøy som kan bidra til at utfordringer løses på nye og mer effektive måter, slik at man oppnår samfunnsmessige gevinster. Innovative anskaffelser innebærer at kommunene utnytter de mulighetene regelverket gir i alle faser av anskaffelsesprosessen, og setter klare krav til markedet om utvikling av innovative løsninger på noen definerte behov. På denne måten presses markedet til å utvikle tjenester som møter fremtidens behov, og som er utviklet på bakgrunn av brukernes behov. Poenget med innovative anskaffelser er at kommuner skal være gode bestillere slik at løsningene som utvikles både tilfredsstiller behov i dag og i fremtiden, i stedet for at det er leverandørene av tjenester samt dagens etablerte tekniske løsninger som er avgjørende for hva som utvikles (Kommunesektorens organisasjon, 2017).

Stordata innebærer alt fra offentlige data, informasjon som ligger på internett, data fra bedrifter eller sanntidsinformasjon fra sensorer i det offentlige rom som trafikklysdata eller data fra bomstasjoner som sier noe om trafikkbildet. Denne typen data kan analyseres for å evaluere effekten av eksisterende tjenester eller i utviklingen av nye tjenester, hvor analyse av stordata kan brukes for å kartlegge behov. Analyse av stordata kan i tillegg til å bidra til utvikling av smartere og mer effektive tjenester i det offentlige også bli gjort tilgjengelig for andre relevante aktører som forskere, næringslivet eller innbyggere slik at disse kan benytte dataene i andre sammenhenger (Kommunesektorens organisasjon,

2017). Økt bruk av stordata følges også opp i Kommunal- og moderniseringsdepartementets digitaliseringsstrategi for 2019-2025, i denne sammenheng nevnes en metode kalt datasjø for lagring av alle typer data (dokumenter, bilder, lydfiler, logger etc) som skal fungere som en kilde til all data innenfor et område, og hvor flere kan ha tilgang samtidig. En datasjø kan derfor være en felles standardisert datadelingsløsning for en hel sektor og legger til rette for effektiv deling og tilgang til relevante data (Kommunal- og moderniseringsdepartementet, 2019). Et annet prioritert innsatsområde i det kommunale digitaliseringsarbeidet frem mot 2025 er ifølge Kommunal- og moderniseringsdirektoratet (2019) at forvaltningen skal gjenbruke informasjon fremfor å etterspørre forhold brukerne allerede har opplyst om. Denne målsetningen bygger på prinsippet om «kun-en-gang» og innebærer at den offentlige forvaltningen må gjenbruke data slik at brukerne slipper å oppgi samme type informasjon til ulike offentlige virksomheter/tjenestetilbud (Kommunal- og moderniseringsdepartementet, 2019).

Styrket digital kompetanse og deltakelse er det tredje satsingsområdet i KS digitaliseringsstrategi for kommuner og fylkeskommuner 2017-2020 og handler om at økt bruk av ny teknologi og digitalisering gir bedre muligheter for demokratisk deltakelse samt bedre og mer effektive tjenester. Dette fører samtidig til økte krav om digital kompetanse hos brukerne. I dag mangler mange av brukerne tilstrekkelig kompetanse for å ta i bruk digitale tjenester og kan derfor ikke benytte seg av «selvbetjenings-ordninger» som vil kunne spare kommunene for mye ressursbruk. Kommunene må derfor bidra til at innbyggerne får tilstrekkelig digital kompetanse til å kunne benytte seg av disse tjenestene (Kommunesektorens organisasjon, 2017). Digitaliseringen stiller også økte krav om kompetanse for medarbeidere og ledere i kommunene. Ledere må ha kompetanse til å håndtere digitale omstillingsprosesser for å skape effektive arbeidsprosesser, sørge for at tjenestene er av god kvalitet, redusere sårbarhet grunnet digitalisering, hente ut gevinster og fremstå som en attraktiv arbeidsgiver slik at riktig kompetanse kan rekrutteres. For å kunne håndtere et mer teknologiintensivt arbeids- og samfunnsliv ser Kommunal- og moderniseringsdepatementet (2019) også behovet for å øke digital kompetanseheving i offentlig sektor i årene fremover som et viktig satsingsområde.

Effektiv digitalisering av offentlig sektor handler om at de offentlige tjenestene skal være sammenhengende og helhetlige uavhengig av hvilken offentlig virksomhet som er tilbyder. Mange av de digitale tjenestene kommuner tilbyr, eksempelvis barnehagesøknad

og søknad om utdanning på videregående er relativt like og derfor har digitalisering av tjenester et stort gjenbrukspotensial (Kommunesektorens organisasjon, 2017). Kommunal- og moderniseringsdepartementet (2019) understreker også behovet for økt bruk av fellesløsninger for å sikre bedre samhandling mellom kommuner, fylkeskommuner og statlige virksomheter ved å utvikle et felles digitalt «økosystem» for offentlige virksomheter. Økosystemet skal foruten å sikre bedre nasjonal digital samhandlingen også sikre at de offentlige virksomhetene får tilgang til nødvendig fellesfunksjonalitet og felles IT-arkitekturer. Slike felles IT-løsninger og tekniske plattformer er eksempelvis digital postkasse, helsenorge.no, nav.no og ID-porten.

Informasjonssikkerhet, personvern og dokumentasjonsforvaltning er det siste satsingsområdet i digitaliseringsstrategien for kommuner og fylkeskommuner 2017-2020. Fordi digital sikkerhet anses som en forutsetning for å ivareta tilliten til offentlig sektor og deres digitale tjenester og IT-systemer avhenger en vellykket digitalisering om å ivareta krav til den enkeltes personvern og sikkerhet på en god måte (Kommunesektorens organisasjon, 2017). Når stadig flere av de kommunale tjenestene og kommunikasjonskanalene med brukere blir digitalisert blir også ansvaret på offentlig sektor om å ivareta rettighetene til den enkelte større. Brukere av kommunale tjenester har rett på innsyn i egne saker og riktig informasjon må være tilgjengelig ved behov, men må samtidig sikres slik at den ikke kommer på avveie. Ulike typer hendelser kan ramme kommunale og fylkeskommunale IKT-systemer, noe som gjør at det oppstår et behov for systemer for avvik og krisehåndtering. Kommunene bør derfor samarbeide og dele informasjon om egne opplevelser om uønskede hendelser, slik at disse utfordringene kan håndteres (Kommunesektorens organisasjon, 2017).

2.2 Regelverk som legger føringer for informasjonssikkerhetsarbeidet i kommunal sektor

Lov om kommuner og fylkeskommuner (Kommuneloven)

Kommuneloven (2018) har som formål å fremme kommunalt og fylkeskommunalt selvstyre og legger til rette for lokalt selvstyre og representativt lokaldemokrati. Det kommunale og fylkeskommunale selvstyre slik det fremgår i § 2-1 viser til at enhver kommune og fylkeskommune er å bli ansett som et eget rettssubjekt som kan ta beslutninger etter eget initiativ og ansvar. Det kommunale selvstyret uøves innenfor nasjonale rammer, hvor

begrensninger i kommunenes selvstyre må være hjemlet i lov. I § 5-3 kommer det frem at det er kommunestyret som er det øverste organ i kommunene, og som har myndighet til å ta beslutninger om vedtak på vegne av kommunen. § 17-1 åpner opp for at kommuner og fylkeskommuner kan opprette interkommunale samarbeid for å for å løse felles oppgaver. Digitaliseringsdirektoratet (2020a) skriver på bakgrunn av § 5-3 i kommuneloven at det er de politisk valgte organene som har beslutningsmyndigheten vedrørende hvordan det administrative apparatet i kommuner og fylkeskommuner skal organiseres, og at dette også gjelder i forbindelse med organiseringen av informasjonssikkerhetsarbeidet. Det vil si at det er kommunestyret som tar avgjørelser om hvordan informasjonssikkerhetsarbeidet i enkeltkommuner skal organiseres. Kommuneloven legger derfor opp til stor valgfrihet for kommunene. Til tross for stor frihet i valg av organisering stilles det spesifikke krav til offentlige virksomheter om styring og kontroll på informasjonssikkerhet.

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

eForvaltningsforskriften § 15 stiller krav om internkontroll på informasjonssikkerhetsområdet til forvaltningsorganer som benytter elektronisk kommunikasjon. Forvaltningsorganene som rammes av eForvaltningsforskriften § 15 er pliktet til å beskrive mål og strategi (sikkerhetsmål og sikkerhetsstrategi) for informasjonssikkerhet i sin egen virksomhet, noe som også skal være grunnlaget for virksomhetens internkontroll på informasjonssikkerhetsområdet. Videre skal virksomhetens internkontrollarbeid være basert på anerkjente standarder for informasjonssikkerhetsstyring og burde integreres i virksomhetens helhetlige styringssystem. Innholdet og organiseringen av internkontrollen skal være tilpasset virksomhetens risikonivå (eForvaltningsforskriften, 2004).

Personvernforordningen

Personvernforordningen er EUs regelverk om personvern og er en del av personopplysningsloven som inneholder en rekke prinsipper for ivaretakelse av personvern som alle virksomheter er pliktet til å etterfølge. Ett av disse prinsippene er forsvarlighetsprinsippet som innebærer at virksomhetene til enhver tid skal ha full oversikt over sin bruk og behandling av personopplysninger. Dette innebærer at virksomhetene må utarbeide både tekniske og organisatoriske tiltak som sørger for at lovkravet etterleves. Dette innebærer i praksis at virksomheten må gjøre egne selvstendige vurderinger før de innhenter eller bruker personopplysninger. I tillegg er også virksomhetene ansvarlige for å dokumentere

at lovkravene etterleves, eventuelle lovbrudd kan medføre sanksjoner i form av advarsler, forbud eller pålegg (Datatilsynet, u.å-b). Man finner også prinsippet om integritet og konfidensialitet som innebærer at personopplysningene skal behandles på en måte som beskytter opplysningenes integritet, konfidensialitet og tilgjengelighet. I praksis betyr dette at den virksomheten som er ansvarlig for behandling av personopplysninger også er ansvarlig for å implementere relevante tiltak for å forhindre utilsiktet og ulovlig ødeleggelse, tap av, eller endringer i personopplysningene (Datatilsynet, u.å-a).

Lov om nasjonal sikkerhet (Sikkerhetsloven)

Sikkerhetsloven (2019) gjelder for statlige, fylkeskommunale og kommunale virksomheter og har som formål å bidra til å (A) trygge Norges suverenitet, territorielle integritet og demokratiske styreform i tillegg til andre nasjonale sikkerhetsinteresser, (B) forebygge, avdekke og motvirke sikkerhetstruende virksomhet og (C) sørge for at sikkerhetstiltak gjennomføres i tråd med grunnleggende rettsprinsipper og verdier for demokratiske samfunn. Sikkerhetsloven kapittel 4 inneholder en rekke generelle krav til forebyggende sikkerhetsarbeid. § 4-1 omhandler sikkerhetsstyring og angir virksomhetsleder som ansvarlig for virksomhetens forebyggende sikkerhetsarbeid. Det stilles krav om at det forebyggende sikkerhetsarbeidet skal integreres i virksomhetens styringssystem. I tillegg er virksomheten ansvarlig for at ansatte, leverandører og oppdragstakere har en adekvat risiko- og sikkerhetsforståelse. § 4-2 setter krav til at virksomhetene skal gjennomføre risikovurderinger regelmessig, og disse vurderingene skal legges til grunn for iverksetting av forebyggende tiltak. Som del av risikovurderingen skal virksomhetene kartlegge egne avhengigheter, disse kartleggingene skal gjennomgås regelmessig og eventuelt revideres. § 4-3 viser til plikt om å gjennomføre sikkerhetstiltak og øvelser for å oppnå et forsvarlig sikkerhetsnivå. Kostnadene ved sikkerhetstiltak skal være rimelige i forhold til forventet måloppnåelse og virksomhetene skal regelmessig vurdere effektiviteten av de tiltakene de innfører ved å avvikle øvelser. § 4-4 setter krav til at virksomhetene dokumenterer vurderinger av risiko, implementerte og planlagte sikkerhetstiltak. § 4-5 sier at virksomhetene er pliktet til å varsle sikkerhetsmyndigheter og tilsynsmyndigheter dersom de har blitt utsatt for, eller mistenker at de selv eller andre kan bli utsatt for sikkerhetstruende virksomheter (Sikkerhetsloven, 2019).

3.0 Teori

I dette kapittelet presenteres relevante teoretiske bidrag som sammen med empirisk datamateriale skal bidra til å besvare studiens problemstilling. Kapittelet starter med en begrepsavklaring som deretter vil følges opp av en mer inngående beskrivelse av sentrale teoretiske bidrag. Kapittelet avsluttes med en oppsummering som utdyper hvordan teori og begreper vil benyttes i denne undersøkelsen.

3.1 Begrepsavklaring

Risiko

Økende krav til digitalisering og bruk av digitale fellestjenester i kommunal sektor medfører risiko. Risikoen i kommunal sektor er knyttet til både tilsiktede og utilsiktede hendelser som kan føre til negative konsekvenser av ulik alvorlighetsgrad. Risiko kan defineres som: «*et uttrykk for konsekvens/utfall av uønskede hendelser og usikkerhet assosiert med hendelser og utfall*» (Njå, Sommer, Rake, & Braut, 2020, s. 46). Sannsynlighet kan forstås som en måte å uttrykke usikkerhet på, altså hvor trolig det er at en bestemt hendelse vil inntreffe, samt konsekvensene/utfall av hendelsen, gitt at den inntreffer (Aven, Røed, & Wiencke, 2017). Informasjonssikkerhetsrisiko kan ifølge Sutton (2014) forstås som en delmengde av en organisasjons overordnede risiko. Informasjonssikkerhetsrisiko kan forårsakes av teknologiske feil, manglende etterlevelse av prosedyrer, retningslinjer og prosesser, samt tilsiktede handlinger. Konsekvensene av brudd på informasjonssikkerheten kan resultere i uønskede konsekvenser av ulik alvorlighetsgrad, som tap av penger, juridiske problemer, tap av tillit, omdømme og manglende mulighet for organisasjonen til å utføre oppgavene sine (Sutton, 2014).

Risikostyring

Brudd på informasjonssikkerheten kan forårsakes av en rekke ulike hendelser og føre til konsekvenser av ulik alvorlighetsgrad. Kommunene har derfor behov for å ha oversikt og kontroll over risikoen de står ovenfor når det kommer til informasjonssikkerhet og systematisk jobbe for å redusere risiko. Risikostyring handler ifølge Aven et al., (2017) om

alle forhold, aktiviteter og hendelser som kan påvirke virksomheten, og dens evne til å nå egne visjoner og målsetninger. Med utgangspunkt i sistnevnte kan begrepet defineres som:

« *... alle tiltak og aktiviteter som gjøres for å styre risiko. Risikostyring handler om å balansere konflikten mellom å utforske muligheter på den ene siden, og å unngå tap, ulykker og katastrofer på den andre siden*». (Aven et al., 2017, s. 19).

Ifølge Aven et al (2017) består risikostyringsprosessen av ulike aktiviteter der det er vanlig å inndele disse i planlegging, risikovurdering og risikohåndtering. Det er ulike årsaker til at virksomheter utfører risikoanalyser. Foruten å tilfredsstille kravene i regelverk og hos myndighetene skal risikoanalyser gi et grunnlag for å kunne ta gode beslutninger. Med henvisning til sistnevnte skal risikoanalysen bidra til å finne den rette balansen mellom økonomi og sikkerhet. Risikohåndtering handler om å følge opp resultatene fra risikovurderingen, og kan beskrives som prosessen der det implementeres ulike virkemidler for å modifisere risiko.

Sårbarhet

Sårbarhet er et begrep som brukes for å beskrive et systems manglende evne til å fungere når det blir utsatt for en hendelse og problemene som oppstår når systemet skal gjenopprette funksjonaliteten sin etter å ha blitt utsatt for uønskede hendelser. Sårbarhet kan defineres som: *«et utrykk for et systems evne til å fungere og oppnå sine mål når det utsettes for påkjenninger»* (Aven, 2006, p. 13). Man kan eksempelvis si at et system er sårbart dersom man vet at systemet mangler effektive barrierer og/eller beredskapssystemer om det skulle bli utsatt for en uønsket hendelse (Aven, 2006). Systemene som undersøkes i denne studien er norske mellomstore og store kommuner. Vi forstår sårbarhet som den evnen kommunene har til å håndtere hendelser som kan true informasjonssikkerheten i digitale fellesløsninger og evnen de har til å gjenopprette (gjenoppta driften av) sin tjenesteleveranse dersom en hendelse skulle inntreffe.

3.2 Informasjonssikkerhet

Kongsvik (2013) hevder at sikkerhet generelt kan sies å omhandle trygghet mot farer som kan true noe som er verdifullt for oss – som liv, helse og materielle verdier. I dag er virksomhetenes informasjonsressurser av stor verdi ettersom at disse utgjør både kjerneoppgaver og støttefunksjoner for hvordan disse utføre sine oppgaver, leverer sine

tjenester og når sine målsetninger. På bakgrunn av informasjonens verdimessige betydning, bør disse derfor behandles og sikres på lik linje med andre strategiske ressurser som kapital, bygning og produksjonsutstyr (Daler, Sjølstad, Høie, & Gulbrandsen, 2019). Et effektivt informasjonssystem skal bidra til å sørge for at informasjon og data om kunder, marked, regnskap, avtaler, varer m.m. gis til rett person til rett til tid. En utfordring i arbeidet med å sikre informasjon og informasjonssystemer er at den store økningen innen utvikling og utbredelse av informasjonsteknologi de siste tiårene har ført til et såkalt *risikogap* der sikkerhetsaspektet har blitt hengende etter utviklingen (Daler et al., 2019).

Informasjonssikkerhet innebærer sikkerhetstiltak innenfor organisatoriske, systemtekniske og fysiske områder (Daler et al., 2019). Begrepet kan defineres på ulike måter, men felles er at begrepet ofte relateres til å ivareta informasjonens egenskaper og inkluderer vanligvis de tre aspektene konfidensialitet, integritet og tilgjengelighet (Von Solms & Van Niekerk, 2013). Informasjonsressursene som skal sikres kan være all form for informasjon som er kritiske eller verdifulle for organisasjonens aktiviteter, samt mer sensitive personopplysninger der effekten av å miste denne informasjon kan få store konsekvenser for virksomhetene så vel som enkeltpersonene informasjonen angår (Åhlfeldt, Nohlberg, Söderström, Lennerholt, & van Laere, 2018). Hensynet til informasjonens konfidensialitet, integritet og tilgjengelighet handler ifølge Normann & Tranvik (2012) om å hindre at uvedkommende får tilgang til informasjonen (konfidensialitet), hindre at informasjonen eller opplysningene endres eller slettes av personer som ikke har autorisasjon til å gjøre dette (integritet), samt sørge for at opplysningene til enhver tid er tilgjengelig for rett person (tilgjengelighet).

Figur 1 The fundamental attributes of an information assets (Calder, 2009)

Den store utbredelsen av IKT i lokalforvaltningen og det pågående arbeidet med å digitalisere kommunale tjenester og systemer utfordrer sektorens eksisterende måter for hvordan informasjonen behandles, lagres og håndteres på, og gjør det mer komplisert å ivareta

hensynet til informasjonssikkerhet etterhvert som IT-bruken øker (Normann & Tranvik, 2012). Særlig har arbeidet med informasjonssikkerhet vist seg å være en utfordring i kommuner der arbeidet har vist seg å utføres på ustrukturerte og lite sammenhengene måter, i stor grad som følge av kompleksitetene i de forskjelligere grenene av aktiviteter kommunene har ansvar for (Åhlfeldt et al., 2018).

3.3 Regulering

Regulering omfavner bredt, noe som gir variasjoner i hvordan begrepet blir omtalt og forstått i ulike akademiske sammenhenger. Mangelen på entydige beskrivelser medfører at reguleringsbegrepet har ulik anvendelse innenfor ulike samfunnsområder, i tillegg til at vår forståelse av reguleringsbegrepet og selve motivene for regulering har endret seg over tid (P. Lindøe, Kringen, & Braut, 2012). Til tross for begrepets vide omfang hevder Baldwin, Cave & Lodge (2012) at regulering kan forstås som et fenomen som dekker følgende områder:

- *Spesifikke ordre* der regulering kan ses i forbindelse med kravene som fremgår i den norske helse, miljø og sikkerhetslovgivningen.
- *Bevisst statlig påvirkning* der regulering dekker alle statlige handlinger som er utformet for å påvirke virksomheter eller sosial atferd.
- *Alle former for sosial eller økonomisk innflytelse* der alle mekanismer som påvirker vår atferd enten om disse pålagt fra staten eller av andre kilder anses som regulerende.

Foruten variasjonene i hvordan reguleringsbegrepet kan forstås, kan det være ulike motiver og argumenter som fremmer et reguleringsbehov. Baldwin, Cave & Lodge (2012) hevder eksempelvis at de tekniske motivene for regulering kan ses i sammenheng med at myndighetene ønsker å sikre at samfunn, organisasjoner og industrier opptrer på en måte som kommer felleskapet til gode (Baldwin et al., 2012). Sistnevnte begrunner med andre ord reguleringsbehovet gjennom at regulering er et nødvendig virkemiddel for å påvirke og styre aktørenes atferd i ønsket retning.

Reguleringsregimer

Man kan hovedsakelig skille mellom to strategier for å regulere risiko og promotere sikkerhetsarbeid i organisasjoner fra et regulatorperspektiv. Hopkins (2011) omtaler disse strategiene som henholdsvis *risk management* (risikobasert) og *rule-compliance* (regelbasert) reguleringsregimene. Til tross for å være to ulike tilnærminger til risikoregulering, er disse

ikke nødvendigvis gjensidig utelukkende strategier, men heller komplementære, og i praksis vil disse ofte opptre i kombinasjon der man finner elementer fra begge. Det regelbaserte reguleringsregimet har historisk sett vært den dominerende reguleringsformen, og beskrives som en ovenfra og ned tilnærming til regulering der myndighetsorganer angir spesifikke, detaljerte og ofte tekniske krav som skal styre retningen på virksomhetenes sikkerhetsarbeid (Jore, 2015). Organisasjonene som dekkes av de samme preskriptive myndighetskravene kan dermed forventes å implementere de samme tiltakene, uavhengig om dette samsvarer med den enkeltes lokale kontekst eller risikobilde. Den risikobaserte reguleringsformen gir i motsetning til den regelbaserte sjeldent klare føringer, og er heller basert på funksjonelle krav. Sistnevnte innebærer forenklet en regelverkstype som setter krav til resultatet uten å si noe om hvordan det skal oppnås (P. Lindøe et al., 2012).

Mer utdypende kan et funksjonelt utformet regelverk sies å ha som hovedfokus at den beskriver målene organisasjonene skal oppnå, uten at det foreligger verken detaljerte beskrivelser eller krav om hvilke løsninger som skal benyttes for å nå disse målene. Det risikobaserte kontrollregime fikk ifølge Lindøe et al. (2012) sitt gjennombrudd på 1970-tallet der myndighetskontrollen på HMS området ble flyttet fra myndighetenes detaljerte regler til fordel for økt egenkontroll i relasjon til virksomhetens sikkerhetsarbeid. Internkontroll ble i den sammenheng sett på som det nye virkemiddelet som skulle erstatte de tradisjonelle reguleringsformene, og førte til at virksomhetene fikk økt ansvar og frihet til å utvikle individuelle løsninger tilpasset lokale behov og en lokal kontekst (P. H. Lindøe, 2018). Videre ble virksomhetene pålagt å vurdere risikoen i tilknytning til egne produksjonssystemer, arbeidsprosesser og produkter. Grunntanken med den risikobaserte tilnærmingen er ifølge Jore (2015) at den bygger på oppfatningen om at det er organisasjonene selv som besitter nødvendig kompetanse for å vurdere fremtidig risiko, samt kunnskap for å håndtere disse. Det blir dermed opp til virksomhetene å finne løsninger som er optimale for virksomheten selv, i tillegg til at et funksjonelt utformet regelverk vil ha lettere for å henge i samfunnsutviklingen som følge av økende kompleksitet, teknologisk utvikling og raske omstillinger (P. Lindøe et al., 2012). Motsatt vil et preskriptivt regelverk ha større vansker med å holdes oppdatert i tråd med utviklingen, på bakgrunn av tiden det tar å oppdatere regelverket som regulerer aktivitetene i virksomhetene på en mer direkte måte. Sistnevnte kan også relateres til hvorfor Jore (2015) beskriver den regelbaserte reguleringsformen som mer reaktiv, da nye reguleringer påføres virksomhetene som en respons på uønskede hendelser som allerede har inntruffet.

På bakgrunn av at regelverket som regulerer informasjonssikkerhetsarbeidet i kommunal sektor er funksjonelt utformet, vil denne studien ha et større fokus på den risikobaserte reguleringsformen. Hvorvidt dette er den optimale reguleringsformen, er det på en annen side uenigheter om i den akademiske litteraturen. Hopkins (2011) hevder blant annet at fremfor å forsøke å velge mellom en av disse reguleringsstrategiene, bør fokuset heller være å forsøke å oppnå en riktig balanse mellom strategiene. Hopkins mener utviklingen i alt for stor grad har gått i retning av den risikobaserte reguleringsformen, og påpeker at regler har sin nytteverdi og funksjon i form av at disse kan veilede aktører i krevende beslutningssituasjoner.

3.4 Barry Turner Man-made Disaster

På bakgrunn av sitt eget doktorgradsarbeid to år i forkant publiserte Barry Turner boken om «Man-Made Disasters» i 1978. Boken fikk en ny utgave i 1997 med Nick Pidgeon som medforfatter. Turner argumenterte med utgangspunkt i sin analyse av 84 britiske ulykkesrapporter at katastrofer kan ses som et resultat av samspillet mellom menneskelige og organisatoriske betingelser i sosio-tekniske systemer (Pidgeon & O'Leary, 2000). Fremfor å årsaksforklare katastrofer fra et teknisk ståsted, og/eller betrakte disse som tilfeldige inntrufne hendelser, kan disse på tross av å fremstå som store overraskelser, relateres til en rekke tidlige signaler som ble oversett, ignorert og/eller mistolket. Sentralt i Turners perspektiv er at han forklarer katastrofer med hensyn til de sosiologiske konsekvensene disse påfører systemer fremfor de fysiske innvirkningene disse har for liv, helse og miljø (Pidgeon & O'Leary, 2000). Turner observerte gjennom sin forskning at alle organisasjoner operer med en rekke kulturelle overbevisninger og normer med hensyn til farer, og håndteringen av disse. Med henvisning til katastrofers sosiologiske konsekvenser viser Turner til hvordan slike hendelser påfører kollaps eller sammenbrudd av de kulturelle virkelighetsoppfatningene, holdningene og normene i systemet.

Etter denne teorien skiller en katastrofe seg fra mindre ulykker ved at det foreligger et kritisk avvik mellom de rådende antakelsene og den reelle sikkerhetstilstanden i systemet (Pidgeon & O'Leary, 2000). Det har med andre ord vært et misforhold mellom det risikobildet organisasjonene har forholdt seg til og drevet sine risikostyrende aktiviteter etter, og det faktiske risiko- og sårbarhetsbilde disse omgir seg i. Til tross for at fokuset i denne undersøkelsen ikke spesifikt retter seg mot forebyggingen av storulykker og katastrofer, kan

flere av de elementene i Turners sosiotekniske tilnærming benyttes som grunnlag for å beskrive hvordan uønskede hendelser og systemsvikt kan oppstå i kommunale virksomheter.

Selv om de fleste ulykker og katastrofer har tekniske aspekter med seg hevder Turner at majoriteten av disse kan ses i sammenheng med en rekke sosiale, administrative og ledelsesmessige faktorer (Barry A. Turner, 1994). Turner (1994) er særlig opptatt av hvordan *sloppy* management, altså kombinasjonen av ledelsesmangler og organisatoriske ordninger, skaper forutsetninger for slike ulykker. Disse er igjen bidragsytende faktorer til at kritiske signaler ikke fanges opp i forkant av ulykker, i perioden Turner omtaler som inkubasjonstiden. Med inkubasjonstiden illustrer Turner hvordan ulykker kan ses på som en prosess som utvikler seg gjennom en lang kjede av hendelser, der inkubasjonsperioden bidrar til at feil, misforståelser og misoppfatninger om risikoproblemer får utvikle seg ubemerket, og gjør systemet sårbart for katastrofer. Dersom utviklingen av slike forhold ikke avdekkes vil de senere fungere som latente betingelser som i påvente av den rette triggeren vil utløse en ulykke og/eller systemsvikt (Barry A. Turner, 1994).

Informasjonsvansker og informasjonsprosessering

I tidsrommet før en katastrofe eller ulykke kan en rekke indikatorer anses som signaler på at en inkubasjonstid er i ferd med å bygge seg opp. Turner fremhever blant annet hvordan kommunikasjonsmangler og problemer knyttet til informasjonsflyt kan bidra til at organisasjoner mister kontakten med sin operasjonelle virkelighet (Barry A. Turner, 1994). Vi vil videre gjennomgå tre utfordringene relatert til informasjonsvansker som Turner tar for seg.

Avledningsproblemet (The decoy problem) viser til et tilbakevendende trekk i mange av ulykkesrapportene Turner studerte. Fenomenet handler om hvordan tiltak og handlinger iverksatt for å løse et problem eller for å håndtere en fare flytter oppmerksomheten fra de reelle problemene (Barry A Turner, 1976). Avledningsproblemet viser altså til hvordan organisasjoner har misforstått signalene i form av at tiltak rettet mot et klart definert problem har ledet oppmerksomheten bort fra mer komplekse og mindre strukturerte problemer i forbindelse med hendelsens inkubasjonsfase. *Variabel atskillelse av informasjon* er et fenomen som Turner relaterer til informasjonsvansker og beskriver hvordan informasjon spredt mellom mange aktører bidrar til mangelfull forståelse og klassifisering av problemet blant de involverte partene (Pidgeon & O'Leary, 2000). Risikoproblemene som akkumuleres,

skyldes ikke forvirring eller manglende teknologisk forståelse, men forårsakes av at ulike personer besitter ikke-overlappende biter av informasjon om hva som skjer, slik at det utvikles ulike teorier om problemene i systemet (Weick, 1998). Ulike fortolkninger av problemet forsterkes ytterligere av problemets komplekse og dynamiske karakter noe som bidrar til stadig nye problemforståelser blant de involverte aktørene som besitter biter av informasjonsgrunnlaget.

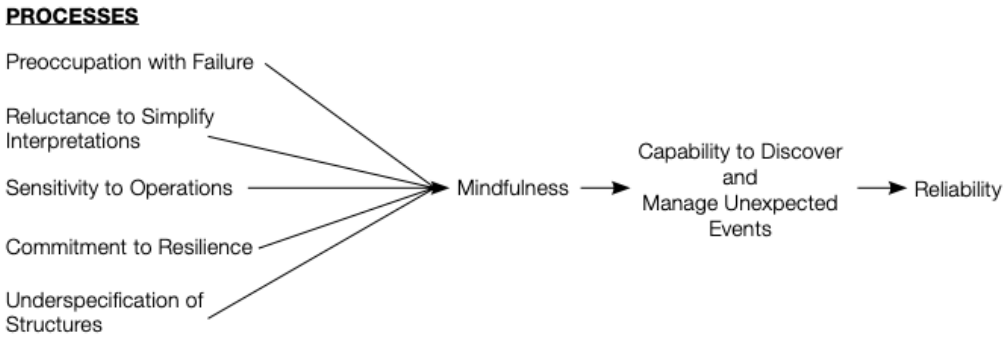
Motvilje til å prioritere fremvoksende farer handler om et fellestrekk Turner identifiserte i mange av de studerte ulykkene. Turner hevdet at en gjentakende prosess i flere av disse var at når mulige farer først ble oppfattet, ble disse undervurdert (Barry A Turner, 1976). Resultatet får derfor store konsekvenser for det preventive arbeidet ettersom de involverte partene vil ha en tendens til å minimere faren når den først identifiseres, eller benekte at faren truer dem direkte (Pidgeon & O'Leary, 2000).

3.5 Høy pålitelige organisasjoner (HRO)

Der Perrows (1999) Normal accident theory kan sies å ha et pessimistisk syn når det gjelder vår evne til å håndtere risikoen i tilknytning til komplekse og tett koblede systemer har High Reliability-teorien som utgangspunkt at ulykker i høyteknologiske systemer kan forebygges. Teorien som i sin helhet omtales som *High Reliability Organisation* (HRO) ble utviklet av en gruppe forskere ved University of California, Berkeley, og vektlegger hvordan høyrisikoorganisasjoner kan fungere trygt til tross for at disse innehar egenskapene i form av å være komplekse og tett koblede systemer (Sutcliffe, 2011). Weick, Sutcliffe & Obstfeld (2008) omtaler HRO som en samlebetegnelse på organisasjoner som har til felles at de opererer under svært krevende sosiale og politiske omgivelser der alvorligheten av potensielle feil gjør at organisasjonene til tross for høy ytelse må klare å opererer mest mulig feilfritt. Der ikke-HRO organisasjoner har en tendens til å prioritere effektivitet og produksjonsmål, er et særtrekk med de beste HRO organisasjonene at unngåelsen av feil og pålitelig ytelse sidestilles med produktivitet som dominerende målsetning (Roberts, 1990). Pålitelig ytelse oppnås når organisasjonene er i stand til å håndtere og tilpasse seg uforutsette situasjoner på en måte som forebygger utilsiktede konsekvenser. Premissene for pålitelig ytelse er det Vogus, Rothman, Sutcliffe & Weick (2014) omtaler som en nødvendig tilstand av mindfulness som innebærer at organisasjonene er proaktive i sine søk etter svake signaler i omgivelsene slik at effektivt kan oppdage og respondere ovenfor uforutsette situasjoner. Sutcliffe (2011) omtaler mindfulness som en «motgift» mot overraskelser. Hos individene

som opererer systemet krever dette på sin side at disse er fleksible nok til å gjenkjenne svake signaler samt gripe inn i riktig øyeblikk.

Figur 3 gir en oversikt over det Weick et al. (2008) beskriver som premissene for høy pålitelighet og årvåkenhet (state of mindfulness). Figuren viser også til det forskerne omtaler som fem kognitive prosesser som videre anses som nødvendige betingelser for å skape tilstanden mindfulness, for effektiv feildeteksjon i omgivelsene.



Figur 2 A mindful infrastructure for high reliability (Weick et al., 2008)

(1) Preoccupation with failure beskriver en form for «kronisk uro» man finner i de beste HRO organisasjonene der disse har til felles at de aktivt søker etter overraskelser og svake signaler i omgivelsene for å finne ut hvorvidt systemet opptrer på en uventet måte (Sutcliffe, 2011). Da HRO organisasjoner har lite erfaring og datagrunnlag fra ulykker og større hendelser, blir dette søket videre betraktet som viktige forutsetninger for læring og for å styrke påliteligheten til systemet (Weick et al., 2008). Organisasjonene har i tillegg en atmosfære av tillit der de ansatte både belønnes og oppfordres til å melde fra om feil og nesten-hendelser da dette muliggjør for ytterligere læringspunkter. Sistnevnte har også sammenheng med at enhver feil som rapporteres anses som viktige indikatorer på større problemer og sårbarheter i systemet som helhet, og som kan true systemets pålitelighet.
(2) Reluctans to simplify interpretations betyr at organisasjonene aktivt søker ulike synspunkter som kan stille spørsmål til etablert kunnskap, avdekke «blind spots» og skiftende krav for å skape et mer helhetlig og nyansert bilde av pågående situasjoner (Sutcliffe, 2011). Sutcliffe (2011) hevder forenklinger er hemmende i komplekse og dynamiske omgivelser fordi det kan skape en falsk trygghetsfølelse ved at operatørene har forventninger om hva som vil møte dem. Slike forventninger kan dermed føre til at medlemmene av

organisasjonene ignorerer viktige signaler i omgivelsene og at det begrenser nødvendige forholdsregler operatørene tar, samt antall uønskede hendelser de forestiller seg. Et særtrekk med de aller beste HRO organisasjonene er at de fremfor å gjøre forenklinger har færre antagelser og sosialiserer menneskene til å legge merke til mer (Weick et al., 2008).

(3) Sensitivity to operations betyr at HRO organisasjonene skaper og vedlikeholder et integrert bilde av pågående situasjoner gjennom kontinuerlig oppmerksomhet til sanntidsinformasjon (Weick et al., 2008). *(4) Commitment to resilience* hevder Sutcliffe (2011) innebærer en kontinuerlig utvidelse av evner for å komme seg etter uventede hendelser. Et fellestrekk med de beste HRO organisasjonene er at de utvikler en evne til å både forutse (anticipate) i tillegg til å være resiliente (Weick et al., 2008). Førstnevnte handler om evnen til å forutse og forhindre potensielle farer før disse får manifestert seg. Resiliens handler på sin side om evnen organisasjonene har til å håndtere uforutsette farer og overraskelser etter de har manifestert seg for så å deretter gjenvinne funksjonaliteten til systemet. (5) Underspecification of structure viser til egenskapen de beste HRO organisasjonene har i form av at disse har en fleksibel styringsstruktur og beslutningsmyndighet ut fra situasjonsbildet (Weick et al., 2008). I normale rutinepregede operasjoner kan HRO-organisasjonene beskrives som å ha en sentralisert styring, med klar hierarkisk fordeling av beslutningsmyndigheten. I mer krevende situasjoner som avviker fra den normale driftssituasjonen, endrer beslutningsmyndigheten seg i form av at de med mest forståelse, erfaring og kunnskap for å håndtere situasjonen kan ta beslutninger for å imøtekomme den. Den fleksible styringsstrukturen gir HRO-organisasjonene mulighet til å operere pålitelig på tross av usikre omgivelser preget av informasjonsmangler (Sutcliffe, 2011). De er altså adaptive ovenfor situasjonene og desentraliserer beslutningsmyndigheten ved behov, hvor kunnskap og erfaring trumfer den enkeltes formelle rolle i organisasjonen.

3.6 Oppsummering av teori

Hensikten med dette kapittelet har vært å redegjøre for det teoretiske fundamentet i denne studien. Teoriene favner bredt, men vil brukes for å belyse ulike deler som er nødvendige for å besvare undersøkelsens problemstilling og forskningsspørsmål. Risiko og sårbarhetsbegrepet vil benyttes i kapittel 6.1 for å diskutere hvordan bruken av digitale fellesløsninger kan føre til informasjonssikkerhetsutfordringer i kommunene i form av økt risiko og sårbarhet. Risikostyring er et sentralt tema i store deler av undersøkelsen. I kapittel

6.3 vil Aven et al., (2017) sin definisjon av risikostyring ses opp mot kommunenes tilnærming til risikostyring på informasjonssikkerhetsområdet. Informasjonssikkerhetsteori vil bli benyttet i flere av diskusjonskapitlene hvor vi særlig vektlegger hvordan økt anvendelse av teknologi og digitale løsninger kan skape sikkerhetsutfordringer i kommunenes arbeid med å ivareta informasjonssikkerheten i egen virksomhet. Reguleringsteori vil videre brukes for å diskutere hvordan myndighetenes krav og regelverk på informasjonssikkerhetsområdet påvirker kommunene arbeid med risikostyring på informasjonssikkerhetsområdet.

Turners Man-made disaster teori vil brukes i analysen for å diskutere hvordan særlig informasjon og kommunikasjonsutfordringer, ledelsesutfordringer og organisatoriske ordninger i kommunene kan være en barriere i virksomhetenes digitale sikkerhetsarbeid. Ettersom HRO-teorien er utarbeidet med bakgrunn i studiet av høyrisikosystemer innen luftfart, militære hangarskip og kjernekraftverk er ikke hensikten med å anvende teorien å diskutere hvorvidt kommunale virksomheter kan betraktes som høypålitelige organisasjoner. Teorien vil istedenfor brukes for å diskutere hvorvidt vi kan identifisere organisatoriske likhetstrekk i måten HRO-organisasjoner og kommunale virksomheter tilnærmer seg risiko og arbeider for å ivareta påliteligheten i egne digitale systemer.

4.0 Metode

I dette kapittelet redegjør vi for våre metodiske valgt og avgjørelsene som er blitt tatt gjennom forskningsprosessen for å besvare studiens problemstilling og forskningsspørsmål.

4.1 Metodisk tilnærming

Forskningsdesign

Vi har valgt å benytte oss av et abduktivt forskningsdesign i denne studien fordi vi ønsker at både teori og empiri i kombinasjon skal forme vår forståelse av fenomenet vi studerer og studien som helhet. Teorien vi bruker gir oss et rammeverk, vinkling og naturlige avgrensninger, samtidig som informantene får mulighet til å påvirke den fortolkningen vi gjør av fenomenet gjennom innspill i intervjuene. Abduksjon plasserer seg et sted mellom deduksjon og induksjon. Det vil si at man har et visst teoretisk fundament som brukes for å analysere og skape forståelse av et fenomen. Hensikten er å gi en troverdig og interessant forklaring av funnene våre basert på noen allerede eksisterende teoretiske rammeverk. Teorien vi tar i bruk vil fungere som rammeverk for analysen hvor noen aspekter ved fenomenet vies oppmerksomhet og andre aspekter faller bort. Likevel legger en abduktiv tilnærming opp til at informantene får en stor innvirkning på hvordan vi tolker og forstår fenomenet vi studerer ettersom deres erfaringer, refleksjoner og holdninger vil farge dataen vi samler inn og påvirke vår forståelse. Abduksjon skiller seg fra induksjon ved å ikke være basert på rene empiriske generaliseringer (teorigenerering), og fra deduksjon fordi den ikke følger den samme strenge logiske formen som kjennetegner en deduktiv tilnærming (Danermark, Ekstrom, Karlsson, & Jakobsen, 2005). Danermark et al., (2005) beskriver videre abduksjon som en form for rekontekstualisering hvor man tar i bruk teori som ikke tidligere har blitt anvendt på et allerede kjent fenomen. Dette kan for eksempel være ved å bruke ny teori, eller ved å overføre teorier fra andre fagfelt som får frem aspekter ved, og tolkninger av fenomenet, som ikke har blitt forstått eller vurdert tidligere. Abduksjon kan på denne måten bidra til økt forståelse for fenomenet man studerer samtidig som man kan teste, utvikle og modne teorier ved å kontinuerlig bruke dem i nye settinger og forskningssituasjoner (Danermark et al., 2005).

Undersøkelsesopplegg

Vår undersøkelse vil kunne beskrives som det Halvorsen (2008) kaller et intensivt opplegg fordi vi ønsker å undersøke flere variabler og gå i dybden på noen få kommuner. På bakgrunn av dette valgte vi å utforme undersøkelsen som en case-studie hvor fokuset var å innhente en dyp forståelse av opplevd problematikk ved bruk av digitale fellesløsninger i noen få caser (kommuner). Hovedfokuset i denne undersøkelsen er å kunne sammenligne kommunene for å danne oss en forståelse over de typiske utfordringene, og hvorvidt det er variasjoner i hvordan kommunene forstår og tilpasser seg disse i tilknytning til organisering og risikostyring. Kriteriene for å velge ut caser (kommuner) var at disse (1) deltar i det interkommunale samarbeidet «Digi Rogaland» slik at vi kunne undersøke hvordan de ulike kommunene benytter seg av ressursene i et slikt samarbeid og om det er forskjeller i hvordan dette gjøres. (2) Vi ønsket også å ha litt variasjon i størrelsen til kommunene. Vi benytter oss av den tredelte størrelsesgrupperingen til SSB[1] som har kategorisert kommunene etter innbyggertall. Vi valgte videre å ta for oss det SSB omtaler som mellomstore og store kommuner fordi vi anså disse som best egnet til å generere gode data, ettersom små kommuner gjerne ikke har kommet like langt i prosessen med å implementere digitale fellesløsninger.

Ifølge Halvorsen (2008) kjennetegnes case-studier ved at man er opptatt av prosesser, altså hvordan noe forløper/utvikler seg. Ofte har man ikke en klart formulert problemstilling, men heller en hensikt om å gi en detaljert beskrivelse av et sosialt system og bygge opp en god helhetsforståelse (Halvorsen, 2008). Beskrivelsen til Halvorsen passer godt overens med hvordan vi bruker case-studie ettersom formålet vårt har vært å bygge opp en god helhetsforståelse for de sikkerhetsutfordringene kommunene opplever ved bruk av digitale fellesløsninger. Flyvbjerg (2006) argumenterer for et strategisk utvalg av informanter hvor man velger ut caser basert på validitet fremfor representativitet, ettersom dette vil generere den beste dataen. Vår informantutvelgelse kan beskrives som et strategisk utvalg, hvor informantene har blitt kontaktet på bakgrunn av at vi mener de besitter egenskaper som gjør at de kan belyse forhold relevante for problemstillingen vår. I denne undersøkelsen har vi derfor valgt å kontakte informanter vi mener har de beste forutsetningene for å gi oss gode data om potensielle sikkerhetsutfordringer ved bruk av digitale fellesløsninger.

[1] https://www.ssb.no/a/publikasjoner/pdf/rapp_201108/rapp_201108.pdf s.10.

Kvalitativ metode

Vi har valgt en kvalitativ tilnærming til denne undersøkelsen. Dette fordi det foreligger lite forskning som spesifikt undersøker sammenhengen mellom ivaretakelse av informasjonssikkerhet og bruk av digitale fellesløsninger i kommunesektoren. En kvalitativ tilnærming var derfor både hensiktsmessig, og nødvendig, for å innhente en økt forståelse og innsikt på området. I tillegg ønsket vi å få en god dybdeforståelse av teamet og for de valgene som har blitt gjort i kommunene, noe vi legger opp til gjennom hvordan-spørsmålet vårt i problemstillingen. Dette kan best oppnås ved å bruke en kvalitativ tilnærming som gir rom for at informantenes egne opplevelser, forståelser, refleksjoner og meninger kommer inn som et supplement til dokumentanalysen. Ved hjelp av å samle inn data fra mennesker med inngående kunnskap om informasjonssikkerhet og bruk av digitale fellesløsninger i kommunene kan disse bringe fram et annet perspektiv basert på egne erfaringer og refleksjoner som de skriftlige kildene ikke kan gi oss. I tillegg vil studien bli styrket ved å kombinere skriftlige kilder med data fra menneskene som daglig jobber tett opp mot de problemstillingene vi er interessert i å undersøke. Kombinasjonen av intervju og dokumentanalyse gir oss muligheten til å sammenligne hva informantene sier opp mot hva dokumentene forteller, og eventuelt kunne stille spørsmål rundt motsetninger mellom disse. I tillegg gir en kvalitativ tilnærming oss mer fleksibilitet og nærhet til empiri ettersom informantene får en større innvirkning på undersøkelsen, og har mulighet til å trekke inn temaer, problemstillinger og utfordringer utover det dokumentene nevner. Valget om å bruke kvalitativ metode henger også sammen med den abduktive tilnærmingen vår. Kombinasjonen av intervju og dokumentanalyse vil styrke mulighetene våre for å kunne benytte teorien på en meningsfull måte, og få frem interessante perspektiver og tolkninger av sikkerhetsutfordringene ved bruk av digitale fellesløsninger. Hovedskillet mellom kvalitative og kvantitative metoder beskrives av Halvorsen (2008) som forskjeller i hvilke typer data de egner seg til å samle inn. Til tross for at kvalitative data ikke utelukker bruk av tallmengder og statistikk, vil disse som regel oftest bestå av tekst og/eller verbale utsagn. Kvalitativ metode egner seg derfor bedre til å samle inn det som omtales som fyldige data om personer eller situasjoner som gjør det mulig å forstå atferd eller situasjoner slik de oppfattes og oppleves av informantene selv (Halvorsen, 2008). Kvalitativ metode gir i tillegg mer rom for fleksibilitet fordi man ikke låser seg til en spesifikk datainnsamlingsmetode på forhånd. Ved å bruke et abduktivt forskningsdesign i kombinasjon med kvalitativ metode har vi hatt en viss teoretisk forankring og tanker om hva studien vil ha hovedfokus på, samtidig som vi har vært

fleksible slik at problemstilling, forskningsspørsmål og andre momenter har endret seg som følge av empirien vi har samlet inn.

Forskningsprosessen

Forskningsprosessen består av ulike trinn. I denne undersøkelsen kan forskningsprosessen best beskrives som en sirkulær prosess hvor problemstilling, forskningsspørsmål og teoretisk rammeverk har endret seg etter hvert som prosjektet har utviklet og modnet seg. Tabell 1 gir en oversikt over fremdriften i prosjektet med henvisning til tidsperiode.

Periode	Hva som ble gjort	Hensikten med dette	Resultat
Januar	I startfasen av undersøkelsen var hovedfokuset på å finne og lese oss gjennom diverse rapporter og artikler for å få en oversikt over temaet og mulige innfallsvinkler. Etterhvert formulerte vi en problemstilling samt foreløpige forskningsspørsmål og tok parallelt med dette kontakt med en del relevante aktører for å få innspill på ideene våre. Vi ferdiggjorde også søknaden til NSD og sendte denne inn til vurdering.	Hensikten var å posisjonere oss i forhold til temaet slik at vi kunne få innspill og tilbakemeldinger på de foreløpige ideene. Vi valgte å bruke mye tid på å utarbeide søknad og dokumentasjon til NSD på et tidlig tidspunkt for å unngå at lang saksbehandlingstid skulle hindre datainnsamlingen på et senere tidspunkt.	Vi fikk lest oss godt opp på temaet og fikk utarbeidet en tentativ problemstilling. Vi fikk tilbakemeldinger fra aktører vi kontaktet om at den foreløpige problemstillingen omfavnet svært bredt. 22.01 fikk vi tilbakemelding fra NSD om at vi hadde fått godkjent det innmeldte meldeskjemaet. Vi fikk i slutten av måneden (29.01) tildelt ny veileder pga. sykdom.
Februar	Vi fortsatte arbeidet med problemstilling og FS og forsøkte å spisse disse ytterligere. Videre startet vi prosessen med å skrive på innledning- og kontekstkapitlene i undersøkelsen. Tok kontakt med potensielle informanter for å høre om disse kunne være interesserte i å delta i intervju på et senere tidspunkt. Begynte å søke etter relevant litteratur til kapittelet om tidligere forskning.	Vi fant tidlig ut at vi fortsatt hadde en for bred tilnærming og problemstilling etter tilbakemeldinger fra både veileder og informantene vi kontaktet. På dette tidspunktet var vi opptatt av å snevre oss inn slik at vi kunne begynne å tenke på teoretisk vinkling.	Etter oppstartssamtale med ny veileder bestemte vi oss for å ta undersøkelsen i en annen retning hvor vi ønsket å gå mer i dybden og avgrense oss til utilsiktede hendelser Fikk positive tilbakemeldinger fra flere kommuner.
Mars	Vi fortsatte å justere på problemstilling og FS og rettet mer fokus mot bruken av digitale fellesløsninger. Vi tok igjen kontakt med kommunene for å informere om endringene.	Vi ønsket å ha gode nok avgrensninger til å kunne begynne å starte utformingen av spørsmål til intervjuguiden. Vi	Fikk en del nye kontaktpersoner i kommunene på bakgrunn av endringene og avgrensingene vi gjorde.

	Jobbet videre med kontekstbiten og skrev ferdig kapittelet om tidligere forskning. Startet med å skrive på teori og empiri. Vi gjennomførte et digitalt videomøte med representanter fra Digitaliseringsdirektoratet hvor vi diskuterte undersøkelsens tema og problemstilling.	fokuserte også på å få gjort mest mulig på empirikapittelet før vi startet datagenereringen slik at vi hadde gode forutsetninger for å lage relevante intervjuspørsmål.	Fikk skrevet mye på teorikapittelet og kom i gang med å skrive på empiri. Vi laget fortløpende kategorier som kunne være aktuelle for intervju mens vi arbeidet med empirien.
April	Arbeidet videre med teori og empiri. Brukte mye tid på å strukturere og skrive på metodekapittelet. Skrev ferdig intervjuguide, informasjonsskriv og samtykkeskjema og fikk veileder til å gå over disse. Deretter gjorde vi noen endringer på bakgrunn av tilbakemeldingene vi fikk. Vi startet å gjennomføre intervjuene med informantene våre i midten av måneden der vi fortløpende startet arbeidet med å transkribere.	På dette tidspunktet var undersøkelsen moden og avgrenset nok til å gå i gang med datagenereringen, og vi ønsket å komme i gang med intervjuene raskest mulig.	Vi fikk et ferdig utkast av empiri og metode. Sendte ut intervjuguide, informasjonsskriv og samtykkeskjema til informantene. Gjennomførte samtlige intervjuer fra midten til slutten av april, og fikk startet transkriberingen.
Mai	Jobbet videre med å transkribere dataen og begynte etter hvert med selve analysen og prosessen med å kode og kategorisere intervjudataen. Startet å skrive på diskusjonskapittelet. På bakgrunn av funnene våre ble også problemstilling og forskningsspørsmål justert.	Her var hovedfokuset på å få transkribert ferdig intervjuene og få bearbeidet datamaterialet slik at vi kunne begynne å sammenstille de skriftlige dokumentene med intervjudataen.	Ble ferdige med databehandlingen og fikk ferdigstilt empirikapittelet Skrev ferdig et utkast til diskusjon
Juni	Gikk gjennom tilbakemeldinger fra tidligere veiledninger og gjorde mindre justeringer i metode, empiri og kontekstkapittelet for å sørge for en rød tråd gjennom hele undersøkelsen. Skrev ny innledning til undersøkelsen.	Her hadde vi ett ferdig utkast til undersøkelsen og ønsket å gå systematisk gjennom alle kapitler for å gjøre nødvendige endringer og gjennomføre korrekturlesning	Undersøkelsen ble ferdigstilt og innlevert 14.06.2021.

Tabell 1 Beskrivelse av fremdriften i forskningsprosjektet

4.2 Datainnsamling

Vi startet datainnsamlingen vår ved å foreta en dokumentanalyse. Alle dokumentene med unntak av ett som er et internt DSB-dokument[2] ligger åpent tilgjengelige for offentligheten, en oversikt over dokumentene er presentert i vedlegg 1. Dokumentanalysen har vært omfattende og består i alt av 24 dokumenter. Kort oppsummert kan dokumentene kategoriseres i følgende grupper; digitaliseringsstrategier for offentlig sektor, strategier for

[2] Direktoratet for samfunnssikkerhet og beredskap. (2018). *IKT-sikkerhet på regionalt og lokalt nivå*

digital sikkerhet både rettet mot offentlig sektor som helhet og spesifikt mot helse og omsorgssektoren, tilsynsrapporter om informasjonssikkerhet og personvern rettet mot kommuner og diverse IKT-sikkerhetsrapporter både rettet mot offentlig sektor og næringslivet. Enkelte dokumenter har blitt valgt ut etter innspill fra representanter i Digdir, tips fra informanter og egen søkeprosess. Etter hvert som vi systematisk har gjennomgått ulike dokumenter, har vi opplevd at det henvises til andre relevante dokumenter som også har blitt tatt med i analysen. Vi har derfor endt med å genere et betydelig datamateriale.

De ulike dokumentene har blitt brukt til ulike formål og i forskjellige deler av studien. Digitaliseringsstrategiene har blant annet blitt brukt for å bygge opp en forståelse og gi en beskrivelse av digitaliseringstrenden og prioriteringsområder i offentlig sektor. Strategier for digital sikkerhet og tilsynsrapporter har blitt brukt for å kunne si noe om dagens sikkerhetstilstand, hva utfordringene har vært og ønsket utvikling fremover. Det var i digitaliseringsstrategiene og strategiene for digital sikkerhet vi oppdaget at bruk av digitale fellesløsninger var et interessant tema for undersøkelsen. Tilsynsrapportene har gitt oss verdifull innsikt i hva som forventes av kommunene i relasjon til informasjonssikkerhet, samt hvilke utfordringer kommunene har hatt i arbeidet med å ivareta god informasjonssikkerhet. Disse dokumentene har både blitt brukt i empiridelen av undersøkelsen og som utgangspunkt for intervjuspørsmålene våre. IKT-sikkerhetsrapportene er utarbeidet av offentlige myndigheter og ekspertorganer som NSM og NORSIS, og sier noe om utviklingen av trusselbildet, sårbarheter og behov i offentlig og kommunal sektor. I noen tilfeller har vi brukt flere versjoner (årganger) av disse dokumentene ettersom de har årlige variasjoner i tematikk. Disse dokumentene har hovedsakelig blitt brukt for å skrive ut empiri relatert til sikkerhetsutfordringer, sårbarheter og andre utfordringer relatert til digitalisering. IKT-sikkerhetsrapportene har også vært verdifulle med tanke på utarbeidelsen av spørsmål til intervjuene med informanter i kommunene.

Vi har analysert dokumentene ved å først skaffe oversikt over relevante dokumenter for deretter å gjøre en tematisk gjennomgang med utgangspunkt i forskningsspørsmålene. Vi fortsatte med å lese oss opp på undertemaer som vi sammenlignet på tvers av rapportene slik at vi fikk oversikt over hva de ulike rapportene skrev om temaene vi var interessert i. Rent praktisk utførte vi denne prosessen ved å lage undertemaer ut fra forskningsspørsmålene, skrev ut rapportene og leste gjennom dem, og markerte ut informasjon relatert til undertemaene med markeringstusj i ulike farger basert hvilke temaer de passet til. Dette har

gjort det mulig å trekke ut gode data om trender, trusler, sårbarheter og utfordringer som bekreftes i flere ulike, uavhengige og troverdige kilder. Likevel påpeker Halvorsen (2008) at valget av dokumenter og tekster kan være forutinntatt og selektivt, altså påvirket av forskerens subjektivitet, og at det derfor er viktig å klargjøre hvilke kriterier som har ligget til grunn for utvalget. Vi har valgt å benytte datagenerering i tillegg til datainnsamling, hvor dataene som genereres vil ses i sammenheng med hva som kommer frem i de skriftlige dokumentene vi har valgt ut, og derfor kunne moderere vår subjektive påvirkning på datamaterialet.

4.3 Datagenerering

Primærdata kan beskrives som datamateriale som er samlet inn av forskeren selv for å besvare spesifikke forskningsspørsmål (Blaikie & Priest, 2019). Vår innsamling av primærdata er hovedsakelig basert på gjennomføring av intervjusamtaler med personer som kunne bidra med data relevant for å besvare studiens problemstilling og forskningsspørsmål. Valget om å kombinere dokumentanalyse med intervjuer har vært hensiktsmessig av flere grunner. For det første har data- og kunnskapsgrunnlaget i flere av de studerte dokumentene som inngår i vår dokumentanalyse primært vært basert på spørreundersøkelser, dokumentanalyser og statistikk. Intervjuene gav oss dermed en unik mulighet til å bygge videre på det eksisterende kunnskapsgrunnlaget fra disse undersøkelsene ved at vi gjennom oppfølgingsspørsmål kunne videreutvikle og utfylle de observasjonene som allerede var gjort. Tjora (2012) mener datagenerering fremfor datainnsamling kan være nødvendig i de tilfeller data ikke «finnes», men må konstrueres i forskningen. Intervju har også vært nødvendig i denne undersøkelsen på bakgrunn av at undersøkelsens problemstilling dekker områder rundt det kommunale digitaliseringsarbeidet som i liten grad har vært et sentralt fokusområde i de studerte dokumentene. Samtalene med studiens informanter muliggjorde dermed for at vi kunne uthente nye data som i liten grad har blitt fremhevet i disse dokumentene. At deler av studien i større grad er avgrenset mot kommunenes risikostyrende aktiviteter for å forebygge og håndtere utilsiktede hendelser i forbindelse med digitale fellesløsninger fremmet også behovet for å utføre intervjuer. Sistnevnte henger sammen med at eksisterende publikasjoner og tilstandsrapporter som tar for seg det digitale situasjonsbildet for kommunesektoren i større grad er rettet mot cyber- og security-relaterte hendelser. Mangelen på empiriske dokumenter som i større grad rettet seg mot utilsiktede hendelser synliggjorde dermed behovet for at informanter ble kontaktet med den hensikt om å innhente mer fyldig og omfattende informasjon for å belyse studiens avgrensede fokusområde.

Informantutvalg

På bakgrunn av at studiens formål er avgrenset til å omhandle kommuners informasjonssikkerhetsarbeid i forbindelse med digitale fellesløsninger var det nødvendig at informantene vi intervjuet kunne bidra med inngående relevant informasjon for studien. Etter hvert som vi fikk økt bakgrunnskunnskap relatert til kommunenes arbeid med informasjonssikkerhet gjennom vår dokumentinnsamling, startet vi arbeidet med å kontakte potensielle intervjukandidater via e-post. I den forbindelse ble det gjort et strategisk utvalg av informanter ved at vi kontaktet deltakere vi mente å innehar kvalifikasjoner og roller som var strategiske i forhold til undersøkelses teoretiske perspektiver og problemstilling (Thagaard, 2013). Etter en gjennomgang av de respektive kommunenes kontaktlister ble deltakere valgt på bakgrunn av sin tilhørende avdeling, samt rollen personene innehadde i disse avdelingene. Til tross for at det overordnende ansvaret for informasjonssikkerheten hviler på virksomhetsleder, valgte vi å kontakte personer som innehar ulike støttefunksjoner og ansvarsområder i kommunenes informasjonssikkerhetsarbeid fremfor virksomhetsledere. Dette henger sammen med at det tidligere har blitt observert variasjoner omkring hvordan ledere og fagansvarlige responderer på spørsmål om virksomhetens informasjonssikkerhetsarbeid. Sistnevnte er et poeng som fremheves i Difi (2018) sin undersøkelse i statsforvaltninger, hvor det har blitt observert at ledere virker å uttrykke seg langt mer optimistiske på spørsmål sammenlignet med fagansvarlige på området. I den innledende mailkorrespondansen var vi opptatt av å redegjøre for studiens formål og fokusområder slik at vi kunne forsikre oss om at kandidatene som ble kontaktet eventuelt kunne sette oss i kontakt med andre personer i kommuneorganisasjonen som hadde bedre forutsetninger til å bidra med informasjon vi kunne nyttiggjøre oss av.

Etter hvert som både problemstilling og forskningsspørsmål endret seg var vi opptatt av å ha en åpen dialog med de respektive kontaktpersonene slik at disse kunne vurdere hvorvidt de på bakgrunn av endringene kunne bidra med nøkkelinformasjonen vi var ute etter. Sistnevnte medførte at vi i noen tilfeller fikk tildelt nye kontaktpersoner i forkant av intervjuene ettersom at disse hadde bedre forutsetninger for å besvare spørsmålene vi var interessert i. Informantene kan derfor sies å ha likhetstrekk med det Andersen (2006) omtaler som nøkkelinformanter, ettersom at disse er ressurssterke personer i noen av landets kommuner som kan bidra med informasjon om det fenomenet vi er interessert i å undersøke. I vårt tilfelle består disse nøkkelinformantene av personer som i sin respektive kommune besitter posisjoner der dem til daglig har arbeidsoppgaver i tilknytning til digitalisering og styring og

kontroll på informasjonssikkerhetsområdet. Videre har disse som medlemmer av Digi Rogaland kjennskap til det interkommunale samarbeidet i regionen så vel som implementeringen og ivaretakelsen av sikkerheten i tilknytning til digitale fellesløsninger. Det blir tatt i bruk koder når intervjusitater fra de ulike informantene trekkes frem i kapittel fem og seks. For å differensiere mellom de ulike kommunene og informantene har vi valgt å bruke koder som eksempelvis «I-1 og I-2». En nærmere oversikt over studiens informanter illustreres i tabell 3, vedlegg 2.

Intervjusituasjon og intervjuguide

Vi har gjennomført totalt seks intervjuer med fem informanter i denne studien. Et intervju kan utformes på ulike måter, og vi valgte en semistrukturert tilnærming. Vi hadde derfor utarbeidet en intervjuguide på forhånd som var veiledende for samtalene. Fordelen med semistrukturerte intervjuer er at til tross for at temaer og spørsmål relatert til problemstillingen er bestemt i forkant, gir intervjuformen både forskerne og informantene frihet til å kunne stille oppfølgingsspørsmål, samt styre samtalen i retning av nye temaer som kommer frem i intervjusituasjonen (Thagaard, 2013). Sistnevnte bidro dermed til at interessante opplysninger og refleksjoner fra et intervju kunne brukes til å utforme spørsmålene i senere intervjuer. Informantene hadde noe ulik kompetanse og erfaring som påvirket deres forutsetninger til å besvare intervjuspørsmålene, dette gjorde at vi ved et tilfelle også valgte å gjennomføre et oppfølgningsintervju med en av informantene. Samtlige intervjuer ble gjennomført via den digitale plattformen *Teams* ettersom koronasituasjonen gjorde at vi ikke kunne gjennomføre intervjuene ved fysisk oppmøte. Med unntak av to intervjuer hadde intervjuene en varighet på omkring 60 minutter. Oppfølgingsintervjuet hadde en likeledes varighet. Det kan tenkes at variasjon i intervjulengde ble påvirket av forhold som den enkeltes erfaring og kompetanse når det gjaldt spørsmål som ble stilt. Videre kan den enkeltes interesse og engasjement for temaene ha hatt en innvirkning på selve intervjuvarigheten. Der den ene informanten eksempelvis etterspurte å fortsette intervjuet en annen dag, startet en annen informant dialogen med å opplyse om at vedkommende hadde begrenset med tid, og det var derfor viktig med en rask gjennomgang.

Til tross for at intervjuene ble gjennomført digitalt, opplevde vi dialogen med informantene som svært god. Foruten et enkelt tilfelle sitter vi igjen med et inntrykk av at vi fikk til en god diskusjon med våre informanter, uten at informantene ble avbrutt av ytre faktorer. Ved et tilfelle ble derimot den ene informanten oppringt på telefonen mens vedkommende var i ferd

med å besvare et spørsmål. Vi opplevde at oppringningen forstyrret informantens resonnement rundt et sentralt poeng, og at informanten fikk utfordringer med å komme tilbake til poenget i ettertid. Til tross for dette mener vi dialogen ble positivt forsterket av at vi benyttet en taleopptaker, slik at vi begge kunne aktivt delta i samtalen og stille oppfølgingsspørsmål fremfor at fokuset var på å ta notater underveis. Generelt sett kan det tenkes at bruk av taleopptaker under intervjuer kan påvirke informantenes villighet til å uttale seg kritisk om egen kommune og ledelse. Likevel opplevde vi ikke dette som problematisk under intervjuene ettersom vi på forhånd hadde garantert for informantenes anonymitet. Selve intervjuguiden med oversikt over temaer og spørsmål som ble stilt under intervjuene ligger som vedlegg 3.

Koding og kategorisering av intervjudata

Etter å ha gjennomført intervjuene startet vi fortløpende med å transkribere samtalene slik at vi kunne begynne med selve analysen av intervjudataene. Etter transkriberingen satt vi igjen med omlag 80 sider transkribert intervjudata. I arbeidet med koding og kategorisering benyttet vi oss av kategorier vi hadde laget oss med utgangspunkt i forkunnskapene vi hadde innhentet fra dokumentanalysen, i tillegg til kategorier vi mente var relevante for å belyse det teoretiske rammeverket. Til tross for at vi hadde laget oss kategorier i forkant opplevde vi at intervjudataen ga oss interessante funn utover det som kom frem i dokumentene. Kategoriseringen bar derfor preg av en kombinasjon mellom dokumenter, teori og intervjudataen. Kategoriene vi har brukt kan dermed sies å representere temaer som har en referanse til problemstillingen, i tillegg til temaer vi har utviklet i løpet av analysen. Selve prosessen foregikk slik at vi gikk gjennom hvert enkelt ferdigtranskriberte intervju og plasserte sitater/poenger inn i en tabell med kategorier og koder. Kodene ble brukt til å uttrykke meningsinnholdet i teksten der selve kategoriseringsprosessen innebar å plassere data som var kodet inn i passende kategorier. Vi endte opp med 6 ulike tabeller med kodet og kategorisert data, disse hadde samme form men noe variert innhold avhengig av hva som kom frem under intervjuene. Analyse av intervjudata kan i prinsippet ikke skilles fra tolkning (Thagaard, 2013). Måten vi har valgt å inndele og klassifisere intervjudataen på kan dermed først og fremst forstås som å reflekterer den forståelsen vi har utviklet i forhold til dataen.

4.4 Kvalitetskriterier

Validitet

I en samfunnsvitenskapelig sammenheng brukes begrepet validitet for å vurdere i hvilken grad metoden som har blitt benyttet er egnet til å undersøke det den skal undersøke (Dalland, 2020). Gjennomføringen av denne undersøkelsen kan best beskrives som en fleksibel prosess hvor vi kontinuerlig har gjort endringer og justeringer etter hvert som vi har fått mer kunnskap om temaet. Etter å ha lest gjennom et stort antall skriftlige dokumenter samt gjennomført et videomøte med representanter fra digitaliseringsdirektoratet besluttet vi å undersøke hvordan digitale fellesløsninger påvirker informasjonssikkerhetsarbeidet i kommunene. Etter å ha gjort denne avgrensningen ble det enklere å plukke ut de mest relevante skriftlige dokumentene. For å øke validiteten av undersøkelsen gjennomførte vi en ny søkeprosess, og fant en rekke nye rapporter om digitale trusler og sårbarhet, samt tilsynsrapporter og veiledere på informasjonssikkerhetsområdet som ble benyttet for å utforme ny problemstilling og FS. Arbeidet med problemstilling og FS i denne undersøkelsen kan best beskrives som en runddans, hvor endringer har forekommet etter hvert som vi har fått mer kunnskap om temaet.

For å ivareta kravet om validitet ble funn i datamaterialet samt innspill fra digitaliseringsdirektoratet benyttet som utgangspunkt for utformingen av spørsmål til intervjuguiden. Ved å bruke en abduktiv tilnærming i kombinasjon med semistrukturerte intervjuer fikk vi mulighet til å justere intervjuspørsmålene etter hvert som vi fikk testet disse ut i en intervjusetting. På denne måten fikk vi fjernet irrelevante spørsmål, reformulert uklare og utformet nye spørsmål basert på funn i tidligere intervjuer. Intervjusituasjonen tillot også at vi under hele prosessen kunne stille oppfølgingsspørsmål når vi var usikre på hva informantene mente, noe som gjorde at vi fikk kvalitetssikret at informantene forstod spørsmålene på samme måte som var tiltenkt når vi utarbeidet dem. På denne måten sørget vi for at dataen vi samlet inn var relevant for å besvare problemstilling og forskningsspørsmål. Ved bruk av intervju dannet vi oss også en relasjon til informantene, noe som var nyttig ettersom vi kunne kontakte informantene på nytt for oppklaring og eventuelle oppfølgingsspørsmål i etterkant av intervjuene.

Reliabilitet

Reliabilitet ses i sammenheng med begrepene pålitelighet og troverdighet og omhandler forskningsresultatenes konsistens og troverdighet (Dalland, 2020). I denne undersøkelsen har vi lest gjennom, og hentet ut, data fra en rekke skriftlige dokumenter samt foretatt intervjuer med informanter i flere kommuner. Det er flere faktorer som kan påvirke dette prosjektets reliabilitet, blant annet har vi brukt noen dokumenter som ikke spesifikt er rettet mot kommunal sektor. Det kan derfor stilles spørsmål ved om bruk av disse dokumentene kan representere potensielle feilkilder. For å redusere sannsynligheten for feilkilder i det skriftlige datamaterialet tok vi kontakt med utenforstående aktører med kunnskap innenfor området, blant annet gjennomførte vi et videomøte med digitaliseringsdirektoratet hvor vi fikk mye god informasjon om interessante vinklinger som ville være relevante for kommunesektoren. På en annen side understrekte aktørene fra Digdir, som også var medforfattere i flere av undersøkelsene, at funn fra både statsforvaltningen og fylkeskommuner også var relevante utfordringer for kommunene. Vi har også gjennomført intervjuer med personer som har mye erfaring og fagkunnskap om temaet vi studerer, denne dataen ble sett i sammenheng med hva som kom frem i dokumentene. Selv om det foreligger lite forskning på bruk av digitale fellesløsninger har vi også brukt funn fra kapittelet om tidligere forskning for å støtte opp om egne funn der hvor dette har vært relevant. En annen faktor som kan påvirke undersøkelsens reliabilitet er at alle intervjuer har blitt gjennomført som videomøter på grunn av covid-19 pandemien. Når man gjennomfører intervjuer som videosamtaler vil man ikke ha samme mulighet til å fange opp sentrale elementer som informantenes kroppsspråk, noe som kan påvirke studiens reliabilitet. Relasjonen mellom informanter og forskere kan også bli påvirket av at man ikke møtes personlig. For å redusere mulighetene for feilkilder i intervjusituasjonen tok vi opp samtalene med båndopptaker, noe som ga oss muligheten til å gå gjennom intervjuene flere ganger for å gjøre tolkningen av dataen enklere. I tillegg har også alle informantene fått mulighet til å lese gjennom det bearbeidede datamaterialet, og gi tilbakemeldinger, slik at mulige feiltolkninger eller feilsiteringer har blitt rettet.

Overførbarhet

Thagaard (2013) knytter begrepet overførbarhet til vurderinger om hvorvidt funn og tolkninger fra en enkelt undersøkelse, kan overføres til å også gjelde i andre sammenhenger. Vi har valgt å bruke case-studier som innebærer at man har få undersøkelsesenheter i kombinasjon med kvalitativ metode som egner seg best for å oppnå en god dybdeforståelse, og som tar for seg mange ulike variabler. Utvalget vårt av informanter har heller ikke blitt

valgt på bakgrunn av noen målsetning om representativitet, men heller for å generere best mulig data for å besvare problemstillingen. Disse valgene får konsekvenser for overførbarheten til studien vår. Det at vi har få undersøkelsesenheter, et ikke-representativt utvalg og et kvalitativt datamateriale som ikke egner seg for statistiske mål, og som blir påvirket av vår subjektivitet (tolkning og utvelgelse) gjør at overførbarheten av studien vår er begrenset. Likevel har formålet vårt vært å gi en beskrivelse av de typiske sikkerhetsutfordringene kommunene står ovenfor i forbindelse med bruk av digitale fellesløsninger. Kommunene har uavhengig av størrelse og geografisk plassering stort sett de samme lovpålagte oppgavene, og det er derfor sannsynlig at mange av de lokale momentene og utfordringene som kommer frem i denne undersøkelsen også er gjeldene for andre kommuner utover de som har deltatt i undersøkelsen.

4.5 Etiske refleksjoner

Dalland (2020) skriver at etiske vurderinger går utover å bare følge regler, noe som innebærer at man må tenke gjennom hvilke etiske utfordringer prosjektet man jobber med kan føre med seg. Dette gjelder også for vår oppgave, hvor de største etiske utfordringene kan ses i sammenheng med innsamling og håndtering av data som kan være identifiserende. Dette begrunnes ut ifra at noen av spørsmålene i intervjuguiden la opp til at informantene kunne komme med kritiske bemerkninger om ledere og egen organisasjon for øvrig. Samtidig garanterte vi for anonymitet i informasjonsskrivet informantene fikk tilsendt sammen med forespørsel om deltakelse. Det er ofte enkeltpersoner som er i besittelse av den informasjonen man trenger i en forskningssammenheng, og derfor er ifølge Dalland (2020) tillitt et nøkkelord i denne sammenheng. Vi har gjennom hele prosjektet forsøkt å ivareta den tilliten informantene har vist oss ved å være villige til å bruke sin egen tid og kunnskap på å hjelpe oss med denne studien. En forutsetning for å få godkjenning til å samle inn og behandle data av NSD er å sende inn en søknad hvor vi redegjør for databehandlingen og personvern. Vi opplevde søknadsprosessen hos NSD som veldig nyttig, ettersom vi fikk laget en gjennomtenkt plan for hvordan dataene kunne bli lagret og håndtert for å ivareta personvernet til informantene våre. Etter å ha fått søknaden om datainnsamling godkjent hos NSD jobbet vi med å utforme et informasjonsskriv hvor vi redegjorde for både prosjektet, hva deltakelse ville innebære, samt hvilke rettigheter man har som informant. På bakgrunn av dette informasjonsskrivet kunne informantene gi et informert og frivillig samtykke til å delta i forskningsprosjektet.

Metodiske styrker og svakheter

Den kvalitative metoden har sine kjente styrker og svakheter. Den kvalitative metoden har sin styrke i å produsere et rikt datamateriale som gjør det mulig å gå i dybden på fenomenet man studerer (Halvorsen, 2008). Dette har vært en styrke i vår undersøkelse ettersom det foreligger lite forskning på bruk av digitale fellesløsninger og påvirkningen dette har på kommuners arbeid med å ivareta informasjonssikkerheten. Valget falt derfor på å benytte oss av kvalitativ metode i denne undersøkelsen, ettersom kvantitative undersøkelser forutsetter at man på forhånd har en god forståelse av fenomenet man studerer.

Dokumentstudiet har på mange måter fungert som et fundament for undersøkelsen, og dannet grunnlaget for intervjuene vi har gjennomført. Innsamling av intervjudata fra informanter med bred kjennskap og ekspertise innenfor feltet har bidratt til å styrke studien. Funn fra dokumentene har blitt tema under intervjuene, hvor informantene har hatt mulighet til å supplere med egne erfaringer, observasjoner og refleksjoner. En svakhet med denne undersøkelsen er at utvalget av informanter har vært lite, og vi har ikke tatt for oss de mindre kommunene. Dette kan være en svakhet ettersom mindre kommuner kan ha noen særegne utfordringer og erfaringer som ikke har blitt innhentet eller vurdert i denne studien. VFårt fokus har vært på mellomstore og store kommuner fordi disse i mange tilfeller har kommet lengre i digitaliseringsarbeidet. En kvantitativ undersøkelse ville også hatt bedre forutsetninger for å undersøke utbredelsen og sammenhengen mellom variabler i ett bredere og mer representativt utvalg, men dette har som tidligere nevnt ikke blitt vurdert ettersom kunnskapen på området per nå er begrenset.

5.0 Empiri

I dette kapitelet presenteres empiriske funn som har blitt hentet ut fra 24 dokumenter og våre gjennomførte intervjuer som tidligere er beskrevet i kapittel 4. Funnene som presenteres i dette kapitelet vil bidra til å besvare problemstillingen:

«*Hvordan endrer bruk av digitale fellesløsninger kommunenes arbeid med informasjonssikkerhet i egen virksomhet?»*

Kapittelet er strukturert i fire hoveddeler der ett av kapitlene (5.1) tar for seg temaer som er relevante for å besvare problemstillingen, men som ikke kommer naturlig under forskningsspørsmålene, de tre resterende kapitlene vil være strukturert etter forskningsspørsmålene med tilhørende undertemaer. Det er også verdt å nevne at noen av funnene overlapper og er tett sammenknyttet, noen av utfordringene kan for eksempel være relevante innenfor både organisering og risikostyring.

5.1 Digitale fellestjenester, felleskomponenter og utilsiktede hendelser

Digitale fellesløsninger

Begrepsbruken rundt fellesløsninger er noe uklar og inkonsekvent mellom ulike aktører. Her anser vi begrepet «digitale fellesløsninger» som en samlebetegnelse på det noen aktører omtaler som henholdsvis «fellestjenester/løsninger» og «felleskomponenter» I dette avsnittet redegjøres det for innholdet i begrepet digitale fellesløsninger.

Digi helse er et eksempel på et nasjonalt prosjekt som det arbeides med
i Digi Rogaland. Digi helse er en digital løsning hvor man kan administrere avtaler og kommunisere med kommunens helsetilbud. Digi Helse gir innbyggerne mulighet til å sende og motta meldinger digitalt fra helse og omsorgstjenesten, man har oversikt over, og kan avbestille hjemmebesøk og man kan få varsler på sms eller e-post om utførte hjemmebesøk (Kommunesektorens organisasjon, 2018b). De forventede gevinstene ved bruk av digi helse handler blant annet om at man reduserer kostnader knyttet til bomturer ved hjemmebesøk og telefonsamtaler inn til tjenestetilbyder. I tillegg vil bruk av Digi Helse kunne bidra til et bedre samarbeid og mer effektiv kommunikasjon mellom helsepersonell og pårørende (Direktoratet for e-helse, 2020a) Ett annet eksempel på en digital fellesløsning er DigiSos-prosjektet i Digi Rogaland som er en digital sosialtjeneste, hvor formålet er at man skal kunne levere søknad om økonomisk sosialhjelp digitalt. DigiSos-ordningen er et samarbeid mellom staten og

kommuner om å gjøre skillet mellom forvaltningsnivåene usynlig for innbyggerne. Dette betyr at brukerne slipper å oppgi den samme typen informasjon mer enn en gang (Digi Rogaland, u.å-a).

En felleskomponent kan beskrives som en byggekloss som ulike offentlige virksomheter kan bruke i utviklingen av sine egne tjenester. Disse løsningene blir kun utviklet en gang, deretter kan mange forskjellige aktører ta dem i bruk. Det er de mest sentrale fellesløsningene som blir omtalt som nasjonale felleskomponenter (Digitaliseringsdirektoratet, u.å-b).
Offentlig sektor har utviklet flere åpne og gjenbrukbare digitale løsninger som dekker mange sentrale behov innenfor digitalisering, dette gjelder blant annet løsninger for innlogging, autentisering eller registre. Felleskomponentene skal legge til rette for at virksomhetene kan bruke tid og ressurser på egne faglige utfordringer i stedet for at alle virksomheter skal utvikle egne løsninger eller funksjonaliteter som andre etater allerede har utviklet (Kommunal- og moderniseringsdepartementet, 2014b). De nasjonale felleskomponentene kan derfor bidra til å heve kvaliteten på tjenestene samtidig som man reduserer ressursbruken ved etablering og drift av de digitale tjenestene. De digitale felleskomponentene skal også gjøre det lettere å tilby enhetlige tjenester i forvaltningen på tvers av sektorer. Et eksempel kan være ID-porten som gjør det mulig å standardisere innloggingsfunksjonaliteten slik at denne er den samme uavhengig av hvilken etat eller kommune man logger inn hos (Kommunal- og moderniseringsdepartementet, 2014b). Det finnes per i dag 7 nasjonale felleskomponenter bestående av Altinn, ID-porten, digital postkasse for innbyggere, kontakt og reservasjonsregisteret, folkeregisteret, matrikkelen og enhetsregisteret (Kommunal- og moderniseringsdepartementet, 2019). Foruten de nasjonale felleskomponentene har eksempelvis KS etablert KS svarUT og KS læring som fellesløsninger for kommunal sektor (Kommunesektorens organisasjon, 2018a).

Mange av de digitale tjenestene kommuner tilbyr er relativt like, digitalisering av tjenester har derfor et potensiale for gjenbruk. For å kunne utnytte mulighetene for gjenbruk forutsettes det at kommunene er samordnet på digitaliseringsområdet, i tillegg må også den digitale samhandlingen mellom stat og kommuner styrkes. Samordning handler i denne sammenheng om at kommuner tar i bruk kommunale og nasjonale fellesløsninger i digitaliseringen og bidrar i utvikling av nye fellesløsninger der hvor det er behov (Kommunesektorens organisasjon, 2017). Offentlig sektor har et stort behov for å redusere kostnader og hente ut

gevinstpotensialet som ligger i digitalisering, bruk av fellesløsninger er viktig i denne sammenheng (Kommunal- og moderniseringsdepartementet, 2019).

Ifølge NSM (2017b) er etablering av en felles infrastruktur for samhandling og kobling av data et viktig innsatsområde. NSM argumenterer for at det er ønskelig med færre IKT-miljøer i offentlig sektor. De ønsker større og mer robuste kompetansemiljøer som kan bidra til stordriftsfordeler og mer kostnadseffektive løsninger på sikkerhetsområdet. Store IKT-miljøer vil kunne både tiltrekke, utvikle og bygge opp sikkerhetskompetanse i større grad enn hva små og spredte miljøer kan. Felles IKT-løsninger vil bedre sikkerheten i behandlingen av sensitiv informasjon sammenlignet med å ha flere små og spredte systemer. Felles IKT-løsninger vil kunne bidra til en reduksjon i sårbarhet fordi de bidrar til å redusere variasjoner på nettverk, tjenester og systemer, noe som reduserer kompleksiteten i IKT-systemene (Nasjonal sikkerhetsmyndighet, 2017b). I Nasjonal Sikkerhetsmyndighet (2021) er en målsetning at en tjeneste eller applikasjon som utvikles av en virksomhet skal kunne gjenbrukes av andre virksomheter som har samme behov.

Utilsiktede hendelser som kan påvirke informasjonssikkerheten i IKT-systemer

Digitale systemer utsettes kontinuerlig for uønskede hendelser der disse kan ha både tilsiktet og utilsiktet karakter. Det er utilsiktede hendelser som utgjør majoriteten av uønskede hendelser i IKT-systemer (NOU 2018: 14, 2018).

En rekke ulike værfenomener kan ramme IKT-systemer og føre til uønskede hendelser. Stormer, skred, brann og flom er de vanligste værfenomenene som forårsaker problematikk i Norge (NOU 2015: 13, 2015). Sterk vind kan forårsake trefall over høyspentlinjer, skred kan ødelegge kabler både under og over bakkenivå, branner og flom kan ødelegge utstyr og systemer som drifter strømforsyning eller ramme selve IKT-systemene selv. I 2016 inntraff tre ekstremværhendelser som skadet infrastruktur og resulterte i utfall av elektronisk kommunikasjon (NOU 2018: 14, 2018). En av informantene nevnte at «*strømbrudd er aktuelt, og selv om vi ikke har hatt strømbrudd som har slått ut systemene i alt for lang tid, så har det vært strømbrudd i området som har vart i rundt ett døgn*» (I-3).

Menneskelige feil kan oppstå av flere ulike årsaker og kan forårsake uønskede IKT-hendelser som påvirker informasjonssikkerheten i virksomheter. Ofte har mennesker gode intensjoner, men gjør allikevel feil. Ansatte kan sende dokumenter med sensitiv informasjon til feil

mottakere, fiberkabler kan bli gravd over og kuttet av, og oppgraderinger av IKT-systemer kan feile og sette systemer ut av spill (NOU 2015: 13, 2015). Flere av informantene nevner eksempler på dette. En av informantene uttaler: «*Vi hadde for ca. 6 måneder siden en hendelse i forbindelse med noe gravearbeid på Rennesøy hvor linjer med fiberkabler ble revet av, noe som førte til at vår forbindelse med norsk helsenett gikk ned, og var nede i 2 døgn»* (I-1).

En annen informant nevner at menneskelige feil blir vurdert som en av de største risikoene i hver eneste ROS-analyse som gjennomføres, og uttaler: *«Frem til nå har vi hatt veldig mange fellesbrukere for innlogging på felles PCer, hvor det alltid har vært veldig lett å bare gå fra PCen. Når du da i tillegg har glemt å logge av pasientjournalsystemet vil neste mann som kommer inn og journalfører noe gjør dette på noen andres navn.»* (I-3).

Informant (I-4) nevner i forbindelse med oppdateringer/endringer av systemer at: «*Ofte så er det når vi gjør en endring at det skjer ett eller annet som vi ikke hadde tenkt på, konsekvensen kan kanskje være større for andre type hendelser, men dette skjer jo hele tiden. Jo større prosjektet eller løsningen er, jo lengre tid tar det å fikse den type problem»* (I-4).

Lav brukervennlighet, manglende sikkerhetskunnskap, kompliserte rutiner og manglende forståelse for hvordan IT-systemene fungerer er eksempler på årsaker som alene, eller i kombinasjon kan føre til menneskelig svikt. En utfordring som trekkes frem er at mindre enn halvparten av norske virksomheter gir nyansatte opplæring i IT-systemer og sikkerhetsrutiner, og bare rundt en femtedel får opplæring senere i ansettelsesforholdet (NOU 2015: 13, 2015). De ansattes holdninger til sikkerhetsarbeidet og sikkerhetskulturen i virksomheten for øvrig er andre faktorer som påvirker sikkerheten i virksomheter. Konflikter mellom sikkerhet og andre mål og prioriteringer kan bidra til feil og svikt. Denne målkonflikten bekreftes av informant (I-2) som uttaler:

«Hovedtyngden av våre ansatte er mest opptatt av å gi våre tjenestemottakere en forsvarlig tjeneste. Så kommer dette med journalføring og bruk av digitale verktøy som noe ekstra man må forholde seg til. I en allerede presset hverdag er det derfor fort gjort å gå inn å dokumentere på feil brukere» (I-2).

Ansatte kan videre komme i situasjoner hvor de må velge mellom å følge sikkerhetsrutiner eller få gjort ferdig arbeidsoppgaver innenfor tidsfrister. I andre tilfeller kan sikkerhetsrutinene være vanskelige å følge i praksis. Sikkerhetsrutinene kan gjerne innebære å følge strenge retningslinjer som er tungvinte eller upraktiske for de ansatte å etterleve (NOU 2015: 13, 2015). *Organisatorisk svikt* kan skyldes manglende kunnskap om informasjonssikkerhet i virksomheter og manglende oversikt over egne verdier. Under halvparten av virksomheter gjør verdivurderinger av informasjonen de besitter. En viktig årsak til at informasjon kommer på avveie skyldes slurv i virksomhetene, for eksempel ved at programvare er utdatert som følge av manglende sikkerhetsoppdateringer (NOU 2015: 13, 2015). Informant (I-3) tar opp problemstillingen knyttet til å holde systemene oppdatert:

«Det er et stadig oppdateringsjag på systemene, og hvis du ikke følger med så ligger du langt bak i versjonene. Når vi skulle ta i bruk digisos så var det det noen forutsetninger som skulle være på plass, som eksempelvis et digitalt arkiv i sikker sone. Selve kostnaden av å gjøre disse endringene kan medføre etterslep i oppdateringene» (I-3).

Systemsvikt starter ofte på grunn av enkeltkomponenter som svikter som følge av overbelastning. Elektronikk kan eksempelvis kortslutte og ta fyr, harddisker kan svikte, og logiske feil i programkoder kan resultere i systemfeil (NOU 2015: 13, 2015). Systemsvikt kan bli særlig alvorlig i kombinasjon med menneskelige feil. Et eksempel her kan være at svikt oppstår i en komponent og fører til at viktig informasjon går tapt, i kombinasjon med at rutinene om sikkerhetskopiering ikke er blitt fulgt opp, slik at informasjonen heller ikke kan gjenopprettes. Når sikkerhetsmekanismer enten mangler eller ikke blir etterlevd i stor nok grad kan slike type uønskede hendelser fort kunne påvirke og forplante seg i avhengige eller nærliggende systemer (NOU 2015: 13, 2015).

Oppsummering

Empirien viser at digitale fellesløsninger skal være en sentral bidragsyter for økt effektivitet, reduserte kostnader og bedre samhandling, og er et viktig satsingsområde i kommunesektoren. Man ser også at utilsiktede hendelser er en relevant problemstilling for kommunene, og at disse utgjør en sentral sikkerhetstrussel. Her er særlig menneskelig feil fremhevet som relevante årsaker til hvordan uønskede hendelser kan inntreffe.

5.2 Hvordan fører bruk av digitale fellesløsninger til sikkerhetsutfordringer

Avhengigheter, lange verdikjeder og manglende kompetanse er sikkerhetsfordringer som ikke er unike for bruk av digitale fellesløsninger. Allikevel vil bruk av digitale fellesløsninger kunne aktualisere disse problemstillingene ytterligere fordi fellesløsningene blir utviklet og driftet utenfor kommunene, noe som kan ha implikasjoner for temaer som ansvarsforhold, kunnskap og oppmerksomhet. Gjennom intervjuene våre har vi også blitt gjort oppmerksomme på utfordringer utover det som kommer frem i rapportene vi har samlet inn data fra. Disse vil vi knytte opp mot henholdsvis organisering og risikostyring senere i kapittelet.

Avhengigheter og verdikjeder

I strategi for digital sikkerhet i helse- og omsorgssektoren nevnes komplekse digitale avhengigheter som en utfordring og sårbarhet som har oppstått som følge av økende digitalisering. Digitaliseringen fører til at verdikjedene blir stadig lengre og involverer flere aktører, noe som skaper utfordringer med å holde oversikt og kontroll over hvilke avhengigheter man har, og hvilke konsekvenser som kan oppstå dersom en uønsket hendelse skulle inntreffe. Trenden med lengre og mer komplekse verdikjeder kan også føre til fragmentering av ansvar og uklarheter rundt hvem som er ansvarlig for sikkerheten (Direktoratet for e-helse, 2020b). DSB skriver også i sin rapport om risikostyring i digitale verdikjeder at komplekse systemer fort blir uoversiktlige, hvor det er mange ulike aktører involvert og hvor systemansvaret blir fragmentert (Direktoratet for samfunnssikkerhet og beredskap, 2020). Helse og omsorgssektoren er avhengige av flere understøttende funksjoner for å levere tjenestene sine. Norsk helsenett leverer eksempelvis tjenester og drifter løsninger for store deler av helse- og omsorgssektoren, noe som har muliggjort standardisering av en rekke felles tjenester og sikkerhetsløsninger i sektoren (Direktoratet for e-helse, 2020c). Utfordringen ligger i at helsenettets funksjonalitet er fullstendig avhengig av tredjeparter i ekomsektoren for å fungere, noe som brukere av helsenettet ikke i stor nok grad er klar over, eller tar høyde for når de foretar egne vurderinger. Den økende sammenkoblingen mellom sektorer kan beskrives som et særpreg ved de moderne digitale avhengighetene (Direktoratet for e-helse, 2020b). Informant (I-1) kom med følgende innspill i forbindelse med eksempelet om gravearbeidet på Rennesøy som førte til at flere fiberkabler ble kuttet av og at kommunens forbindelse til norsk helsenett gikk ned *« [...] Det var flere organisasjoner som*

ble påvirket av dette, og vi fikk en ''aha'' opplevelse om hvor sårbart dette er. Det viste seg at organisasjoner mye større enn oss bare har én linje inn til norsk helsenett» (I-1).

NSM skriver i sin årlige risikorapport for 2021 at mange grunnleggende nasjonale funksjoner blir driftet av virksomheter med omfattende og uoversiktlige verdikjeder med avhengigheter på tvers av både sektorer og landegrenser. Den manglende oversikten eller forståelsen av verdikjedene man er en del av, og avhengighetene mellom virksomheter og tjenester på tvers av ulike sektorer utgjør en nasjonal digital sårbarhet (Nasjonal sikkerhetsmyndighet, 2021). Sårbarheten kan forklares ved at avhengigheter til ulike underleverandører gjør at virksomhetene mister kontroll over tjenester eller leveranser som er kritisk for ens egen virksomhets funksjon. Et eksempel på slike avhengigheter er at mange virksomheter er avhengige av at underleverandører leverer elektrisitet, bredbånd, IKT-tjenester eller lignende. Dersom disse underleverandørene av en eller annen årsak ikke klarer å levere disse tjenestene, vil det kunne medføre store konsekvenser for de virksomhetene som er avhengige av dem. Grunnleggende nasjonale funksjoner kan på den måten arve sårbarhetene som ligger i verdikjedene til virksomhetene som drifter dem (Nasjonal sikkerhetsmyndighet, 2021).

I NSMs risikorapport for 2020 beskrives sårbarheten ved digitale verdikjeder som en dominoeffekt. Når systemer i stadig større grad integreres med hverandre, vil en uønsket hendelse som oppstår i ett av disse systemene kunne spre seg, og raskt manifestere seg i andre systemer eller samfunnssektorer som er del av samme verdikjede (Nasjonal sikkerhetsmyndighet, 2020b). Informant (I-4) tar opp problemstillingen knyttet til avhengigheter og tett integrerte systemer og forteller om hvordan fellesløsningene er bygget opp: «*De fleste fellesløsningene fungerer per i dag sånn at de syncer opp mot og ''henter ned'' dataen de er avhengige av fra eksempelvis folkeregisteret og har lokale kopier* (I-4). Videre forteller informanten at noen fellesløsninger er bygget opp etter en mer totalsentralisert modell. Denne fungerer slik at eksempelvis navnet på en person i en fellesløsning er en objekt-id i folkeregisteret, noe som vil si at det er en live-referanse til en spesifikk person i folkeregisteret. Informanten opplyser at utfordringen med slike løsninger er at man ikke ville klart å finne ut av navnet på denne personen dersom folkeregisteret sviktet, fordi folkeregisteret til enhver tid slår opp navnene gjennom objekt-id referansen uten av man har lokale kopier i fellesløsningen. «*Dilemmaet knytter seg til noen av de skikkelig store nasjonale fellesløsningene som felles kommunal journal (og ID-porten som er en live-tjeneste) hvor du legger alle eggene i en kurv, og da er det andre aspekter*» (I-4). Videre

forteller informanten at konsekvensene av mer totalsentraliserte modeller er at man må være ekstremt nøye med utviklingen og forvaltningen av tjenesten, noe som kan hindre fleksibilitet og muligheten til å gjøre endringer raskt: «*Du må være skråsikker fordi konsekvensene kan bli så enormt store, og dette kan igjen skape nye problemer for tjenesteleveransen»* (I-4).

Digitale verdikjeder dannes på bakgrunn av kostnadseffektivitet for virksomhetene, og vil i de fleste tilfeller strekke seg over landegrenser. Digitaliseringen av tjenester utvikler seg ekstremt raskt, noe som gjør at de digitale verdikjedene blir svært dynamiske og kontinuerlig endrer seg. Dette innebærer også at virksomheter arver sårbarhetene til de virksomhetene som ligger tidligere i verdikjeden enn en selv. Kompleksiteten i de digitale verdikjedene gjør det også stadig vanskeligere å holde oversikt over den totale sårbarheten en gitt digital tjeneste står ovenfor (Nasjonal sikkerhetsmyndighet, 2020b). Samtlige informanter anerkjenner avhengigheter og tett koplede digitale verdikjeder som en sentral utfordring for å ivareta informasjonssikkerheten i kommunene. Informant (I-1) uttaler følgende om utfordringene ved digitale verdikjeder:

«*Jeg tenker oppetid er en utfordring, jo flere ledd i verdikjeden jo større sannsynlighet for at et eller annet bryter sammen. Videre er spørsmålet hvorvidt sikkerheten er ivaretatt gjennom hele denne lenken. Sistnevnte er en veldig aktuell problemstilling, og dets mer utfordrende når disse kjedene blir lengre og lengre*» (I-1).

Informant (I-4) knytter utfordringen med digitale verdikjeder opp mot bruk av fellesløsninger og forteller at det hovedsakelig er to aspekter som er utfordrende: «*ID-porten hadde en sikkerhetsglipp i år der folk som logget seg på samtidig fra forskjellige plasser ble feilkoblet, noe som gjorde at du kom inn i en tjeneste for en annen person enn deg selv i et lite tidsrom»* (I-4). Det andre aspektet knytter seg særlig til avhengighetsproblematikk og hvordan feil raskt kan spre seg og få konsekvenser utover den opprinnelige feilen:

«Dersom tjenesten ikke fungerer, vil heller ikke de underliggende tjenestene du skal ha tilgang til fungere. Det er mange positive ting med tanke på sikkerheten når man tar i bruk digitale fellesløsninger, men det er viktige ting å tenke på i forhold til sårbarheten og ''hvor mange egg du legger i en kurv''» (I-4).

Informant (I-3) har en litt annen vinkling og legger mer vekt på den økte avhengigheten kommunene har til en kontinuerlig tilgang på data. Informanten knytter videre dette opp mot hvordan kommunene har fått økt tilgang og bedre kvalitet på dataen som følge av digitaliseringen og de nye løsningene, og at man får en helt ny forståelse for risiko når denne plutselig ikke er tilgjengelig:

«*Tidligere hadde du ikke tilgang til disse dataene. Risikobildet endrer seg etter hvert som flere digitale løsninger tas i bruk. Du blir mer avhengig av å ha løsningene. Før når alt var på penn og papir så hadde du alltid noe å gå tilbake til, men viss e-meldingene ikke fungerer har du plutselig ikke tilgang til viktig informasjon*» (I-3).

DSB skriver at behovet for å danne seg oversikt over de digitale verdikjedene man er en del av, avhenger av kritikaliteten til den tjenesten som understøttes av verdikjeden(e) (Direktoratet for samfunnssikkerhet og beredskap, 2020). Det er ifølge DSB også flere ulike aspekter ved de enkelte verdikjedene som har betydning for tjenestens sårbarhet, men presiserer at man ikke kan analysere disse aspektene med mindre man har skaffet seg oversikt over verdikjedene (Direktoratet for samfunnssikkerhet og beredskap, 2020). Flere av informantene forteller at de ikke fokuserer på å kartlegge egne avhengigheter og verdikjeder. Informant (I-3) uttaler følgende på vårt spørsmål om hvordan kommunen arbeider for å få oversikt over digitale verdikjeder og avhengigheter:

«*Det er ikke noe som har vært i fokus, men jeg ser poenget. Vi er ikke store nok eller har penger nok til å utvikle noe selv og holde styr på ting. Det at vi har fellesløsninger gjør at ting kan håndteres enklere og mer sentralt slik at man får bedre kontroll på sikkerheten. Men det er jo risiko med det også, det at verdikjedene blir lengre, men det har egentlig ikke vært et tema hos oss*» (I-3).

På oppfølgingsspørsmål om hvorfor det ikke fokuseres på å kartlegge egne digitale verdikjeder og avhengigheter utdyper informanten:

«Det er jo der det kanskje er litt forskjell på kommunene, en større kommune vil ha en større stab og andre typer folk og kompetanse til å se på dette her. Det er jo en grunn til at vi kjøper tjenester, fordi at andre skal ha den kompetansen» (I-3).

En av årsakene til at virksomheter burde se nytten av å skaffe seg oversikt og forståelse av egne verdikjeder handler om muligheten for å avdekke det som omtales som falsk eller svekket redundans. Dette begrepet handler om tilsynelatende redundante løsninger som viser seg å egentlig inneha samme type sårbarheter utover i verdikjeden. Det kan eksempelvis være at alle redundansløsningene på et punkt er koblet til samme tjeneste eller løsning som de er avhengige av for å fungere, og dersom denne svikter vil også alle redundansløsningene kunne svikte samtidig (Direktoratet for samfunnssikkerhet og beredskap, 2020). Et annet viktig poeng er at avhengigheter kan ha varierende kritikalitet, man kan være avhengig, men ha muligheter for redundans, og man kan være absolutt avhengig uten gode muligheter for redundans. Man er derfor avhengig av god oversikt og forståelse av egne verdikjeder, slik at også alvorligheten eller kritikaliteten av avhengighetene kan analyseres (Direktoratet for samfunnssikkerhet og beredskap, 2020). Til slutt vil også sikkerhetsmål påvirke hvordan man analyserer verdikjedene. Dersom sikkerhetsmålet handler om å ivareta dataens tilgjengelighet vil redundans være et gode, men dersom hovedformålet er å ivareta dataens konfidensialitet kan redundans representere en ytterliggere sårbarhet, ettersom antall potensielle angrepsflater økes (Direktoratet for samfunnssikkerhet og beredskap, 2020).

Manglende digital kompetanse

Digitaliseringsstrategien som er utarbeidet av KS for kommunal sektor for perioden 2017-2020 peker på behovet for at medarbeidere innenfor alle sektorer må være forberedt på å løse arbeidsoppgavene sine på nye måter som følge av digitaliseringen. Endringer i arbeidsmetoder med økt bruk av digitale verktøy og tjenester nevnes som en forutsetning for å imøtekomme innbyggernes forventninger til effektive tjenester av god kvalitet. I denne sammenheng er en målsetning i digitaliseringsstrategien at kommunenes ledelse og ansatte skal ha nødvendig kompetanse til å innføre og ta i bruk digitale tjenester (Kommunesektorens organisasjon, 2017). I digitaliseringsstrategien for offentlig sektor for perioden 2019-2025 påpekes det videre at økt digital kompetanse ikke bare handler om rekruttering, men også om å utvikle og styrke kompetansen til både ansatte og ledere som allerede er ansatt (Kommunal- og moderniseringsdepartementet, 2019). I nasjonal strategi for digital sikkerhet er styrket digital sikkerhetskompetanse et prioritert område. Her fokuseres det på hvordan kompetanse og kunnskap om aktuelle trusler, sårbarheter og sikkerhetstiltak er en viktig forutsetning for å oppnå og ivareta god digital sikkerhet. Dette innebærer at alle, både privatpersoner, offentlig forvaltning, private virksomheter og myndighetene har informasjon om mulige sikkerhetsutfordringer og tiltak som kan benyttes for å håndtere disse (Departementene,

2019). Informant (I-3) uttaler følgende om sikkerhetsutfordringene ved bruk av digitale fellesløsninger:

«Jeg har tenkt på om det egentlig er noen forskjell på dette med fellesløsninger i forhold til andre ting. Jeg klarer ikke å komme på noe konkret i forbindelse med fellesløsninger. Jeg tenker at de fleste hendelser både kan ramme fellesløsninger og andre type digitale løsninger» (I-3).

Sitatet underbygges av flere av informantene våre. Hovedvekten trekker heller frem at økt kompetanse er viktig fordi konsekvensene av utilsiktede hendelser kan bli større ved bruk av digitale fellesløsninger. Informantene (I-2, I-3 og I-4) eksemplifiserer dette:

«Spesielt opp mot dette med e-meldinger registrerer jeg dette med feilsendte meldinger der kommunen eksempelvis opplever å få meldinger vi ikke skal ha. Leger og sykehus sender meldinger til kommunen om brukere som ikke bor her. Da får vi informasjon om pasienter som vi ikke skal ha, noe som går på dette med personvernet» (I-2).

Informant (I-3) mener at bruken digitale fellesløsninger som kjernejournalen i kommunen øker tilgjengeligheten på informasjon, men kan samtidig medføre utfordringer for ivaretakelsen av informasjonssikkerheten: « *[...] Dersom noen andre får innsyn i dette så er det jo enda mer informasjon som andre kan få urettmessig tak i»* (I-3). Videre legger informant (I-4) til på spørsmål om hvorvidt bruken av fellesløsninger kan gjøre konsekvensene av eventuelle feil større, at til stross for bedre styringsmuligheter, ligger dataen mer strukturert nå enn tidligere:

«Dersom noen får uautorisert tilgang til den type data så er det lettere å ''make sense of it''. Tenk dersom du får tilgang til en database med informasjon i ett strukturert format så er det mye enklere å forstå og eventuelt misbruke den strukturerte dataen sammenlignet med om du får tilgang til 10.000 ustrukturerte word-dokumenter» (I-4)

Nasjonal sikkerhetsmyndighet (2019) viser i sin årlige rapport «Helhetlig digitalt risikobilde» at organisatoriske endringer samt endringer og videreutvikling av IKT-systemer alltid vil innebære å ta risiko. Man kan aldri fjerne risikoen helt dersom man skal forsøke å oppnå gevinstene som digitaliseringen kan gi, men NSM er opptatt av at man må tilpasse

hastigheten på digitaliseringen etter forholdene. NSM erfarer at farten på digitaliseringen i mange tilfeller medfører større risiko enn hva virksomhetene selv er klar over, noe som resulterer i manglende kontroll. Ifølge NSM forutsetter en trygg digitalisering en balansegang mellom «gass og brems», hvor rask digitalisering forutsetter mer kompetanse og større sikkerhetsinvesteringer (Nasjonal sikkerhetsmyndighet, 2019). Informant (I-5) har opplevd denne typen problematikk som NSM tar opp og uttaler følgende:

«Vi ser en økt anvendelse av digitale løsninger på mange områder, og det øker bare mer og mer. Vi kjenner dette videre på sårbarhetene i systemene våre, at vi ikke er skikkelig rigget for å håndtere dette. Vi har eksempelvis ikke et eget supportapparat til å hjelpe, ettersom vi ikke har vaktordninger og slikt.» (I-5).

Ipsos har på oppdrag fra KS gjennomført en undersøkelse om endrede kompetansebehov som følge av digitalisering i helse- og omsorgssektoren. Rundt 9 av 10 kommuner har implementert velferdsteknologiske løsninger i løpet av de siste 2 årene, og over halvparten av kommunene har digitalisert pasient og brukeropplysninger. I tillegg har omkring halvparten av kommunene digitalisert kommunikasjonskanaler samt innført nye IKT-systemer (Ipsos Public Affairs, 2018). I undersøkelsen til Ipsos kommer det frem at rundt 6 av 10 kommunalsjefer for helse og omsorg mener digitalisering har ført til større endringer i arbeidsoppgavene til ansatte innenfor helse- og omsorgssektoren i kommunen sin. Videre vises det til at et stort flertall av kommunalsjefene for helse og omsorgssektoren mener at de ansatte mangler nødvendig digital/teknologisk kompetanse, dette gjelder spesielt grunnleggende digital kompetanse, innovasjonskompetanse og evne til læring og omstilling (Ipsos Public Affairs, 2018). Rundt 3 av 5 kommunalsjefer innen helse og omsorg forteller at de ansatte har fått et bredere ansvars og oppgavespekter sett i sammenheng med tradisjonelle fag og profesjonsgrenser som følge av økende digitalisering. Dette trekker også informant (I-2) frem og uttaler: *«Hovedtyngden av deres ansatte er mest opptatt av å gi tjenestemottakerne en forsvarlig tjeneste, så kommer dette med journalføring og bruk av digitale verktøy som noe ekstra man bare må forholde seg til»* (I-2). Bare litt over 40 prosent av kommunene i undersøkelsen har en forankret plan og/eller strategi for kompetanseheving innenfor helse og omsorgssektoren. 3 av 4 kommuner oppgir å ha på plass rutiner for opplæring av ansatte innenfor teknologi relatert til deres arbeidsoppgaver i helse- og omsorgssektoren, allikevel sier også 9 av 10 kommuner at de ser et behov for å bruke mer tid på opplæring av ansatte innenfor teknologi og digitale prosesser i helse- og omsorgssektoren (Ipsos Public Affairs,

2018). Informant (I-2) trekker opp utfordringene med opplæring i forbindelse med kommunens IKT-systemer:

«*Det er vanskelig med opplæring. Vi har mange ansatte, og ansatte som jobber i mindre stillinger, og i mange av disse er det videre relativt stor turnover. Så opplæring er absolutt noe av det mest krevende som vi må prøve å finne løsninger på»* (I-2).

Informant (I-3) problematiserer hvordan de ansattes holdninger til digital sikkerhet kan være en barriere for kommunens opplæringsarbeid:

«Det første året jeg var ansatt jobbet så arrangerte jeg nasjonal sikkerhetsmåned og deltok på ansattes-dag hvor jeg leverte ut informasjonsskriv fordi ikke alle hadde ansatt-epost. Det var mange som nektet å ta imot informasjon, og jeg fikk som respons at "jeg jobber ikke med data så det gjelder ikke meg"» (I-3).

Videre påpeker informanten at manglende ressurser til oppfølging i kommunen kan være et hinder for å sikre tilstrekkelig digital kompetanse:

«Vi bruker eksempelvis KS læring og KINS-kurset som er et interaktivt kurs om informasjonssikkerhet med spørsmål som jeg syntes er veldig bra og som er tilgjengelig for alle ansatte. Spørsmålet var om dette skulle være obligatorisk, noe jeg fikk beskjed om at det skulle være, men når alt er obligatorisk så klarer jeg ikke å følge det opp. Så foreløpig er det sånn at jeg håper at folk ser sitt eget ansvar» (I-3).

Oppsummering

Empiriske funn som har blitt fremhevet i dette delkapittelet viser at digitale avhengigheter, lengre verdikjeder samt manglende kompetanse er en økende sikkerhetsutfordring ved bruk av digitale fellesløsninger i kommunesektoren. Det er først og fremst det økte konsekvenspotensialet ved bruk av digitale fellesløsninger som problematiseres. De digitale verdikjedene kjennetegnes av å være tett koblede, hvor feil kan spre seg raskere og føre til mer alvorlige konsekvenser for informasjonssikkerheten. Dette illustreres med eksempler fra informantene som viser det kan oppstå feil hvor man blir feilkoblet/logget inn for noen andre og får tilgang til data man ikke skal ha. Samtidig vil også de lange verdikjedene gjøre at feil på ett sted i verdikjeden kan medføre at alle underliggende tjenester blir utilgjengelige.

Videre viser empirien at kommunene i stor grad har blitt avhengige av at sentrale fellesløsninger fungerer til enhver tid for å kunne opprettholde sin egen funksjon. Det fremheves videre at manglende oversikt og forståelse av egne digitale verdikjeder, og avhengigheten til disse utgjør en nasjonal sårbarhet. Sistnevnte viser seg også å være en utfordring som gjenspeiles i kommunesektoren der empirien viser at kommunene jobber lite målrettet mot å danne seg oversikt over egne avhengigheter og verdikjeder, og her er nevnes særlig manglende interne ressurser og kompetanse som hindre i denne sammenheng.
Videre viser både de skriftlige dokumentene og intervjudataen at manglende digital kompetanse utgjør en sentral utfordring for kommunene. Det økte konsekvenspotensialet av menneskelige feil underbygger viktigheten av god digital kompetanse. Videre demonstrerer empirien at de ansatte gjerne har andre hovedoppgaver som gjør at informasjonssikkerhet ikke prioriteres tilstrekkelig, og at de ansattes holdninger til det digitale sikkerhetsarbeidet samt manglende ressurser og kapasitet til oppfølging fremstår som sentrale hindre for kommunenes kompetansehevende tiltak.

5.3 Hvilke utfordringer opplever kommunene i forbindelse med regelverket og intern organisering på informasjonssikkerhetsområdet?

Digi Rogaland

Digi Rogaland er et samarbeid mellom alle kommunene i Rogaland fylke, fylkesmannen, fylkeskommunen og KS Rogaland om å ta i bruk digitale verktøy som skal bidra til et bedre tjenestetilbud for både innbyggere og næringsliv. Rogaland er det første fylket i Norge som har fått til et samarbeid hvor alle kommunene i fylket deltar. Ordningen finansieres gjennom bidrag fra hver enkelt medlemskommune og fylkesmannen. I tillegg samarbeider Digi Rogaland med lignende samarbeidsordninger i andre fylker/regioner hvor man både får og gir læring om utvikling og implementering av nasjonale prosjekter (Digi Rogaland, u.å-b). Digi Rogaland har også dialog med KS gjennom både nasjonale prosjekter og gjennom KommIT-rådet. Ambisjonen med Digi Rogaland-samarbeidet er at innbyggerne skal tilbys samme tjenester og digitale løsninger på tvers av kommunegrensene. Et av målene til Digi Rogaland er at medlemskommunene i samarbeid skal bidra i utviklingen og videreutviklingen av nasjonale fellesløsninger. Finansiering gjennom fellesressurser i Digi Rogaland og fra lokalt næringsliv skal sørge for at kommunene får mulighet til å sette i gang nasjonale prosjekter eller videreutvikle eksisterende løsninger. Deling og gjenbruk av løsninger, prosessforbedring og hjelp i forbindelse med gevinstrealisering beskrives som

sentrale byggeklosser i samarbeidsprosjektet (Digi Rogaland, u.å-b). Eksempler på dette er at Digi Rogaland skal sørge for at erfaringer i forbindelse med innføring av digitale løsninger i en kommune skal deles, og komme andre kommuner til gode. Dette gjøres ved at Digi Rogaland utarbeider en verktøykasse for implementering av løsninger slik at de potensielle gevinstene som ligger i digitalisering oppnås, og at implementeringsprosessen effektiviseres på bakgrunn av erfaringsdeling (Kommunesektorens organisasjon, 2018b). tre av informantene (I-2, I-3 og I-4) opplyser at enten digi helse, digisos eller begge tjenestene ble innført i kommunen uten bistand fra Digi Rogaland-samarbeidet. Årsakene til dette varierer, informant (I-2 og I-4) var tidlig ute med en eller begge av disse fellesløsningene før Digi Rogaland kom på banen. Informant (I-3) forklarer at de selv viste for lite initiativ opp mot Digi Rogaland når de skulle ta i bruk DigiSOS-løsningen, noe som fikk konsekvenser for implementeringsprosessen:

«Jeg viste for lite initiativ og vi endte derfor opp med å gjøre dette selv, noe løsningen også bærer veldig preg av [...]Det har vært et rot. Jeg har veldig lyst til å gjennomføre digi helse-prosjektet i samarbeid med Digi Rogaland slik at vi ikke går i de samme fellene som andre allerede har gjort» (I-3).

Alle kommuner i landet har tilsvarende lovpålagte oppgaver, og innbyggerne har mange av de samme forventningene, ønskene og behovene uavhengig av hvilken kommune de tilhører. Samarbeidet i Digi Rogaland skal bidra til bedre tjenester for både innbyggere og lokalt næringsliv, noe som skal skje gjennom raskere saksbehandling, bedre kvalitet på tjenestene og økt bruk av digital selvbetjening. Mer deling og gjenbruk av både ressurser og erfaringer skal bidra til mer effektiv gjennomføring av prosjekter i kommunene. En av informantene eksemplifiserer hvordan samarbeidet muliggjør for at kommunene kan dele erfaringer når nye løsninger skal implementeres: «*Digi Rogaland består av en gi og ta praksis, hvor andre kan komme og se på våre implementerte løsninger samtidig som at vi kan få innspill fra andre kommuner om løsninger vi sliter med*» (I-5). I tillegg skal Digi Rogaland ifølge Statsforvalteren i Rogaland (2018) bidra til at kompetansenivået er godt nok i kommunene. For innbyggerne i kommuner tilknyttet Digi Rogaland vil dette i praksis bety at det skal bli enklere å samhandle med kommunen de bor i digitalt, man reduserer «digital ulikhet» mellom kommunegrensene, i tillegg til at nye prosjekter utvikles og testes i Rogaland (Digi Rogaland, u.å-b).

Digi Rogaland har flere faggrupper. Faggruppen for informasjonssikkerhet er en felles arena som alle medlemskommunene i Digi Rogaland kan benytte seg av for å diskutere problemstillinger innenfor informasjonssikkerhet, dele utfordringer og erfaringer fra egen kommune og få råd og veiledning innen oppbygging av god kultur og kompetanse (Digi Rogaland, u.å-c). Informantene har litt ulike erfaringer når det gjelder utnyttelse av denne faggruppen. En av informantene forklarer at rollen til Digi Rogaland i forbindelse med informasjonssikkerhet er å bidra med spredning av kunnskap og kompetanse (I-5). Videre fremhever flere informanter det uformelle aspektet med faggruppen, der fremfor at problemstillinger tas opp i formelle møter, bidrar faggruppen til nettverksbygging: « [...] *Selv om jeg ikke nødvendigvis løfter opp utfordringer eller problemstillinger i et formelt møte, bruker jeg likevel nettverket jeg har som en del av dette samarbeidet for å drøfte og få innspill»* (I-5). En av informantene påpeker videre at det foreløpig er de kompetansehevende tiltakene som i størst grad vektlegges i faggruppen:

«Foreløpig har ikke Digi Rogaland kommet lengre enn at fokuset er på kompetansehevende tiltak. På sikt er det ønskelig å få til mer samarbeid slik at enhver kommune kan ta opp problemstillinger i faggruppen for å unngå at man sitter alene med det» (I-3).

Kommunenes selvstendige ansvar for informasjonssikkerhet

Kommunene har generelt et grunnleggende ansvar for å ivareta befolkningens sikkerhet og trygghet innenfor sitt geografiske område. I dette ansvaret ligger det videre at kommunene er pålagte å gjennomføre helhetlige risiko- og sårbarhetsanalyser, der kommunene skal kartlegge og vurdere sannsynligheten for uønskede hendelser som kan ha betydning for kommunen (NOU 2018: 14, 2018). I forbindelse med digitaliseringsarbeidet har kommunene videre et selvstendig ansvar for digitaliseringstiltak og ivaretakelsen av IKT-sikkerhet i egen virksomhet. Ettersom at digitalisering alltid vil innebære risiko, har virksomheter de senere årene blitt stilt ovenfor nye regulatoriske krav for å påse at digitaliseringsarbeidet foregår på en forsvarlig måte så vel som at sikkerheten ivaretas i forbindelse med de nye digitale løsningene som innføres (Nasjonal sikkerhetsmyndighet, 2020a).

Lovverket (eForvaltningsforskriften, sikkerhetsloven og personopplysningsloven) som regulerer store deler av kommunenes arbeid med informasjonssikkerhet har en funksjonell innretning som gjør at de kommunale virksomhetene har langt større frihet til å tilpasse informasjonssikkerhetsarbeidet til en lokal kontekst og et lokalt trusselbildet. At regelverket

på informasjonssikkerhetsområdet i hovedsak er basert på en risikobasert tilnærming innebærer videre at virksomhetene kontinuerlig må ha et bevisst forhold til endringene i eget risikobilde, og hvorvidt sikkerheten er tilpasset den risikoen som virksomhetene står ovenfor (Departementene, 2012). Mangelen på en risikobaserte tilnærming kunne ført til at kommunale virksomheter ville manglet tilstrekkelig kunnskap om hvilke uønskede hendelser som kunne ha inntruffet og fått betydning for kommunen, i tillegg til hvorvidt etablerte tiltak og kontroller på en god måte evnet å redusere risikoen (KS, 2020). Studiens informanter har ulike synspunkter når det gjelder regelverket. Informant (I-5) retter oppmerksomhet mot de positive aspektene ved et mer funksjonelt utformet regelverk og understreker særlig muligheten til å gjøre tilpasninger med utgangspunkt i den enkelte kommunes behov som positivt:

«*Regelverket gjør jo at man får disse tingene mer tilpasset organisasjonen. Denne tilpasningen gjør oss sikrere på at dette anvendes. Alternativet er at man kommer med noe rigid som de ansatte bare rister på hodet av, og tar snarveier for å omgå regelverket*» (I-5). For de kommunale virksomhetene betyr lovverkets utforming at hver enkelt kommune kan ha forskjellige typer sikkerhetsløsninger og tiltak avhengig av opplevd risikonivå, der gjennomføringen av risikoanalyser skal gjøre disse i stand til å redusere risiko og sårbarhet i egen virksomhet (Nasjonal sikkerhetsmyndighet, 2020a).

Kommunal- og moderniseringsdepartementet (2016) hevder arbeidet med IKT-sikkerhet skal følge de fire prinsippene for samfunnssikkerhet i Norge, som er ansvar, nærhet, likhet og samvirkeprinsippene. Disse understreker virksomhetenes selvstendige ansvar for forebygging og håndtering av uønskede hendelser knyttet til sin bruk av IKT, noe som også understrekes i nasjonal strategi for informasjonssikkerhet (Departementene, 2012) og nasjonal strategi for digital sikkerhet (Departementene, 2019). Et eget delmål i nasjonal strategi for digital sikkerhet er at norske virksomheter skal ta ansvar for håndteringen av uønskede hendelser i egen virksomhet og dele relevant informasjon til myndigheter og andre aktuelle aktører (Departementene, 2019). Kommunal- og moderniseringsdepartementet (2016) påpeker i likhet med gjeldende lover at sikkerhetstiltak skal være utformet på basis i risikoanalyser. Det er virksomhetene selv som må vurdere om informasjon og relevante systemer er tilstrekkelig sikret. Denne vurderingen må tas på bakgrunn av relevant regelverk, trussel og risikobildet, og andre kjente sårbarheter. Virksomhetsledelsen er ansvarlig for å innføre tiltak slik at risikonivået er forsvarlig, dette

innebærer at de også tar stilling til hvor mye risiko som kan aksepteres. Det vises også til at regelverket plikter virksomhetene å ha på plass ett styringssystem for informasjonssikkerhet. I tillegg nevnes viktigheten av å innlemme IKT-sikkerhet med virksomhetenes øvrige mål for å sikre at IKT-sikkerheten får den nødvendige oppmerksomheten i forhold til konkurrerende hensyn og målsetninger. Dette innebærer at IKT-sikkerhet i større grad må betraktes som en viktig forutsetning for virksomhetenes evne til å utføre oppgavene sine (Kommunal- og moderniseringsdepartementet, 2016).

Det risikobaserte regelverket gir virksomheter mer fleksibilitet og muligheter for lokale tilpasninger, allikevel kan regelverket oppleves som utfordrende for noen aktører. Dette problematiseres ytterligere av noe uklar begrepsbruk i lovverket, der ulike begreper brukes for å forklare de samme fenomenene, og de samme begrepene brukes for å beskrive forskjellige krav. For eksempel brukes informasjonssikkerhetsbegrepet ulikt i forskjellige regelverk (NOU 2018: 14, 2018). Informant (I-2) påpeker at den språklige utformingen av lovverket kan gjør det vanskelig å forstå kravene som må etterleves: «*Det er et såpass detaljert og byråkratisk språk, spesielt i personvernforordningen, som gjør at jeg faller av etter første setning omtrent*» (I-2). Difis undersøkelse om arbeidet med informasjonssikkerhet i statsforvaltningen opplyser at en utfordring hos flere statlige virksomhetene er en manglende kjennskap til relevant regelverk. Dette viser seg blant annet i form av manglende referanser til lovbestemmelsene som pålegger virksomhetene styring og kontroll på informasjonssikkerhetsområdet (Direktoratet for forvaltning og ikt, 2018). Digdir (2020a) understreker at funnene i statsforvaltningen også er relevante for kommunene. På spørsmål i tilknytning til regelverket oppgir informantene å ha variert kjennskap til regelverket på informasjonssikkerhetsområdet, en informant uttaler: «*Jeg må tilstå at jeg ikke har satt meg så godt inn i lovverket. Jeg har arvet disse systemene [...] det virker ut som at det mer eller mindre er standarder i kommunene for hvordan problemstillingene er løst*» (I-1).

Datatilsynet (2011) rapporterer videre at flere kommunene har opplevd utfordringer ved å utnytte frihetene som regelverket legger opp til når
det eksempelvis stilles krav om «forholdsmessig sikring» av personopplysninger. På spørsmål om hvorvidt kommunen har behov for mer klarhet og veiledning på informasjonssikkerhetsområdet fra myndighetene uttaler informant (I-2):

« [...]i hvert fall omkring hva som forventes, det er så mange forskjellige lovkrav vi må forholde oss til bare innenfor helse. Jeg skulle ønsket at det var mer tydelighet rundt dette med informasjonssikkerhet. [...] Så lenge vi ikke har opplevd store konsekvenser og brudd på informasjonssikkerhet så lever vi i uvisshet og håper det vil gå godt». (I-2).

Informant (I-3) opplever også regelverket som utfordrende og understreker behovet for gode veiledningsdokumenter: «*Jeg tror de aller fleste opplever regelverket som veldig tungt. [...] Det å ha normen*[3] *gjorde det litt mer praktisk, og ga eksempler og hjelp til å forstå hvordan ting kunne gjøres*» (I-3). Virksomheter som er underlagt flere regelverk opplever også utfordringer når det er mange forskjellige organer og tilsynsmyndigheter som har ansvar for å gi råd og veiledning og føre tilsyn med virksomhetens IKT-sikkerhet. Overlapp i veiledningsmateriell gjelder særlig den veiledningen som er rettet mot stat og kommunene, hvor eksempelvis både datatilsynet og Difi (nå digdir) har laget veiledere for internkontroll og informasjonssikkerhet med utgangspunkt i ISO 27001. Disse veilederne har ulik innretning og er forskjellige på noen områder fordi de er utarbeidet med til dels ulike formål (NOU 2018: 14, 2018). Man opplever derfor at brukere av veiledningsmateriellet er usikre på hvor de skal henvende seg til dersom de har behov for veiledning innenfor IKT-sikkerhet, og at det mangler et tydelig kontaktpunkt. Det kommer også frem at noen brukere har opplevd at aktørene som er ansvarlige for veiledning ikke har kapasitet til å følge opp behovet for veiledning, og at rådgivningen ikke er koordinert og enhetlig. En av informantene (I-3) gir oss innblikk i særlig en utfordring kommunen har stått ovenfor i sin kontakt opp mot tilsynsmyndighetene: *«Jeg har ved et par anledninger kontaktet datatilsynet med en konkret problemstilling og spurt om veiledning, men fått til svar at vi må gjøre vår egen vurdering. Da fikk jeg med andre ord ikke den hjelpen jeg hadde behov for*» (I-3).

Informant (I-3) forteller videre at fokuset deres ikke nødvendigvis er på å ha gjort alle vurderingene riktig. Det viktigste er at de har gjort en vurdering slik at de kan få til en dialog dersom det blir tilsyn: «*Så lenge vi har gjort en vurdering så kan jeg senke skuldrene. Vurderingene er kanskje ikke helt riktige, men hvis datatilsynet kommer på tilsyn så kan vi fortelle hvorfor vi gjorde det slik, og endelig få hjelp til vurderingene.»* (I-3).

[3] *Bransjenorm for informasjonssikkerhet og personvern (Direktoratet for e-helse, 2020b).*

Kommunene opplever blant annet at rådene og veiledningen de mottar tidvis er motstridende. Det vises til at kommuner har utfordringer når det gjelder fagkompetanse, sektorkompetanse og ledelseskompetanse innenfor IKT, noe som gjør at disse har et særskilt behov for råd og veiledning. Kommunene trekker selv frem utfordringer ved at de er underlagt flere sektorielle og tverrsektorielle lover/forskrifter, og opplever at veiledning og rådgivning har bidratt til å skape uklarheter rundt kravene de er underlagt (NOU 2018: 14, 2018). Informant (I-2) fremhever hvordan kommunens omfattende oppgaveportefølje i kombinasjon med begrensede interne ressurser kan skape utfordringer for særlig mindre kommuner med å følge opp regelverket på en tilfredsstillende måte:

«Vi klarer ikke å følge alt godt nok opp, og vi må derfor bare håpe at det er godt nok. Får vi tilsyn fra datatilsynet så får vi nok helt sikkert avvik, men da følger vi det opp når vi får en tilbakemelding om hvordan det faktisk skal være» (I-2).

Sentrale roller og posisjoner i informasjonssikkerhetsarbeidet

Digitaliseringsdirektoratet anbefaler i sin internkontrollveileder at kommunene på et tidlig stadium etablerer støttefunksjoner, eksempelvis en fagansvarlig for informasjonssikkerhet. Hensikten er at vedkommende skal støtte ledelsen med fagkunnskap rundt informasjonssikkerhetsspørsmål og være en ressursperson, pådriver og tilrettelegger for det helhetlige internkontrollarbeidet på informasjonssikkerhet. Det er ifølge internkontrollveilederen virksomhetsledelsens ansvar å etablere disse støttefunksjonene og videre sørge for at vedkommende har tilstrekkelig kompetanse og personlige egenskaper for å ivareta rollen som fagansvarlig for informasjonssikkerhet (Digitaliseringsdirektoratet, 2020b). I digitaliseringsdirektoratets undersøkelse av arbeidet med informasjonssikkerhet i kommuner og fylkeskommuner oppgir et stort flertall av de store kommunene å ha en fagansvarlig for informasjonssikkerhet. Bare litt over halvparten av de minste kommunene rapporterte derimot å ha en egen fagansvarlig for informasjonssikkerhet, de mellomstore kommunene ligger midt mellom (Digitaliseringsdirektoratet, 2020a) Informant (I-4) opplyser at de har en egen fagansvarlig for informasjonssikkerhet og beskriver rollen på følgende måte når vi spør om hvordan vedkommende involveres i sikkerhetsarbeidet rundt de digitale fellesløsningene:

«*Ansvaret for fellesløsningene er nok litt spredt i forhold til hvem som konsumerer dem. Vi har jo en egen informasjonssikkerhetsansvarlig og personvernombud som er med i helheten.*

Disse har ikke noe spesifikt ansvar eller fokus på fellesløsninger, men heller en generell rolle knyttet til all informasjonssikkerhet (I-4).

Kompetansebeskrivelsen til Digdir gir forslag til mulige ansvarsområder, ønsket kompetanse samt oppgavefordeling til ulike roller i forbindelse med informasjonssikkerhetsarbeidet i virksomheter (Digitaliseringsdirektoratet, u.å-a). Rollen som risikoeier (linjeleder) tilfaller alle personer med et mål- og resultatansvar i virksomheten. Risikoeierne er ansvarlig for håndteringen av risiko innenfor de arbeidsoppgaver de er ansvarlige for. Risikoeiere kan også kalles systemeiere dersom de har et særskilt ansvar for ett eller flere IKT-systemer. Dette innebærer at de også har ansvaret for risikoen i tilknytning til informasjonssikkerhet innenfor sitt ansvarsområde, risikoeierne/systemeiere burde derfor ha en grunnleggende kompetanse på informasjonssikkerhet. Ansvaret innebærer at risikoeierne må sørge for å ha tilstrekkelig oversikt over eget ansvarsområdet slik at risikovurderinger samt risikohåndtering kan gjennomføres på en effektiv måte. Videre er risikoeierne ansvarlige for at risikovurderingene gjennomføres, at tilstrekkelige tiltak iverksettes for å håndtere identifiserte risikoer og at risikoer som vedkommende ikke har fullmakt til å håndtere selv løftes opp i linjen slik at beslutninger kan tas på høyere nivå. I tillegg anbefaler digitaliseringsdirektoratet at risikoeiere årlig vurderer om internkontrollen innenfor eget ansvarsområde gjennomføres på en god måte, om etablerte sikringstiltak fungerer etter hensikten og om underordnede ansatte følger lover og regler (Digitaliseringsdirektoratet, u.å-a). De kommunene vi har vært i kontakt med har for øvrig organisert informasjonssikkerhetsarbeidet etter et linjeansvar. Informant (I-3) beskriver denne organiseringen slik:

«*Overordnet er det rådmann som har det juridiske ansvaret. Dette er videre delegert til systemeier som vil være kommunalsjef for eksempelvis helse- og omsorg, som har ett overordnet ansvar for sine løsninger. Så er det daglige ansvaret igjen delegert til en systemansvarlig. På digi helse-løsningen vil det eksempelvis være hun som er ansvarlig for pasientjournalsystemet som vil være systemansvarlig og ha det daglige ansvaret for løsningen*» (I-3).

Topplederen har det overordnede ansvaret for at virksomheten har tilstrekkelig styring og kontroll. Dette innebærer at informasjonssikkerhetsarbeidet gjennomføres systematisk og med stort nok omfang i alle deler av virksomheten, sett i betraktning av virksomhetens egenart og risikonivå. Topplederen og ledergruppen skal gi føringer for hvordan

internkontrollen på informasjonssikkerhetsområdet skal utføres, dette innebærer at ledelsen tar stilling til hvilke aktiviteter som skal prioriteres og gjennomføres, ansvarsfordeling, gi beskrivelser av nivåer for sannsynligheter og konsekvenser og risikoakseptkriterier (Digitaliseringsdirektoratet, u.å-a). Difi (2018) påpeker at føringer fra ledelsen er avgjørende for styring og kontroll på informasjonssikkerhetsområdet. I situasjoner der ledelsen ikke tar ansvaret på alvor, blir dette fort synlig for de ansatte. Dette kan igjen medføre uønskede konsekvenser i form av at organisasjonen får problemer med å lykkes i forbindelse med etableringen av og gjennomføringen av systematiske aktiviteter på informasjonssikkerhetsområdet. Derfor har toppledelsen et viktig ansvar for å kommunisere nødvendigheten av arbeidet med informasjonssikkerhet, samt å vurdere og eventuelt akseptere risikoer som er for store til å kunne bli vurdert i linjen (på operativt nivå) (Digitaliseringsdirektoratet, u.å-a). Digitaliseringsdirektoratet har i sin undersøkelse av arbeidet med informasjonssikkerhet i kommuner og fylkeskommuner funnet at 44 prosent av kommuner oppgir at informasjonssikkerhet er et fast tema i kommuneledelsens styringsdialog. Disse funnene tyder ifølge digitaliseringsdirektoratet på at informasjonssikkerhet ikke får nok oppmerksomhet i styringsdialogen i kommunene (Digitaliseringsdirektoratet, 2020a)

Utfordringer og faktorer som har påvirket kommunenes organisering

Mangel på kompetanse både på ledelsesnivå og blant ansatte trekkes frem som en utfordring på lokalt nivå. Blant annet kommer det frem at IKT-sikkerhet er et relativt nytt ansvarsområde for ledere som ikke prioriteres nok i forhold til andre mer tradisjonelle ledelsesoppgaver. I tillegg har mange en oppfatning av at IKT-sikkerhet er et teknisk komplisert fagområde, og at opplæringen er mangelfull og/eller av for dårlig kvalitet (NOU 2015: 13, 2015). Det kommer også frem at kommunene bare unntaksvis har en tydelig sikkerhetsorganisasjon, dette fører til at de i liten grad etterspør relevant IKT-sikkerhetskompetanse. De fleste kommuner har relativt små IKT-miljøer hvor IKT-sikkerhet inngår som en av mange oppgaver for de ansatte. I mange tilfeller legges ansvaret for IKT-sikkerhet til ansatte som har andre oppgaver som hovedansvar, noe som gjør at kommunene mangler personell som er dedikert til, og har spesialisert kompetanse innenfor IKT-sikkerhet. Informant (I-2) beskriver ansvarsfordelingen rundt digitalisering og IKT-sikkerhet på lavere nivå i virksomheten som litt tilfeldig, hvor ansvaret gjerne legges over til personer som har vist en form for interesse for teknologi:

«*Det at jeg har vist interesse for teknologi har gjort at jeg har fått mange oppgaver i tilknytning til dette [...] Et annet eksempel er at en som opprinnelig satt med et dataansvar ble gjort ansvarlig for å lukke avvikene etter at datatilsynet hadde gjennomført tilsyn*» (I-2).

Det trekkes også frem at mange ledere er lite bevisste over ansvaret de har for IKT-sikkerhet, og mangler vilje og evne til å ivareta rollen som ansvarlig for IKT-sikkerheten (NOU 2015: 13, 2015). DSB (2018) påpeker at mange kommuner har en tendens til å plassere ansvaret for IKT-sikkerheten hos IKT-avdelingen, hvor økonomi har vært en avgjørende faktor. På spørsmål om faktorer som har påvirket den interne organiseringen fremhever informant (I-4) at det økonomiske aspektet har vært premissgivende:

«*Mye bunner i økonomi og kall det en desentralisert styringsmodell hvor kommunale virksomheter har hatt en høy grad av selvråderett [...] Jeg tror ikke at informasjonssikkerhet var en førende faktor når denne organiseringen ble valgt, men det handler mest om å plassere ansvaret der vi mener at det naturlig hører hjemme*» (I-4).

DSB (2018) erfarer at kommunene generelt sett er opptatt av informasjonssikkerhet og har kjennskap til viktigheten av å ha gode systemer og rutiner på området, men at prioriteringen av IKT-sikkerhet ikke kommer frem i praksis i verken systemer eller i økonomiske prioriteringer. DSB konkluderer med at IKT-sikkerhet fremstår som et prioritert område i kommunene, men at ansvaret legges til andre uten at dette blir fulgt opp eller sikret (Direktoratet for samfunnssikkerhet og beredskap, 2018). Informant (I-3) forteller at hen generelt sett møter stor forståelse i ledergruppen og at de er klar over viktigheten av informasjonssikkerhetsarbeidet, spesielt innenfor helse. Allikevel trekker informanten frem utfordringer knyttet til den mer praktiske involveringen fra ledelsens side: *«Jeg opplever ikke at det blir etterspurt nedover, og hvis jeg da går til en leder lengre nede i kjeden [...] hvordan i alle dager skal jeg forvente at de prioriterer dette, når dette ikke er noe ledelsen etterspør»* (I-3).

I tillegg kommer det frem at informasjonssikkerhet ikke blir prioritert som et eget tema i kommuneledelsen eller i den interne styringsdialogen (Direktoratet for samfunnssikkerhet og beredskap, 2018). På spørsmål om informasjonssikkerhet får like mye oppmerksomhet som andre sentrale målsetninger på ledelsesnivå er det varierende svar fra informantene. Informant (I-4) mener at informasjonssikkerheten blir prioritert tilstrekkelig av ledelsen, og at

dette er noe som det i økende grad er fokus på. Informanten knytter det økte fokuset til innføringen av GDPR og hacking-hendelsen i Østre Toten[4]. Flere av informantene stiller seg derimot tvilende til at informasjonssikkerhet sidestilles med andre sentrale målsetninger i kommunen:

«Informasjonssikkerhetsspørsmål håndteres vel egentlig på et lavere nivå i virksomheten. Men det er klart at i de tilfeller det blir alvorlig og kritisk så kommer det nok opp på ledermøter. Men om det er et fast punkt på agendaen, det er det nok ikke» (I-1).

Informant (I-5) legger til: «*Jeg tror ikke informasjonssikkerhet er et tema som står fast på agendaen hver uke [...] men det får oppmerksomhet når der reises opp saker*» (I-5). Informant (I-2) opplever heller ikke at informasjonssikkerhet sidestilles på linje med andre strategiske målsetninger, men forteller at det oppleves som at særlig helsesektoren i kommunen har blitt mer oppmerksomme på informasjonssikkerhetsspørsmål, og har forsøkt å løfte dette opp for ledelsen i større grad:

«*Hun som er sjef innenfor helse har brakt det ganske tungt inn i kommunedirektørens ledermøte for å vise til lovkravene vi må forholde oss til. Så jeg opplever at det er et tema som har blitt mer aktualisert nå enn tidligere*» (I-2).

Informant (I-3) tar også opp utfordringer rundt prioriteringen av informasjonssikkerhet på lavere nivå i virksomheten blant systemeierne. Problematikken knytter seg til forskjeller i hvordan ulike systemeiere ivaretar rollen sin, og informanten uttaler følgende om disse utfordringene:

«*Vi har snakket mye om at vi burde være flinkere til å samle de systemansvarlige for å prate om hva det faktisk betyr å inneha et systemansvar [...] Jeg opplever alt for ofte en holdning om at "der har vi fått løsningen vi ønsket" så bare ruller det og går uten at noen tar noe som helst ansvar for løsningen*» (I-3).

Det er ifølge Norsis (2017) betydelige forskjeller i hvordan kommuner har valgt å organisere IKT-området, noe som kan ses i sammenheng med at modenheten på

[4] NorSIS (2021). *Dataangrepet i Østre Toten kommune*.

informasjonssikkerhet er varierende i kommunene. Det er også store forskjeller mellom større og mindre kommuners evne til å håndtere IKT-sikkerhetshendelser internt på bakgrunn av faktorer som ressurser og kompetanse. Det kommer frem at det foregår uformelle samarbeid mellom enkeltpersoner og mellom kommuner og andre aktører. Slike uformelle samarbeid kan gjøre det utfordrende å ha god oversikt over hvilke ressurser man har tilgjengelig ved håndtering av uønskede IKT-hendelser. Det rettes også oppmerksomhet mot at mange kommuner er avhengige av «ildsjeler» som tar ansvar for IKT-sikkerheten, noe som gjør dem sårbare dersom disse personene forsvinner ut av organisasjonen (Norsis, 2017). Denne problematikken tar også DSB opp i sin rapport om IKT-sikkerhet på regionalt og lokalt nivå, hvor de understreker viktigheten av å ilegge ansvaret for IKT-sikkerheten til funksjoner i stedet for personer. Videre hevder DSB at stor avhengighet til enkeltpersoner gjør kommunene sårbare (Direktoratet for samfunnssikkerhet og beredskap, 2018). På spørsmål om faktorer som har påvirket kommunens organisering tar informant (I-3) opp behovet for en klar og tydelig ansvarsfordeling som en hovedfaktor:

«*Du er nødt til å ha noen som står ansvarlig slik at ikke alle bare tenker "ikke vet jeg" [...] Vi har vært tydelige på at du burde ha en stedfortreder for å unngå at noen sitter med alt ansvaret alene. Dette er viktig i forhold til avhengigheten man har til enkeltpersoner.*» (I-3).

Oppsummering

Det empiriske datamaterialet viser at kommunene i forbindelse med regelverket og intern organisering på informasjonssikkerhetsområdet i varierende grad har benyttet seg av faggruppene i Digi Rogaland. Likevel understrekes det at faggruppene i det interkommunale samarbeidet bidrar til å bygge opp uformelle nettverk mellom kommunene som har vist seg å ha stor nytteverdi. Videre viser empirien at mange kommuner opplever utfordringer ved å utnytte friheten ved et risikobasert regelverk. Særlig fremheves det at kommunenes kompleksitet av oppgaver, utformingen av regelverket samt manglende oppfølging fra tilsynsmyndigheter er viktige årsaker til disse utfordringene. Som belyst i kapittelet oppgir mange av kommunene at det først er når tilsynsmyndighetene utfører tilsyn og avdekker avvik at kommunen får den nødvendige oppfølgingen for å sikre at kommunes drift er i samsvar med regelverkskrav. Den interne organiseringen i kommunene kan best beskrives som en desentralisert modell hvor man opererer etter ett linjeansvar. Manglende praktisk involvering fra ledelsens side, samt en reaktiv og hendelsesbasert oppmerksomhet til informasjonssikkerhet er særlig fremtredende utfordringer i denne sammenheng.

5.4 På hvilken måte utfordrer bruken av digitale fellesløsninger risikostyringsarbeidet i kommunene

Kommunenes tilnærming til risikostyring

Internkontroll er synonymt med intern styring og kontroll. Digitaliseringsdirektoratet (2020b) understreker at myndighetenes føringer på internkontrollområdet skal bidra til å sikre at ledere på alle nivåer i virksomheten får økt trygghet om at virksomheten når sine samlede målsetninger. I praksis innebærer dette at man i alle deler av virksomheten når fastsatte mål og resultatkrav, jobber effektivt, påser at lover og regler etterfølges og har en pålitelig rapporteringspraksis (Digitaliseringsdirektoratet, 2020b). I arbeidet med internkontroll har risikostyring en helt sentral plass, og kan ifølge Digitaliseringsdirektoratet (2020b) forstås som å utgjøre selve kjernen i virksomhetenes internkontroll. Det er de risikostyrende aktivitetene som skal bidra til at de kommunale virksomhetene blir i stand til å identifisere, vurdere og håndtere hendelser som kan påføre virksomhetene uønskede konsekvenser, og som avhengig av alvorlighetsgrad kan få betydning for hvorvidt virksomhetene når sine samlede mål. Ettersom at informasjonsbehandling utgjør en sentral aktivitet for hvordan kommunale virksomheter utfører sine oppgaver, vil en effektiv og pålitelig informasjonsbehandling være avgjørende for at kommunene når sine mål (Digitaliseringsdirektoratet, 2020b). Informasjonssikkerhetsbrudd kan på sin side medføre konsekvenser med betydning for kommunene selv, så vel som for innbyggerne og virksomhetene i form av brudd på rettigheter (rettssikkerhet), omdømmetap og økonomiske tap og beslutningsfeil. Helhetlig systematikk og oppfølging i virksomhetens samlede risikoarbeid nevnes derfor som en viktig forutsetning for at ledelsen og ansatte i virksomheten kan oppnå sikkerhet om at risikoene er under kontroll, og at virksomhetens målsetninger nås. Virksomhetene burde derfor ha en betydelig egeninteresse i å både etablere og vedlikeholde systematisk internkontroll (Digitaliseringsdirektoratet, 2020b). Flere av informantene nevner at hovedfokuset i implementeringsfasen av nye digitale løsninger er å få løsningen opp å gå. Selv om at ROS analyser er nyttige verktøy ettersom det muliggjør for at man kan oppdage forhold som ikke nødvendigvis hadde blitt synliggjort dersom man kun hadde hatt et ensidig fokus på implementeringen, påpeker informant (I-3) at vedkommende har opplevd stor frustrasjon blant kollegaer når hen har utsatt implementeringen for å gjøre nødvendige avklaringer: «*I stedet for å se på ROS som det utrolig nyttige verktøyet det faktisk er så har jeg opplevd at fokuset heller har vært å kunne si at "her er det ikke noe problem"*

slik at en raskt kan få systemet opp» (I-3). Til tross for at informanten opplever at mange ansatte ser på ROS-analysene som noe ″man bare må gjøre″, påpeker informant (I-3) at kommunen på sikt vil kunne tilrettelegge for bedre løsninger samt uthente større gevinster dersom en har fokus på å gjøre de nødvendige sikkerhetsavklaringene før tjenesten tas i bruk, kontra det at en ved en senere anledning blir nødt til å stoppe tjenesten for å gjøre nødvendige korrigeringer.

Det er ifølge internkontrollveilederen viktig å planlegge slik at de som har mest erfaring og kompetanse med systemene eller oppgavene som skal vurderes blir inkludert i risikovurderingsprosessen (Digitaliseringsdirektoratet, 2020b). Ved å involvere leverandører som forvalter digitale fellesløsninger som kan ha innvirkning på tjenestene kommunene leverer, kan disse bistå med relevant dokumentasjon så vel som økt kunnskap og forståelse av risiko og sårbarhet i tilknytning til egne tjenester (Direktoratet for samfunnssikkerhet og beredskap, 2020). Til tross for muligheten kommunen har til å be om innsyn i relevant sikkerhetsdokumentasjon hos sine leverandører uttaler informant (I-3) på spørsmål om hvorvidt leverandører involveres i risikostyringsprosessen at dette kun gjøres i helt spesifikke tilfeller. Informant (I-2) understreker behovet kommunene har for et slikt samarbeid, men trekker samtidig frem kostnadsaspektet som et hinder i denne sammenheng:

«Man skulle gjerne hatt med leverandørene slik at disse kunne svart på spørsmål om hvordan data blir lagret, destruert etc. [...] Kontraktene er på over 200 sider, og når man skal gjennomgå kontrakten for å plukke ut relevant informasjon til analysen samtidig som man har en rekke andre oppgaver, trekker man gjerne bare ut det som vi anser som nødvendig for å få systemet opp. [...] Nå er det helst slik at man unngår å involvere leverandørene på grunn av prisen man må betale for å hente dem inn i x antall timer» (I-2).

Veilederen anbefaler også at kommunene alltid gjennomfører risikovurderinger ved anskaffelse eller utvikling av IKT-systemer og at kommunene burde vurdere å gjennomføre mer avgrensede risikovurderinger rettet mot hendelseshåndtering (Digitaliseringsdirektoratet, 2020b). I undersøkelsen til Digdir (2020a) kommer det frem at 33 % av de minste kommunene, 47,7 % av de mellomstore og 58,9 % av de største kommunene gjennomfører risikovurderinger systematisk og periodisk. På spørsmål om det gjennomføres risikoanalyser i forbindelse med nye digitale løsninger opplyser samtlige informanter at de benytter ROS-analyser ved implementering av nye løsninger. Informant (I-3) påpeker at de har hatt veldig

mye fokus på å gjennomføre ROS i forbindelse med nye løsninger, men at de ikke har kommet dit at det gjennomføres analyser for alle nye systemer. Informant (I-4) legger til at det sjeldent blir foretatt nye risikovurderinger, på tross av at bruksområdet til enkelte tjenester utvides over tid. Sistnevnte får betydning for hvorvidt virksomheten klarer å innhente en oversikt over det samlede risikobilde.

«*ID-porten har vært i bruk ganske lenge, men bruksområdet til ID-porten har økt. Det er summen av alle disse utvidelsene som gjør at både verdikjedene og konsekvensene blir betydelig større ettersom det er flere tjenester som nå er avhengig av ID-porten sammenlignet med når den opprinnelse tjenesten ble risikovurdert. [...] det som er utfordrende med den desentraliserte modellen er at folk har en tendens til å kun fokusere på sin bit fremfor det totale bildet*» (I-4).

Foruten revidering av eksisterende analyser, opplyser informanten (I-4) på spørsmål om hovedutfordringene med en proaktiv tilnærming at kapasitet og ressursmangler er en hovedutfordring i denne sammenheng: « *[...]Hovedmålet er at vi skal være proaktive og jeg vil påstå at vi har god kontroll, men det er jo klart at selve kapasiteten til å få gjennomført og satt inn alle ønskede tiltak ikke alltid er tilstede*» (I-4). Informant (I-1) opplyser en lignende problemstilling i egen kommune og uttaler: «*Spørsmålet er jo alltid hvorvidt vi bør gjøre noe mer, men det er jo alltid dette kostnadsspørsmålet som ligger til grunn for hvordan vi skal prioritere ressursbruken*» (I-1).

Under selve risikovurderingen (identifisere, analysere og evaluere) skal man evaluere risikoen opp mot kommunens risikoakseptkriterier, som burde være eksplisitt formulert i de styrende dokumentene (Digitaliseringsdirektoratet, 2020b). Bruken av risikoakseptkriterier skal gjøre at virksomhetsledelsen må ta stilling til hvilke risikoforhold som kommunen mener kan aksepteres og hvilke som krever ytterligere håndtering. Videre er kriteriene viktige da mangelen på klare retningslinjer for å akseptere risiko kan gjøre det utfordrende å prioritere ressursbruken mot de risikoene det er viktig å håndtere. Funn fra Difis (2018) undersøkelse i statsforvaltningen dokumenterte at kun 35% av respondentene oppga at disse hadde klare retningslinjer for å akseptere risiko. Selv om flere av virksomhetene mente å ha etablert tiltak på bakgrunn av identifiserte behov som følge av risikovurderinger, vurderte Difi at dette i liten grad harmoniserte med mangelen på risikoakseptkriterier i virksomhetene. En av

informantene trekker frem noen utfordringer som har oppstått som følge av manglende risikoakseptkriterier i egen kommune:

«[...] *utfordringen er at folk oppfatter risiko ganske forskjellig. Den type forhold og den risikoskalaen man operer med i forbindelse med hoved-rosen kan ikke overføres til å vurdere digitale tjenester som digi helse. Det har derfor dessverre blitt slik at risikoen blir vurdert "gang for gang" noe som gjør at risikorapportene ikke kan sammenlignes*» (I-4).

I NSMs helhetlige risikorapport for 2017 skrives det at mange virksomheter er sårbare på sikkerhetsbevissthet og sikkerhetskompetanse. Manglende sikkerhetsbevissthet og sikkerhetskompetanse kan øke risikoen for utilsiktede hendelser som kan påføre både virksomheten selv og andre skade. NSM (2017a) har gjennom tilsyn avdekket at mange uønskede sikkerhetshendelser oppstår som følge av organisatoriske svakheter. Selv om IKT-avdelingen i en virksomhet har gjort gode vurderinger og innført fornuftige tiltak hender det at disse ikke er forankret hos virksomhetens ledelse. Dette gjør at sikkerhetsarbeidet ikke får den oppmerksomheten og prioriteringen som er nødvendig i den overordnede virksomhetsstyringen. Ledelsen har derfor heller ikke tilstrekkelig kunnskap om hvilken type risiko de tar på vegne av virksomheten. Det at virksomhetene mangler en helhetlig oversikt og vurdering av tiltak kan føre til at tiltakene totalt sett ikke er tilstrekkelige (Nasjonal sikkerhetsmyndighet, 2017a). Disse poengene tas også opp i NSMs risikorapport for 2021 hvor de skriver at funn fra egne tilsyn tyder på at sikkerhetsarbeidet ikke er tilstrekkelig forankret i ledelsen i mange virksomheter (Nasjonal sikkerhetsmyndighet, 2021).

I NOU-rapporten *IKT-sikkerhet i alle ledd* nevnes også mangelen på IKT-sikkerhetskompetanse som en stor utfordring for IKT-sikkerheten. Det vises til at dette er en økende utfordring, hvor man forventer et underskudd på 4100 personer med IKT-sikkerhetskompetanse i Norge innen 2030, og et globalt underskudd på 1.800.000 personer med denne type kompetanse. Videre understekes det at man behøver spisset kompetanse innenfor flere ulike områder for å oppnå en god evne til å identifisere og håndtere uønskede digitale hendelser (NOU 2018: 14, 2018). Digitaliseringsdirektoratet har avdekket mangelfull risikovurdering og risikohåndtering blant kommunene og skriver at spesielt små og mellomstore kommuner har behov for veiledning for å øke kompetansen på gjennomføring av risikovurderinger. De skriver videre at de også har funnet eksempler på større kommuner som mangler kompetanse på bruk av risikoanalyse rettet mot IKT-systemer

(Digitaliseringsdirektoratet, 2020a). NSM skriver i sin risikorapport for 2021 at mange virksomheter mangler kompetanse for å gjennomføre risikovurderinger. Den manglende kunnskapen om risiko kan videre resultere i svak risikostyring, hvor det er en manglende sammenheng mellom de risikoreduserende tiltakene som blir iverksatt og det faktiske eller reelle risikobildet virksomheten står overfor (Nasjonal sikkerhetsmyndighet, 2021). Flere av informantene trekker frem utfordringer i tilknytning til informasjonsgrunnlag samt intern kompetanse for å gjennomføre risikovurderinger av kommunenes IKT-systemer. «*Vi bruker mye tid på å finne frem til relevant informasjon for å fylle ut analysene og det å finne personer eller maler som kan hjelpe oss i selve gjennomføringen av analysene, det er svært krevende*» (I-2).

Informant (I-4) forteller at en utfordring med risikostyring av digitale fellesløsninger er at mangelen på en fast struktur for gjennomføring skaper usikkerhet når det gjelder selve innstegspunktet i analysene: «*Skal vi risikovurdere vår egen behandling av dataen ved bruk av tjenesten eller de tekniske løsningen i felleskomponenten og overprøve e-helsedirektoratets vurderinger knyttet til kryptering og overføring av data? Jeg mener at kommunene ikke har ressurser til sistnevnte*» (I-4). Informanten utdyper videre at mangelen på en fast struktur gir store variasjoner i hvor omfattende og detaljerte analysene blir, spesielt når det er ulike deltakere som involveres i gjennomføringen av ulike analyser. Informant (I-4) mener at kommunene hadde hatt stor fordel av en sentralgodkjenning av fellesløsninger/leverandører som spesifiserer sikkerhetsnivået og bruksområdet til tjenesten slik at kravene til risikovurdering blir tydeligere, og kommunene dermed hadde sluppet å ta stilling til de tekniske aspektene i sine risikovurderinger. Informant (I-3) opplyser at de som regel gjennomfører ROS-analyser etter å ha implementert nye tjenester, men opplever at dette ikke fokuseres like mye på i forbindelse med digitale fellesløsninger:

«*Vi har en faggruppe for IKT som vi i utgangspunktet skal rådføre oss med før anskaffelse av ulike løsninger, men jeg opplever ikke at dette skjer på fellesløsninger fordi de blir sett på som ett tillegg til et system vi allerede har*.» (I-3).

DSB har i sin rapport om *IKT-sikkerhet på lokalt og regionalt nivå* kommet frem til at risiko og sårbarhetsanalyser (ROS) er et verktøy som generelt sett er godt innarbeidet i kommunal sektor, men finner samtidig at nesten en tredjedel av kommunene ikke har gjennomført risiko og sårbarhetsanalyser på IKT-området (Direktoratet for samfunnssikkerhet og beredskap,

2018). Flere informanter nevner at kommunen ikke har en standardisert tilnærming til risikoanalyse på IKT-systemer, og at ROS på informasjonssikkerhetsområdet derfor er noe som oppleves som vanskelig, en av informantene uttaler: «Det *kvalitetssystemet vi har som kjører ROS er nok best på å kjøre ROS på HMS. Når det gjelder informasjonssikkerhet så opplever jeg ikke å ha hele oversikten i det systemet*.» (I-3). I tillegg oppgir DSB (2018) at mange av de kommunene som har gjennomført analyser på IKT-området ikke har gjennomført analyser det siste året, og at slike typer analyser som regel gjennomføres i forbindelse med anskaffelsesprosesser av kritiske IKT-systemer.

Hvordan arbeider kommunene for å innhente kunnskap om trusler og sårbarheter

De fleste kommunene oppgir å ha systemer for håndtering av varsler om sårbarheter og trusler mot egne IKT-systemer, likevel vurderer DSB (2018) at kommunene har begrenset kunnskap om temaet, og at flere av kommunene har forskjellige oppfatninger av hva dette innebærer. DSB skriver blant annet at kommunene selv oppgir at de retter fokuset sitt mot varsling av uønskede hendelser etter de har inntruffet, og ikke på håndtering av varsler om sårbarhet og trusler som enda ikke har materialisert seg. DSB tolker dette i retning av at kommunene har et større fokus på reaktive rutiner og systemer, og ikke prioriterer proaktivt arbeid for å kartlegge trusler og sårbarheter. I undersøkelsen kommer det frem at noen av kommunene mener at varsling av sårbarheter og trusler er et ansvarsområde som blir ivaretatt av andre aktører, deriblant samarbeidspartnere på IKT-området. Et eksempel på dette er at mange kommuner samarbeider med HelseCert som gir kommunene varsler om trusler og sårbarheter rettet mot helsesystemer og applikasjoner (Direktoratet for samfunnssikkerhet og beredskap, 2018). Flere av kommunerepresentantene som deltok i utredningen til Norsis hevder at mange grunnleggende forutsetninger for god håndtering av IKT-hendelser ikke er til stedet i kommunene. Spesielt trekker de frem at trusselforståelsen er sterkt varierende mellom ulike kommuner, og at det ikke eksisterer noe samlet og helhetlig risikobilde for kommunesektoren (Norsis, 2017). I forbindelse med dette skriver DSB at det er få kommuner som abonnerer på varsler om sikkerhetshendelser fra aktører som NorCERT og NORSIS sammenlignet med eksempelvis HelseCERT, og nevner økonomi, manglende kjennskap til tjenestene og manglende fokus som mulige årsaker til dette (Direktoratet for samfunnssikkerhet og beredskap, 2018). Flere av informantene oppgir å abonnere på nyhetsbrev fra HelseCERT. Informantene har på en annen side ulike tanker når det gjelder nytteverdien av informasjonen fra nasjonale rapporter og trusselvurderinger. Informant (I-5) påpeker at når trusselbildet er såpass dynamisk og omfattende oppleves det som en trygghet,

særlig for mindre kommuner med små IT-avdelinger, å ha et samarbeid med eksterne aktører. Informant (I-3) opplever på en annen side at informasjonen fra de nasjonale rapportene er vanskelig å ta stilling til og oppleves som litt ukjent når det overføres til en kommunal sammenheng, og understreker heller nytten av uformelle samarbeid på tvers av kommunene:

«I forbindelse med et digitaliseringsprosjekt fikk vi delt en ROS fra en annen kommune som var kjempenyttig ettersom vi fikk mange gode innspill på hendelser som kunne inntreffe. Det er dette som er mye av den store jobben, det å tenke seg til hva som kan skje» (I-3).

Informant (I-4) forteller at nytteverdien blant annet er at informasjonen fra eksterne aktører gir kommunen et bilde på hvordan risikobildet endrer seg til enhver tid, men mener at det først og fremst er den informasjonen de selv generer gjennom interne analyser som er viktigst:

«*De fleste hendelsene er utilsiktede hendelser med interne triggere, ikke eksterne faktorer. Så da er det viktig at du ikke bare har en utarbeidet plan, men at du faktisk har utarbeidet den selv. Det er utarbeidelsen som gir den refleksjonen og kompetansen som har enormt mye større verdi enn å bare lese en analyse i etterkant*» (I-4).

Digdir (2020a) observerte i sin undersøkelse av arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner at under 55 prosent av kommunene som deltok i undersøkelsen oppga å ha rapportert inn og brukt erfaringer fra håndtering av uønskede hendelser i risikoanalyser eller for å forbedre informasjonssikkerheten. I tillegg observerte Digdir at under 30 prosent av kommunene har rapportert at erfaringer fra gjennomførte øvelser brukes i risikoanalyser eller til forbedring av informasjonssikkerheten (Digitaliseringsdirektoratet, 2020a). Få av informantene oppgir å ha gjennomført øvelser på å gå over til en manuell arbeidsmetodikk, men enkelte understreker heller viktigheten av å ha gode prosedyrer og retningslinjer dersom en eller flere sentrale fellesløsninger skulle svikte. Informant (I-1) nevner i denne sammenheng at: *«Jeg vil si at helsetjenesten er veldig flinke til å lage prosedyrer og dokumentasjon på å gå over til mer manuell drift. [...] Helsesektoren er nok mer forberedt på å håndtere utfordringer som kan oppstå»* (I-1).

Oppsummering

I kapittelet om risikostyring oppgir både de skriftlige dokumentene og intervjudataen en rekke utfordringer i kommunenes risikostyringsarbeid. Et ensidig fokus på implementering av løsninger, og hvor fellesløsninger gjerne anses som et «tillegg» til eksisterende systemer gjør at sikkerhetsaspektene tidvis nedprioriteres. Empirien viser at kommunenes fokus i mange tilfeller er på gevinstrealisering og det å få løsninger implementert raskest mulig. Videre trekkes det frem at en utvidelse av bruksområdet til digitale fellesløsninger over tid kan medføre vansker med å inneha et oppdatert bilde på risiko og sårbarhet relatert til løsningene. Videre viser også empirien at manglende kompetanse på bruk av risikoanalyser rettet mot IKT-systemer er en sentral utfordring i kommunene. Sistnevnte viser seg særlig i form av at flere kommuner oppgir å ha lite tilpassede risikostyringsverktøy og systematikk i gjennomføring av ROS rettet mot digitale systemer. Et utbredt fenomen i flere kommuner er kommunikasjon og informasjonsutfordringer. Dette viser seg i form av manglende kommunikasjon og involvering av leverandørene som utvikler og drifter fellesløsningene som skal risikovurderes. Empirien viser videre at kommunene oppgir å ha noe varierende opplevelser når det gjelder nytteverdien i informasjonen om risiko og sårbarhetsforhold utarbeidet av eksterne aktører og myndigheter.

6.0 Diskusjon

I dette kapittelet vil de empiriske funnene i undersøkelsen bli sett i sammenheng med det teoretiske bidraget vi presenterte i kapittel 3. Vi vil også inkludere argumenter fra kapittelet om tidligere forskning der dette er relevant. Strukturen i kapittelet vil følge forskningsspørsmålene på samme måte som i empirikapittelet. Diskusjonen vil bidra til å besvare problemstillingen:

«Hvordan endrer bruk av digitale fellesløsninger kommunenes arbeid med informasjonssikkerhet i egen virksomhet»

6.1 Hvordan fører bruk av digitale fellesløsninger til sikkerhetsutfordringer?

Når det gjelder sikkerhetsutfordringer i forbindelse med digitale fellesløsninger er hovedfunnene vi har identifisert i forbindelse med digitale avhengigheter og verdikjeder at; (1) kommunene har blitt svært avhengige av ulike fellesløsninger, (2) feil kan spre seg raskere og føre til mer alvorlige informasjonssikkerhetsbrudd og (3) kommunene arbeider ikke målrettet for å skaffe seg oversikt over egne avhengigheter og verdikjeder. I forbindelse med manglende digital kompetanse viser det samlede datamaterialet at; (4) fokuset til de ansatte er på å tilby tjenestemottakerne en forsvarlig tjeneste og hvor bruk av digitale verktøy kommer som en tilleggsoppgave, (5) Kommunene opplever at en del ansatte ikke anser informasjonssikkerhet og digital kompetanse som noe de selv har ett ansvar for og (6) kommunene mangler ressurser til å følge opp at de ansatte gjennomfører obligatoriske oppgaver som gjennomføring av kompetansehevende aktiviteter og kurs.

Digitale avhengigheter og lange uoversiktlige verdikjeder

Empirien vår indikerer at digitale avhengigheter og lange uoversiktlige verdikjeder er en økende sikkerhetstrussel som følge av digitaliseringen i kommunal sektor. Funnene viser at den økte sikkerhetstrusselen ikke skyldes at nye type hendelser kan oppstå ved bruk av digitale fellesløsninger, men heller at konsekvensene av uønskede hendelser kan bli større. Det samlede datamaterialet viser at bruk av digitale fellesløsninger ikke innebærer endringer i hvilke typer hendelser som kan ramme løsningene. De digitale fellesløsningene står derfor ovenfor de samme sikkerhetstruende hendelsene som andre digitale løsninger eller tjenester.

Risiko kan som definert i teorikapittelet forstås som «*Et uttrykk for konsekvens/utfall av uønskede hendelser og usikkerhet assosiert med hendelser og utfall*» (Njå et al., 2020, s. 46). Selv om dataen vår viser at bruk av digitale fellesløsninger ikke medfører økt risiko fra nye type hendelser som er særegne for de digitale fellesløsningene, utgjør den økte sammenkoblingen av tjenester og aktører en økt risiko ettersom utilsiktede feil kan spre seg raskere mellom systemene som er koblet sammen. Dette kan utgjøre større konsekvenser for informasjonssikkerheten i kommunene. Informasjonssikkerhet defineres som å ivareta dataens integritet, konfidensialitet og tilgjengelighet (Von Solms & Van Niekerk, 2013). Integritet handler om at dataen ikke skal bli urettmessig slettet eller endret, mens konfidensialitet vil si at uvedkommende ikke får tilgang til dataen og tilgjengelighet handler om at dataen skal være tilgjengelig for rett person til enhver tid (Normann & Tranvik, 2012). Intervjudataen viser at informantene er samstemte om at det er et økt potensiale for mer alvorlige konsekvenser ved bruk av digitale fellesløsninger som er koblet sammen med, og er avhengige av, flere andre aktører. I empirien gis flere eksempler på hvordan konsekvensene kan bli mer alvorlige, og dette gjelder blant annet muligheten for at informasjon i større grad kan komme på avveie og bli sendt til, eller gjort tilgjengelig, for andre aktører som er koblet til samme tjeneste. En av informantene nevnte eksempelvis en teknisk feil i ID-porten som gjorde at man ble logget på hos andre og fikk tilgang til deres systemer, noe som utgjør brudd på dataens konfidensialitet (I-4). Informanten understrekte også at informasjonen gjerne ligger mer strukturert, noe som gjør det lettere å forstå informasjonen og konteksten rundt informasjonen dersom den blir tilgjengeliggjort for uvedkommende.

Flere av informantene fremhevet videre utfordringer relatert til avhengigheten de selv har til de digitale fellesløsningene de bruker. Aven (2006) definerer sårbarhet som: «*evnen et system har for å fungere og oppnå målene sine dersom det blir utsatt for påkjenninger» (Aven, 2006, s. 13)*. En av informantene nevnte spesifikt hvordan ID-porten har fått et betydelig større bruksområde, og at en av hovedutfordringene ved bruk av fellesløsninger er at svikt i disse kan føre til at alle de underliggende tjenestene blir utilgjengelige (I-4). En annen informant tok opp utfordringer knyttet til hvordan kommunen i dag har blitt vant til å ha tilgang til mer data, og data av bedre kvalitet sammenlignet med tidligere (I-3). Samme informant understrekte hvordan de tidligere alltid hadde noe å gå tilbake til når de jobbet med penn og papir, men dersom viktige fellesløsninger svikter vil de plutselig mangle tilgang til viktige informasjonsressurser. Disse eksemplene viser hvordan konsekvensene knyttet til dataens tilgjengelighet kan bli større ved bruk av digitale fellesløsninger. Kommunene får derfor en

økt sårbarhet ettersom de i større grad er avhengige av at de digitale fellesløsningene fungerer til enhver tid for å kunne utføre sine oppgaver samt levere tjenester ut til innbyggerne.

Empirien viser videre at de fleste av informantene er klar over at avhengigheter og lange digitale verdikjeder utgjør økt sårbarhet og risiko for kommunene. Likevel viser dataen at det ikke jobbes målrettet for å danne seg oversikt over avhengigheter og verdikjeder i kommunene. Sistnevnte kan i sammenheng med Njå et al., (2020) sin beskrivelse av usikkerhetsdimensjonen i risikobegrepet, ha en betydelig innvirkning på kommunenes evne til å redusere usikkerhet på bakgrunn av manglende forståelse og oversikt over hvilke typer svikt som kan oppstå i verdikjeden. Videre vil det også knytte seg stor usikkerhet til de potensielle konsekvensene av en slik hendelse, ettersom kommunene ikke vil ha oversikt over hvilke systemer som er avhengige av en gitt ekstern tjeneste eller komponent, og hvordan bortfall av denne samlet kan påvirke kommunenes tilgjengelighet til viktige data og tjenesteleveranse. Manglende og/eller ikke-eksisterende kunnskap om fenomenet vil dermed påvirke hvor presise estimater kommunene kan gi av risikoen forbundet med svikt i egne digitale systemer, samt gjøre det utfordrende for kommunene å ta stilling til endringer i risiko over tid. Barry Turner forklarer katastrofer ut fra at det eksisterer et kritisk avvik mellom de rådende antakelsene og den faktiske sikkerhetstilstanden i systemet, slik at det oppstår et misforhold mellom det risikobildet virksomhetene har drevet sine risikostyrende aktiviteter etter, og det reelle risiko og sårbarhetsbildet virksomheten står ovenfor. Turner er særlig opptatt av hvordan kombinasjonen av organisatoriske ordninger og ledelsesutfordringer skaper forutsetningen for katastrofer ved at feil, misforståelser og misoppfatninger om risikoproblemer akkumuleres ubemerket (Barry A. Turner, 1994).

Empiriske funn gir en indikasjon på at kommunenes manglende prioritering av å kartlegge digitale avhengigheter og verdikjeder kan resultere i at kommunene har en manglende forståelse av egne sårbarheter, og kan videre føre til et misforhold mellom kommunenes risikoforståelse og det faktiske risiko- og sårbarhetsbilde i kommunene. Dataen indikerer på en annen side at den manglende prioriteringen ikke skyldes at kommunene ikke anser disse problemstillingene som relevante, men heller at årsaken til den manglende prioriteringen skyldes kapasitet- og ressursutfordringer, særlig i mellomstore kommuner. Utfordringen kan derfor ikke sies å være at disse problemene går ubemerket i kommunene, men heller at kommunene har valgt en mindre ressurskrevende strategi ved å utvikle rutiner for å gå over til en manuell arbeidsmetodikk dersom fellesløsningene skulle svikte.

Manglende digital kompetanse

Intervjudataen har gitt oss flere gode eksempler på hvordan bruk av digitale fellesløsninger kan føre til større konsekvenser som følge av menneskelige feil. Også her kan de økte konsekvensene knyttes til tettere sammenkoblede systemer som gir tilgang til mer informasjon og muligheter for feilkoblinger og feilsending av informasjon. Blant annet nevnes det at ansatte glemmer å logge av systemene, noe som kan gi andre tilgang til informasjon de opprinnelig ikke skal ha tilgang på (konfidensialitet) eller at noen journalfører i andres navn (integritet). Et annet eksempel er at sensitiv informasjon kan bli sendt til feil personer eller kommuner. Flere av informantene har nevnt menneskelige feil som en stor utfordring for kommunen sin. Videre opplyser flere av informantene at menneskelige feil blir identifisert som en av de mest fremtredende hendelsene i de interne ROS-analysene. Våre empiriske funn kan ses i sammenheng med Soomro, Shah & Ahmed (2016) sitt funn om at mennesker er det mest kritiske elementet i styringen av informasjonssikkerhetsarbeidet, og kan være både en ressurs og sårbarhet i denne sammenheng. Det samlede datamaterialet vårt gir videre et klart inntrykk av at manglende digital kompetanse utgjør en stor utfordring i kommunene. De skriftlige datakildene peker på at økt digital kompetanse er en forutsetning for å lykkes med digitaliseringen i kommunal sektor, og for ivaretakelsen, av en god digital sikkerhet. På en annen side viser flere dokumenter og intervjudataen til store utfordringer med å oppnå god digital kompetanse blant de ansatte i kommunene.

Premissene for pålitelig ytelse er ifølge det HRO-teorien omtaler som en nødvendig tilstand av mindfulness, som innebærer at organisasjonene er proaktive i sine søk etter svake signaler slik at de blir i stand til å raskt oppdage og respondere på uforutsette situasjoner (Vogus et al., 2014). Datamaterialet vårt viser derimot at flere av kommunene opplever utfordringer med personalopplæring og kompetansehevende tiltak i egen virksomhet, der holdningene rundt digital sikkerhet blant de ansatte og manglende kapasitet til oppfølging fungerer som barrierer i dette arbeidet. Fortolkning er et viktig aspekt ved mindfulness, og handler om å ha gode forutsetninger for både å oppdage og håndtere svake signaler på en effektiv måte (Weick et al., 2008). Kompetanse er en viktig forutsetning for dette arbeidet, ettersom tilstrekkelig digital kompetanse gjør det mulig for de ansatte å være årvåkne og fokusere på de «riktige» signalene, i tillegg til å ha evnen til å tolke betydningen av disse for å håndtere dem.

Svært få av de ansatte i kommunene har digital sikkerhet som en hovedoppgave, noe som gjør at fokuset deres i mange tilfeller vil være på å selve tjenesteleveransen fremfor å rette fokuset sitt mot å oppdage tegn på potensielle sikkerhetsutfordringer i de digitale verktøyene de benytter i arbeidet sitt. Når ledelsen i tillegg mangler ressurser til oppfølgning av de ansatte vil dette kunne bidra til å ytterliggere dreie fokuset bort fra å ivareta sikkerheten i de digitale løsningene, og vil kunne forsterke holdningene om at digital sikkerhet ikke angår dem med mindre de jobber konkret opp mot digitalisering eller digital sikkerhet. Empirien viser at kommunene på mange måter er bevisst på utfordringene de står ovenfor, dette gjelder både kompetanse og digitale avhengigheter og verdikjeder. Likevel viser datamaterialet at det de fleste kommuner står ovenfor organisatoriske utfordringer samt mangler midler til å kunne følge opp disse problemstillingene, og får derfor en mer reaktiv tilnærming til sikkerhetsarbeidet hvor feil og/eller ulykker håndteres når de først inntreffer.

Delkonklusjon

Funnene i denne studien viser at det ikke er noen særegne hendelser som kan ramme digitale fellesløsninger. Likevel vil bruk av digitale fellesløsninger kunne føre til sikkerhetsutfordringer ved at større digitale avhengigheter og verdikjeder kan gjøre konsekvensene av en uønsket hendelse større. De økte konsekvensene retter seg mot alle delene av informasjonssikkerhetsbegrepet, der dataens integritet, konfidensialitet og tilgjengelighet kan bli påvirket som følge av utilsiktede hendelser i digitale fellesløsninger. Empirien har videre vist at flere av kommunene er klar over sårbarheten og den økte risikoen ved flere digitale avhengigheter og lengre verdikjeder. Samtidig har ikke oppfølgning av denne problematikken vært et fokusområde i kommunene. Dette resulterer videre i økt usikkerhet.

Videre er manglende digital kompetanse en betydelig sikkerhetsutfordring i kommunal sektor. Både de skriftlige dokumentene og intervjuene har vist at det finnes et stort behov for å styrke den digitale kompetansen i kommunal sektor. Kommunene opplever likevel en del utfordringer og barrierer i denne sammenheng hvor flere faktorer har hatt betydning. Den manglende kompetansen og bevisstheten i kommunene gjør det utfordrende å ha en proaktiv tilnærming til informasjonssikkerhet hvor svake signaler plukkes opp, og tolkes riktig av ansatte slik at tiltak raskt kan iverksettes. Oppgavespekteret til ansatte, ressurser til oppfølgning og holdninger blant ansatte viser seg å være viktige faktorer som bidrar til disse utfordringene.

6.2 Hvilke utfordringer opplever kommunene i forbindelse med regelverket og intern organisering på informasjonssikkerhetsområdet?

Når det gjelder regelverket på informasjonssikkerhetsområdet viser hovedfunnene i empirien at; (1) flere kommuner mangler kompetanse og ressurser for å utnytte fleksibiliteten i regelverket, (2) manglende oppfølgning fra tilsynsmyndigheter. Videre viser empiriske funn i forbindelse med intern organisering at; (3) IKT-ansvaret legges til ansatte som har andre oppgaver som hovedansvar og (4) IKT-sikkerhet fremstår som en prioritet hos ledelsen, men dette følges ikke godt nok opp i praksis.

Utfordringer med det risikobaserte regelverket

Empirien gir et klart bilde av at lovverket rundt informasjonssikkerhet legger mye ansvar på den enkelte virksomhet, og er utformet på en måte som gjør at virksomhetene selv må foreta vurderinger av passende sikkerhetstiltak. Disse vurderingene skal være risikobaserte, noe som vil si at virksomhetene skal basere tiltakene sine på bakgrunn av sin kunnskap om risiko innhentet fra egne risikoanalyser. Dataen viser at kommunene opplever en del utfordringer med å etterleve regelverket i praksis, og at dette har fått konsekvenser for hvordan kommunene arbeider med informasjonssikkerhet.

Grunntanken bak den risikobaserte tilnærmingen til regulering er at det er organisasjonene selv som besitter den nødvendige kompetansen og kunnskapen til å kunne vurdere risiko og finne de optimale løsningene for egen virksomhet (Jore, 2015). I tillegg skal også et funksjonelt/risikobasert regelverk gjøre det lettere å følge med i samfunnsutviklingen som preges av økende kompleksitet, teknologisk utvikling og raske omstillinger (P. Lindøe et al., 2012). Funnene i denne studien viser at de fleste kommunene sliter med å praktisere den risikobaserte tilnærmingen til regulering slik den fremstilles i teorien. Teorien om risikobasert regulering tar opp fordelene ved at virksomhetene kan være proaktive og tilpasse sikkerhetstiltak etter risiko og virksomhetens egenart. Manglende kompetanse til å utnytte fleksibiliteten i regelverket og manglende oppfølgning fra tilsynsmyndighetene fremstår som særlige utfordringer for kommunene. Flere av kommunene oppgir eksempelvis at de er klar over at egne vurderinger og praksiser ikke er optimale eller tilfredsstiller samtlige krav i regelverkene på informasjonssikkerhetsområdet.

Den regelbaserte reguleringsformen blir kritisert for å være reaktiv ettersom nye reguleringer/regelendringer påføres virksomhetene som en respons på uønskede hendelser som allerede har inntruffet (Jore, 2015). Funnene våre viser derimot at den risikobaserte tilnærmingen har ført til at flere kommuner har fått en mer reaktiv tilnærming til eget sikkerhetsarbeid. Fremfor å systematisk arbeide for å ivareta kravene i regelverket oppgir flere kommuner at de er avhengige av tilsyn for å få tilbakemeldinger og veiledning om hvordan konkrete problemstillinger kan løses og lovkravene kan ivaretas. Den store usikkerheten assosiert med regelverkene gjør at kommunene i enkelte tilfeller bare må stole på at de vurderingene som er gjort er tilstrekkelige for å unngå at kritiske avvik oppstår. I situasjoner hvor kommunene mangler kompetanse til å gjøre egne vurderinger påpeker Informant (I-3) videre at tilsynsmyndighetene har vært motvillige til å bistå med veiledning på konkrete problemstillinger. Sistnevnte ses i sammenheng med at regelverket plikter kommunene å foreta egne og selvstendige vurderinger. Fremfor å velge en bestemt tilnærming til regulering burde man heller forsøke å oppnå en riktig balanse mellom reguleringsstrategiene (Hopkins, 2011). Det samlede datamaterialet gir en indikasjon på at kommunene hadde hatt stor fordel av styrket veiledning fra myndighetenes side, både i forhold til mer tilpasset veiledningsmateriell og mer proaktive tilsynsmyndigheter. Her er det viktig at lovkravet om at kommunene skal gjøre egne vurderinger ikke hindrer tilsynsmyndighetene i å kunne gi konkrete råd og veiledning til kommuner som mangler intern kompetanse, og som ikke har gode forutsetninger for å gjøre disse vurderingene selv.

Utfordringer ved kommunenes organisering

Funnene i denne studien viser at kommunene organiserer informasjonssikkerhetsarbeidet sitt etter et linjeansvar hvor rådmann har det overordnede ansvaret, men hvor det daglige ansvaret er delegert til roller som systemeier og systemansvarlig. Noen av kommunene har også støttefunksjoner som fagansvarlig for informasjonssikkerhet, men disse har ikke noe konkret ansvar for de digitale fellesløsningene. Det samlede empiriske datamaterialet viser at kommunene står ovenfor noen sentrale utfordringer i forbindelse med den interne organiseringen. Utfordringene knyttes spesielt opp mot manglende oppmerksomhet og involvering fra virksomhetsledelsen.

Ifølge Daler et al., (2019) er virksomhetenes informasjonsressurser i dag av særlig stor verdi ettersom de utgjør både kjerneoppgaver og sentrale støttefunksjoner for hvordan

virksomhetene utfører oppgaver, leverer tjenester og når de sentrale målsettingene. Soomro et al., (2016) har funnet flere argumenter for å se informasjonssikkerhet i sammenheng med ledelse. Det argumenteres for å se informasjonssikkerhet i en bredere kontekst hvor informasjonssikkerhet behandles som et forretningsspørsmål på samme måte som andre aktiviteter som har tilsvarende betydning for virksomhetens markedsposisjon. Det vises til et behov for at informasjonssikkerhet blir drøftet på høyeste nivå i virksomhetene og blir sammenflettet med den overordnede virksomhetsplanleggingen, slik at informasjonssikkerhet får den nødvendige prioriteringen og engasjementet (Soomro et al., 2016). En karakteristikk med høypålitelige organisasjoner er at disse sidestiller unngåelse av feil og pålitelig ytelse med produktivitet som dominerende målsetning (Roberts, 1990).

Det samlede datamaterialet viser at kommunene sliter med å involvere toppledelsen i informasjonssikkerhetsarbeidet. Blant annet gir en av informantene uttrykk for at ledelsen ikke etterspør informasjonssikkerhet nedover, noe som har betydning for hvorvidt ledere på lavere nivåer prioriterer informasjonssikkerhet (I-3). Videre viser empirien at informasjonssikkerhetsspørsmål ikke har en fast plass på agendaen blant ledelsen i kommunene, og at slike spørsmål ofte håndteres på lavere nivåer i virksomheten. Et funn i denne studien er at virksomhetsledelsens fokus på informasjonssikkerhet i mange tilfeller kan beskrives som hendelsesbasert (reaktivt). Intervjudataene viser at informasjonssikkerhetsspørsmål først kommer på agendaen og aktualiseres hos ledelsen etter alvorlige eller kritiske sikkerhetsbrudd. På en annen side gir empiriske funn en indikasjon på at uønskede hendelser i andre kommuner, kan medføre økt bevissthet blant virksomhetsledelsen. Flere av informantene trekker blant annet frem hacking-hendelsen i Østre Toten som en hendelse som har medført økt bevissthet omkring informasjonssikkerhetsspørsmål i egen kommune. Den manglende ledelsesprioriteringen på informasjonssikkerhetsspørsmål som fremheves av empiriske funn står dermed i kontrast med de teoretiske bidragene som understreker behovet for å sidestille og prioritere informasjonssikkerhet på lik linje med andre målsettinger.

Den manglende prioriteringen av informasjonssikkerhet på sentralt nivå i kommunene kan også ses i sammenheng med det Turner (1994) omtaler som *sloppy management* som tar for seg kombinasjonen av ledelsesmangler og organisatoriske ordninger. Sloppy management er i MMD-teorien en viktig bidragsyter til at kritiske signaler ikke fanges opp i forkant av ulykker, slik at feil, misoppfatninger og misforståelser om risikoproblemer får utvikle seg

ubemerket i det som omtales som inkubasjonstiden. Selv om mange av informantene understreker at de møter forståelse dersom de oppsøker ledelsen med informasjonssikkerhetsspørsmål, vil den manglende praktiske involveringen fra ledelsens side kunne medføre utfordringer ved at ledelsen ikke har oversikt over hvilken risiko kommunene står ovenfor på informasjonssikkerhetsområdet. En av utfordringene Turner omtaler i MMD-teorien er motvilje til å prioritere fremvoksende farer. Denne utfordringen handler om at farer som identifiseres ofte undervurderes eller benektes (Pidgeon & O'Leary, 2000). Dataen vår gir ikke inntrykk av at det foregår en bevisst motvilje mot å prioritere informasjonssikkerhet fra ledelsens side i noen av kommunene. Likevel kan den manglende praktiske involveringen føre til at sikkerhetsutfordringer nedprioriteres eller ignoreres fordi ledelsen ikke har tilstrekkelig kunnskap om risikoen de tar, og heller ikke sender signaler nedover i kommuneorganisasjonen om at informasjonssikkerhet er noe som skal prioriteres.

Manglende oppfølging og kunnskap om informasjonssikkerhetsrisiko fra ledelsens side vil også gjøre det vanskelig for kommunene å prioritere ressursbruken målrettet på de områdene hvor behovet for risikoreduserende tiltak er størst. Dette funnet kan ses i sammenheng med funn fra Soomro et al., (2016) om at IT og sikkerhetsspesialister ikke klarer å ivareta ansvaret for informasjonssikkerheten alene uten støtte og engasjement fra ledelsen i organisasjonen. Et annet funn er at ansvaret for informasjonssikkerhet legges til personer som har andre oppgaver som hovedoppgave, og at disse personene gjerne er valgt ut på bakgrunn av å ha vist interesse for teknologi fremfor å ha formell kompetanse på området, noe som kan få konsekvenser for mulighetene til å avdekke sikkerhetsutfordringer.

Delkonklusjon

Det risikobaserte regelverket ble utformet med den hensikt at virksomhetene skulle få mer fleksibilitet og frihet ved å selv velge ut sikkerhetstiltak basert på virksomhetens risikonivå og egenart. Et funksjonelt utformet regelverk skal videre forebygge at regelverket blir hengende etter den samfunnsmessige og teknologiske utviklingen, ved å redusere antall preskriptive myndighetskrav. Empiriske funn i denne studien viser derimot at mange av kommunene sliter med å utnytte friheten i et funksjonelt utformet regelverk i praksis. Resultatet av disse utfordringene er at flere av kommunene har fått en reaktiv tilnærming til eget sikkerhetsarbeid, og er avhengige av tilsynsmyndighetene for å kunne rette opp avvik og forbedre systemene sine.

Den interne organiseringen av informasjonssikkerhetsarbeidet i kommunene følger et linjeansvar, hvor det juridiske ansvaret plasseres hos rådmann, men hvor det daglige ansvaret delegeres nedover i organisasjonen. Empiriske funn viser manglende praktisk involvering fra ledelsens side, der informasjonssikkerhet først aktualiseres etter uønskede hendelser, noe som gir en indikasjon på en reaktiv tilnærming til informasjonssikkerhet. Denne reaktive tilnærmingen vil kunne få konsekvenser for prioriteringen av informasjonssikkerhet nedover i virksomheten, samt kommunenes evne til å prioritere sikkerhetstiltak og innhente oversikt over hvilke sentrale risikoutfordringer de står ovenfor.

6.3 På hvilken måte utfordrer bruken av digitale fellesløsninger risikostyringsarbeidet i kommunene

Empirien viser at bruk av digitale fellesløsninger har ført til utfordringer for kommunenes risikostyring. Hovedfunnene viser at; (1) at hovedfokuset i mange kommuner er på å implementere nye digitale løsninger raskt slik at gevinster kan oppnås, (2) svak informasjonsflyt mellom ulike aktører, (3) den interne styringsstrukturen har betydning for hvordan risiko- og sårbarhet oppfattes og klassifiseres i tilknytning til de digitale fellesløsningene og (4) kompetanse, ressurser og kapasitetsutfordringer som hindrer en proaktiv tilnærming.

Målkonflikter og manglende prioritering av informasjonssikkerhet

Empirien viser at kommunene står ovenfor flere utfordringer i sitt arbeid med å styre risiko, noe som blant annet kan knyttes opp mot bruk av digitale fellesløsninger. Flere av informantene viser til utfordringer i egen kommune ved at hovedfokuset er på å få implementert nye digitale løsninger, noe som kan føre til at sikkerhetsaspektene ved løsningene ikke vies tilstrekkelig oppmerksomhet.

Turner (1976) finner at et fellestrekk i mange ulykkesrapporter er at organisasjonene har en tendens til å vie mye oppmerksomhet og ressurser på å løse bestemte problemer som ikke nødvendigvis er de mest alvorlige. Dette kan føre til at organisasjonene flytter fokuset bort fra, og blir avledet fra de mest kritiske problemene. Funn i denne studien indikerer at enkelte kommuner står ovenfor en situasjon der økonomisk risiko prioriteres på bekostning av andre forhold som kan ha betydning for dens evne til å nå egne målsetninger. Resultatet av denne prioriteringen er at kommunene i noen tilfeller vier betydelig mer oppmerksomhet mot å få digitale tjenester i drift raskest mulig, fremfor å avklare relevante

informasjonssikkerhetsspørsmål. Intervjudataen gir flere gode eksempler på dette, hvor spesielt en av informantene opplevde å bli møtt av frustrasjon blant kollegaer når vedkommende ønsket å gjøre noen sikkerhetsavklaringer av løsningen før den ble tatt i bruk (I-3). Informanten påpekte videre at formålet med risikoanalyser i mange tilfeller var å få løsningene plassert på et akseptabelt risikonivå, fremfor å bruke analysen som et verdifullt verktøy for å innhente et godt kunnskapsgrunnlag om risiko. Videre fortalte informanten om en tendens til å anse digitale fellesløsninger som et "tillegg" til systemer de allerede har, og at de derfor ikke rådfører seg med den interne faggruppen for IKT, noe som vanligvis gjøres i forbindelse med anskaffelser av løsninger.

Ifølge Weick et al., (2008) er et kjennetegn ved HRO-organisasjoner at disse innehar en form for «kronisk uro» hvor virksomhetene aktivt søker etter tegn på problemer i omgivelsene. Dette forutsetter at organisasjonene har en atmosfære av tillit, hvor det å melde fra om feil, avvik og nestenulykker oppfordres og belønnes (Weick et al., 2008). Empirien viser derimot at et for stort fokus på de økonomiske aspektene ved digitaliseringen kan føre til at oppmerksomheten dreies bort fra sikkerhetsrelaterte problemstillinger, og hvor forsøk på å ta opp sikkerhetsutfordringer blir sett på som noe negativt som vil kunne hindre målet om å oppnå økonomiske gevinster. Fokuset på økonomiske forhold kan derfor få konsekvenser for det samlede risikostyringsarbeidet, hvor verktøy som ROS blir mer en formalitet, og hvor gjennomføringen er preget av et sterkt ønske om å kunne iverksette løsningen raskest mulig. Sistnevnte vil ytterligere kunne forhindre virksomhetene fra å fange opp signaler om farer, sårbarheter og andre risikoforhold.

Aven (2006) beskriver risikostyring som en balansegang mellom å utforske muligheter å unngå uønskede hendelser. Risikostyring innebærer alle tiltak og aktiviteter en virksomhet gjennomfører for å styre risiko. I forbindelse med Avens beskrivelse av risikostyringsbegrepet tyder dataen vår på at det for noen kommuner foreligger et misforhold i balansen mellom det å utforske muligheter og det å unngå tap, hvor for mye av fokuset er på førstnevnte. Datamaterialet kan derfor ses i sammenheng med funnene til Bekkevik et al. (2018) som viser at organisatoriske maktforhold og konflikter mellom ulike målsettinger kan skape utfordringer med å tilpasse informasjonssikkerhet til andre organisasjonsmål.

Informasjonsvansker og svak informasjonsflyt mellom ulike aktører

Empiriske funn i intervjudataen viser at de kommunale virksomhetene i arbeidet med risikostyring sjeldent involverer sine leverandører av digitale fellesløsninger i gjennomføring av risiko- og sårbarhetsanalyser. Utfordringene med en manglende involvering fremheves av den ene informanten som at vedkommende blir sittende alene for å plukke ut informasjonen som kan være relevant for analysen, fremfor at leverandørene involveres for å bidra med sin kunnskap og innsikt om den digitale fellesløsningen (I-2). Funn fra dokumentstudiet og intervjudataen viser videre at mange virksomheter opplever utfordringer i forbindelse med bruk av risikoanalyser rettet mot IKT-systemer og mangler på IKT-kompetanse internt.

Katastrofer i teknologiske systemer forklares av Turner ved at informasjonssvikt og feiltolkninger bidrar til at en serie av hendelser får utvikle seg ubemerket under katastrofens inkubasjonsperiode (Barry A. Turner, 1994). Risikoproblemene som akkumuleres, og som i påvente av en trigger hendelse i senere tid utløser en ulykke, skyldes ikke forvirring eller manglende evne til å forstå teknologiske hendelser, men heller at ulike personer besitter ikke-overlappende biter av informasjon om hva som skjer, og har ulike teorier om problemene i systemet (Weick, 1998). Utfordringene knyttet til manglende kommunikasjon og informasjonsdeling mellom de kommunale virksomhetene og deres leverandører mener vi kan ses i sammenheng med fenomenet Turner beskriver som variabel atskillelse av informasjon. Fenomenet illustrerer hvordan informasjon spredt mellom ulike individer og organisasjoner kan bidra til mangelfull forståelse og klassifisering av et risikoproblem blant aktørene (Pidgeon & O'Leary, 2000). Denne problematikken kan oppstå ettersom kommunene ikke nødvendigvis verken besitter tilstrekkelig teknisk kompetanse eller har tilgang på de kritiske informasjonsbitene for å belyse relevante risikoforhold i tilknytning til de digitale fellesløsningene. Sistnevnte er særlig et element som fremheves av informantene som påpeker at kommunen bruker svært mye tid på å lete etter informasjon for å utfylle ROS-analysene (I-2). Med henvisning til empiriske funn vil vi argumentere for at kommunene vil ha stor nytteverdi av å involvere eksterne leverandører i sitt risikostyringsarbeid. Leverandørene kan bidra med potensielt verdifull informasjon og kunnskap fra en alternativ synsvinkel, som både utfordrer og korrigerer kommunenes oppfatninger når det gjelder de mest fremtredende sikkerhetsutfordringene i deres systemer, og hvordan disse bør håndteres. Ettersom det er viktig å sikre at de med mest erfaring og kunnskap om systemet involveres i risikovurderingsprosessen, kan leverandører bidra med å belyse tekniske aspekter med de digitale løsningene som kommunene ikke har samme forutsetninger for å identifisere selv.

Sistnevnte er spesielt relevant ettersom fellesløsningene både utvikles og driftes utenfor kommunene, noe som kan ha betydning for hvorvidt kommunene har den nødvendige oversikten og kunnskapen for å kunne gjennomføre meningsfulle analyser og iverksette relevante tiltak.

Foruten at kommunene sjeldent involverer eksterne leverandører i arbeidet med ROS-analyser, viser empiriske funn at kommunene ikke er samstemte når det gjelder nytteverdien av utarbeidede rapporter fra eksterne aktører og nasjonale myndigheter. Mens en av informantene påpeker at det bidrar til å skape økt trygghet i et ellers krevende og dynamisk trusselbilde, opplyser en annen informant at informasjonen oppleves som vanskelig å ta stilling til. Sistnevnte informant legger til at det helst er de uformelle samarbeidene med andre kommuner som har størst verdi når det gjelder kommunenes arbeid med å kartlegge hendelser som kan inntreffe (I-3). I den forbindelse trekker flere informanter frem det uformelle aspektet ved digi Rogaland, der faggruppene i det interkommunale samarbeidet fungerer som arenaer for nettverksbygging. Funn fra dokumentstudiet viser videre at det er få kommuner som abonnerer på sikkerhetsvarsler fra eksterne aktører, og at trusselforståelsen i de enkelte kommunene er svært varierende. *Reluctance to simplify interepretations* er en egenskap HRO-organisasjoner har til å aktivt søke alternative synspunkter som stiller spørsmål til etablert kunnskap, og som kan bidra til å avdekke skjulte risikoproblemer for å skape et mer helhetlig og nyansert bilde av pågående situasjoner (Sutcliffe, 2011).

Til tross for at informasjonen fra eksterne aktører og myndigheter kan ha variert nytteverdi for den enkelte kommunen, mener vi likevel at informasjonsgrunnlaget kan være en viktig forutsetning for at kommunesektoren skal kunne tilpasse sitt risikostyrende arbeid i tråd med samfunnsutviklingen og en stadig mer digital sektor. Til tross for at den ene informanten påpeker at det hovedsakelig er de interne analysene som bidrar til gode refleksjoner og kompetanseheving, kan likevel det å aktivt søke alternative synspunkter bidra til at kommunene ikke låses til et fast handlingsrepetoar der tiltak for å håndtere risiko- og sårbarhetsutfordringer i kommunene gjøres som en respons på hendelser kommunen har erfaring eller kjennskap til. Til tross for at erfarte og kjente hendelser kan være en indikasjon på risiko, kan den økte digitaliseringen stille kommunene ovenfor nye komplekse utfordringer, og andre risikoforhold kommunene har begrenset eller ingen kjennskap til. Når flere kommuner benytter de samme digitale fellesløsningene kan informasjonen fra eksterne aktører ytterligere bidra med å fremheve de sentrale utfordringene andre kommuner opplever

i forbindelse med de samme løsningene. For den enkelte kommunen kan dette dermed bidra til at kommunen har et oppdatert bilde på hvilke risikoforhold som utgjør størst risiko i eget IKT-system. En mer aktiv innhenting og bruk av informasjon fra eksterne aktører kan dermed være en nødvendig forutsetning for å øke trusselforståelsen internt i kommunene, og styrke samsvaret mellom kommunes risikostyrende aktiviteter og hvorvidt disse er i samsvar med de reelle risiko og sårbarhetsutfordringene disse står ovenfor.

Foruten eksterne forhold knyttet til informasjonsflyt som kan medføre fenomenet variabel atskillelse av informasjon, kan også interne forhold knyttet til organisering ha betydning for hvordan ulike deler av en organisasjon forstår og klassifiserer risikoproblemer. En av informantene uttalte at den desentraliserte modellen som kjennetegner kommunesektoren kan medføre situasjoner der hver enkelt sektor har en tendens til å fokusere på eget ansvarsområde (I-4). Weick (2008) hevder at HRO-organisasjoner kjennetegnes av å ha en fleksibel styringsstruktur hvor de i normalsituasjoner styres på en sentralisert måte, men innehar egenskaper til å raskt omstille seg til en mer desentralisert tilnærming i stressituasjoner. Funnene i denne studien indikerer at kommunene mangler den fleksible styringsstrukturen og evnen til å skifte mellom en sentralisert og desentralisert tilnærming som kjennetegner HRO-organisasjoner. Utfordringene i kommunene har vært at styringsstrukturen i for stor grad er desentralisert, og mangler det helhetsperspektivet en mer sentralisert tilnærming kan gi. Problemet oppstår når ingen har en samlet oversikt og forståelse over hvilken risiko og sårbarhet avhengigheten til eksempelvis ID-porten har for kommunen som helhet, og hva konsekvensene kan være for informasjonssikkerheten i kommunen på et overordnet nivå dersom denne tjenester svikter. Når bruksområdet til digitale fellesløsninger utvides over tid, øker også kommunenes avhengighet til løsningene. Våre empiriske funn indikerer at den desentraliserte modellen kan medføre konsekvenser i form av manglende oversikt over den totale sårbarheten et bortfall kan representere for kommunenes samlede tjenesteleveranse på tvers av sektorer. Når risikostyringen er fragmentert i ulike avdelinger og sektorer i kommunen kan dette videre ha betydning for ledelsesforankring, og hvorvidt ledelsen har tilstrekkelig kunnskap om hvordan ressursbruken kan prioriteres for å håndtere områder der sårbarhetene er størst i kommunen.

Barrierer mot en proaktiv tilnærming til risikostyring

Empiriske funn gir en indikasjon på at flere kommuner mangler kompetanse til å gjennomføre risikovurderinger av IKT-systemer. I tillegg opplever også flere av kommunene manglende kapasitet og ressurser som en barriere mot å få satt inn relevante tiltak dersom man har blitt klar over en sårbarhet eller trussel.

Ifølge Sutcliffe (2011) er et kjennetegn ved høypålitelige organisasjoner at disse innehar evnen til å både forutse farer (anticipate) og være resiliente, der førstnevnte handler om at organisasjonen er i stand til å både forutse og forebygge farer og uønskede hendelser før disse inntreffer. Et hinder i kommunens arbeid med å forutse og forebygge uønskede hendelser i egen virksomhet, er tempoet i den digitale utviklingen som har medført et risikogap der sikkerhetsaspektet har blitt hengende etter utviklingen (Daler et al., 2019). Datamaterialet i denne studien gir en klar indikasjon på at flere av kommunene opplever det som utfordrende å gjennomføre risiko- og sårbarhetsvurderinger av IKT-systemer. Informantene nevner blant annet manglende standardisering og lite tilpassede verktøy for risikovurdering av IKT-systemer, vansker med å finne informasjon til å utfylle analysene, og forvirring rundt innstegspunktet i risikoanalysene som utfordringer. Sistnevnte omhandler uklarheter rundt hvorvidt kommunene først og fremst skal risikovurdere sin egen behandling av data, eller om de skal risikovurdere de tekniske valgene som har blitt gjort i løsningen. Denne problemstillingen gjelder særlig fellesløsningene ettersom disse blir utviklet og driftet utenfor kommunene, noe som gjør det utfordrende å etterprøve tekniske valg rundt eksempelvis dataoverføring og kryptering. Samlet kan datamaterialet gi en indikasjon på at det foreligger et misforhold mellom den økte avhengigheten til IKT, og det faktiske sikkerhetsnivået i virksomhetene.

Disse funnene kan videre ses i sammenheng med det Åhlfeldt et al., (2018) hevder om at særlig kommunene kjennetegnes av å ha en ustrukturert og lite sammenhengende tilnærming til informasjonssikkerhetsarbeidet grunnet sitt brede spekter av oppgaver. Det samlede datamaterialet peker videre i retning av at kompetanse er en utfordring knyttet til gjennomføring av risikoanalyser, noe som vil kunne påvirke kommunenes muligheter til å forutse og forebygge uønskede hendelser slik HRO-teorien beskriver. Manglende kompetanse kan føre til at risikovurderinger ikke gjennomføres eller påvirke kvaliteten på analysene, noe som vil gjøre det vanskelig for kommunene å ha en proaktiv tilnærming til risikostyring.

Sistnevnte fordi det er risikoanalysene som skal generere informasjon om risiko og sårbarhetsforhold i kommunene og gi beslutningsgrunnlag. Videre indikerer intervjudataen at kommunene i noen tilfeller mangler relevante verktøy og systematiske fremgangsmåter for å identifisere og håndtere risiko og sårbarhet på informasjonssikkerhetsområdet. Flere av informantene uttrykker at manglende kapasitet og ressurser fremstår som en barriere mot en proaktiv tilnærming til risikostyringsarbeidet, og gjør at kommunene ikke alltid vil være i stand til å håndtere risikoforholdene de avdekker.

Foruten sin evne til å forutse farer, karakteriseres effektive HRO-organisasjoner av sin forpliktelse til resiliens som skal sørge for at organisasjonene kan håndtere overraskelser og feil som på tross av forebyggende arbeid likevel oppstår (Weick et al., 2008). Dette ses i sammenheng med at HRO-organisasjoner anerkjenner feilbarligheten til teknologien som brukes og menneskene som operer systemene. Empirien viser at noen av de digitale fellesløsningene har innebygget redundans ved at de har lokale kopier av kritisk informasjon, slik at løsningene til tross for å ikke kunne motta ny informasjon fortsatt vil kunne opprettholde funksjonaliteten sin dersom tilgangen til eksempelvis registre skulle svikte. Andre fellesløsninger mangler disse funksjonene, og vil derfor ikke fungere dersom det oppstår en svikt i sentrale komponenter. Likevel viser funnene i denne studien at flere av informantene mener å ha gode rutiner og prosedyrer for å gå over til en manuell arbeidsmetodikk dersom det oppstår svikt i fellesløsningene. På en annen side viser dataen at det i liten grad gjennomføres øvelser på dette området. Funnene tyder derfor på at kommunene har en plan for å opprettholde funksjonaliteten og evnen til å yte tjenester til tross for svikt i fellesløsningene. Samtidig kan det argumenteres for at kommunene kunne hatt en mer resilient tilnærming ved å i større grad gjennomføre målrettede øvelser på slike scenarier.

Delkonklusjon

Funnene viser at kommunene står ovenfor en rekke utfordringer i risikostyringsarbeidet, noe som blant annet kan knyttes opp mot bruken av digitale fellesløsninger. Empirien viser blant annet at noen av kommunene opplever et misforhold i balansen mellom økonomi og sikkerhet, hvor det rettes et større fokus på å få løsninger implementert for å oppnå økonomiske gevinster. Dette har fått negative konsekvenser for risikostyringen hvor bruk av

risikoanalyser tidvis har blitt gjennomført med et formål om å få systemet plassert på et akseptabelt risikonivå, fremfor å avdekke forhold av betydning for informasjonssikkerheten. Videre har digitale fellesløsninger en tendens til å bli ansett som et «tillegg» til systemer kommunene allerede har, noe som får ytterligere betydning for kommunenes prioritering av sikkerhetsaspektene ved løsningene. Empiriske funn viser at kommunene sjeldent involverer leverandører av fellesløsningene i gjennomføringen av risikoanalyser. Denne manglende involveringen kan skape utfordringer for hvordan risikoproblemer kategoriseres og forstås i kommunene, noe som er særlig aktuelt ettersom fellesløsningene utvikles og driftes utenfor kommunene. I tillegg viser dataen at kommunene har ulike formeninger om bruksverdien til risiko- og sårbarhetsrapporter som er utarbeidet av eksterne aktører. Noen av kommunene understreker heller nytten av uformelle samarbeid og internt utarbeide risikovurderinger i arbeidet med å ivareta en god risikoforståelse. Et annet funn er at den desentraliserte styringsformen i kommunene gjør det utfordrende å danne seg en helhetsforståelse over den samlede sårbarheten ved et bortfall av sentrale fellesløsninger.

Videre viser dataen at manglende kompetanse, ressurser, systematikk og kapasitet påvirker mulighetene kommunene har til å forutse og forebygge uønskede hendelser. I tillegg viser empiridataen at noen av de digitale fellesløsningene mangler innebygget redundans, noe som vil gjøre konsekvensene av svikt større. De fleste av kommunene oppgir å ha rutiner og prosedyrer for å kunne gjenvinne funksjonaliteten og fortsette tjenesteytingen til tross for bortfall av fellesløsningene. likevel viser også dataen at det i liten grad gjennomføres øvelser på slike scenarier.

7.0 Konklusjon

Dette kapittelet representerer avslutningen på denne studien, og har som hensikt å besvare problemstillingen som har drevet fram denne undersøkelsen. Problemstillingen som skal besvares i dette kapittelet er:

«*Hvordan endrer bruk av digitale fellesløsninger kommunenes arbeid med informasjonssikkerhet i egen virksomhet?»*

Bruk av digitale fellesløsninger har blitt beskrevet som en viktig forutsetning for å oppnå målsetningene om bedre tjenester, økt effektivitet og økte gevinster for kommunal sektor. Gjennom en sikkerhetsfaglig tilnærming har vi i denne studien funnet ut at bruken av digitale fellesløsninger stiller kommunene ovenfor en rekke utfordringer i arbeidet med å ivareta informasjonssikkerheten i egen virksomhet. Årsakene til disse utfordringene er sammensatte og kan knyttes til:

- Digitale avhengigheter og lange verdikjeder samt manglende digital kompetanse har blitt identifisert som sikkerhetsutfordringer ved bruk av digitale fellesløsninger fordi konsekvensene av utilsiktede hendelser kan medføre mer alvorlige brudd på informasjonssikkerheten. Kommunene arbeider ikke målrettet for å danne seg oversikt over avhengighetene og verdikjedene, og sliter med å ivareta god digital kompetanse, noe som gjør at kommunene står ovenfor betydelig usikkerhet.
- Ansvaret for de digitale fellesløsningene i kommunene følger linjen som følge av en desentralisert styringsmodell. Manglende oppmerksomhet til informasjonssikkerhet og praktisk involvering fra toppledelsen identifiseres som en hovedutfordring. Noe som kan medføre at ledelsen mangler kunnskap om hvilke risiko- og sårbarhetsforhold kommunen står ovenfor, samt hvilke risikoer de velger å ta på vegne av virksomheten.
- Økt andel av lovkrav og reguleringer underbygger viktigheten av å prioritere digital sikkerhet og informasjonssikkerhet i kommunal sektor. Funn viser at et funksjonelt utformet regelverk blir møtt med utfordringer i kommunene der manglende intern kompetanse kombinert med utilstrekkelig oppfølging fra tilsynsmyndighetene har gjort kommunene avhengige av tilsyn for å imøtekomme regelverkskrav. Disse utfordringene har bidratt til en reaktiv tilnærming til sikkerhetsarbeidet på informasjonssikkerhetsområdet.

- Fellesløsningene utvikles og driftes utenfor kommunene noe som skaper utfordringer i arbeidet med å gjennomføre meningsfulle risikoanalyser. Funn viser at det i noen tilfeller har oppstått forvirring rundt hvilke aspekter ved løsningene som skal risikovurderes. Til tross for disse utfordringene involveres sjeldent leverandørene av fellesløsningene eller andre eksterne aktører i denne prosessen. Flere av kommunene benytter heller uformelle samarbeid hvor informasjon deles på tvers av kommunene ettersom de ofte gjennomfører risikovurderinger av samme fellesløsninger.
- Den desentraliserte styringsmodellen i kommunene har ført til utfordringer for risikostyringen av de digitale fellesløsningene. Enkeltaktørenes fokus på eget ansvarsområde har bidratt til at kommunene mangler helhetsoversikten over den totale avhengigheten og sårbarheten de har til fellesløsninger.
- Målkonflikter mellom sikkerhet og økonomi har i noen tilfeller ført til at sikkerhetsarbeidet har blitt nedprioritert ettersom hovedfokuset er på å få løsninger i drift raskest mulig for å oppnå økonomiske gevinster.
- Manglene kompetanse på risikovurdering av IKT-systemer, lite standardiserte og tilpassede verktøy for risikoanalyse, samt ressurs og kapasitetsproblemer er identifisert som barrierer mot at kommunene klarer å få en proaktiv risikostyringsprosess opp mot fellesløsningene.

Med formål å undersøke hvordan bruken av digitale fellesløsninger har endret kommunenes informasjonssikkerhetsarbeid peker funnene i denne undersøkelsen på at den økte anvendelsen av digitale fellesløsninger både endrer og utfordrer kommunenes eksisterende informasjonssikkerhetsarbeid. Når både kvaliteten og tilgjengeligheten på informasjonsressursene øker, medfører disse endringene også nye risiko- og sårbarhetsaspekter. Endringene stiller økte krav om en mer proaktiv tilnærming til risikostyring samt at kommunene jobber mer målrettet for å fremskaffe seg helhetlig oversikt over det totale risikobilde i kommunen. Kommunene blir også i større grad avhengig av uformelle samarbeid samt kommunikasjon med eksterne aktører for å innsamle informasjon som kan brukes i gjennomføringen av risiko- og sårbarhetsanalyser.

7.1 videre forskning

Det ville vært interessant å undersøke hvordan det store fokuset på tilsiktede (cyberhendelser) hendelser i ulike rapporter og trusselvurderinger kan påvirke risikopersepsjonen og

risikostyringsarbeidet i virksomheter. Etter å ha lest gjennom et stort antall dokumenter i utarbeidelsen av denne undersøkelsen har vi observert at det gjerne anerkjennes at det er de utilsiktede hendelsene som står for majoriteten av sikkerhetsbrudd på informasjonssikkerhetsområdet, allikevel er fokusområdet i de fleste rapporter om digital sikkerhet på tilsiktede hendelser. Det hadde derfor vært interessant å undersøke hvordan dette fokuset på tilsiktede hendelser i ulike rapporter og trusselvurderinger kan påvirke risikostyringsarbeidet i ulike virksomheter.

På bakgrunn av at økt anvendelse av digitale fellesløsninger kan ses i sammenheng med det pågående digitaliseringsarbeidet i kommunesektoren kan senere forskning ha som formål å undersøke hvorvidt kommunene har klart å tilpasse seg utfordringene fremhevet i denne studien over tid. I den forbindelse vil det være interessant å undersøke hvor aktuelle disse funnene er med det digitale situasjonsbildet for sektoren etterhvert som føringene for det digitaliseringsarbeidet nås.

8.0 Litteraturliste

Andersen, S. S. (2006). Aktiv informantintervjuing. *Norsk statsvitenskapelig tidsskrift, 22*(03), 278-298.

Aven, T. (2006). *Pålitelighets- og risikoanalyse* (4. ed.). Stavanger: Universitetsforlaget.

Aven, T., Røed, W., & Wiencke, H. S. (2017). *Risikoanalyse* (2. ed.). Oslo: Universitetsforlaget.

Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding regulation: theory, strategy, and practice*: Oxford University Press on Demand.

Bekkevik, F. M., Holm, O. R., Vassilakopoulou, P., & Hustad, E. (2018). *Information security practices in organizations: A literature review on challenges and related measures.* Paper presented at the Digital and social transformation for a better society-Proceedings of the Twelfth Mediterranean Conference on Information Systems (MCIS 2018).

Blaikie, N., & Priest, J. (2019). *Designing social research: The logic of anticipation*: John Wiley & Sons.

Calder, A. (2009). *Information Security based on ISO 27001/ISO 27002*: Van Haren.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems, 26*(6), 605-641. doi:10.1057/s41303-017-0059-9

Daler, T., Sjølstad, T., Høie, T. A., & Gulbrandsen, R. (2019). *Håndbok i datasikkerhet : informasjonsteknologi og risikostyring* (4. utgave. ed.). Oslo: Fagbokforlaget.

Dalland, O. (2020). *Metode og oppgaveskriving* (7. utgave. ed.). Oslo: Gyldendal.

Danermark, B., Ekstrom, M., Karlsson, J. c., & Jakobsen, L. (2005). *Explaining Society: An Introduction to Critical Realism in the Social Sciences*: Taylor and Francis.

Datatilsynet. (2011). *Kommuneundersøkelsen 2010-2011,* . Retrieved from https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/rettigheter-og-plikter/rapporter/kommuneunders_2010_2011_internkontroll_informasjonssikkerhet.pdf

Datatilsynet. (u.å-a). Personvernprinsippene,. Retrieved from https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/

Datatilsynet. (u.å-b). Virksomhetenes plikter,. Retrieved from https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

Dawes, S. S. (2008). The evolution and continuing challenges of e-governance. *Public Administration Review, 68*, S86-S102.

Departementene. (2012). *Nasjonal strategi for informasjonssikkerhet,*. Retrieved from https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf

Departementene. (2019). *Nasjonal strategi for digital sikkerhet*. Retrieved from https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/

Digi Rogaland. (u.å-a). Digisos,. Retrieved from https://digirogaland.no/digisos/

Digi Rogaland. (u.å-b). Hva er Digi Rogaland. Retrieved from https://digirogaland.no/hva-er-digi-rogaland/

Digi Rogaland. (u.å-c). Informasjonssikkerhet. Retrieved from https://digirogaland.no/faggrupper/informasjonssikkerhet/

Digitaliseringsdirektoratet. (2020a). *Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner: kunnskapsgrunnlag - En dokumentstudie,* . Retrieved from Oslo: https://www.digdir.no/informasjonssikkerhet/arbeidet-med-informasjonssikkerhet-i-fylkeskommuner-og-kommuner/2102

Digitaliseringsdirektoratet. (2020b). *Internkontroll i praksis- informasjonssikkerhet grunnleggende innføring,* . Retrieved from https://internkontroll-infosikkerhet.difi.no/sites/sikkerhet/files/grunnleggende_innforing_-_internkontroll_informasjonssikkerhet.pdf

Digitaliseringsdirektoratet. (u.å-a). *Kompetansebeskrivelser,* . Retrieved from https://www.digdir.no/media/1006/download
Digitaliseringsdirektoratet. (u.å-b). Spørsmål og svar om nasjonale fellesløysingar,. Retrieved from https://www.digdir.no/digitale-felleslosninger/sporsmal-og-svar-om-nasjonale-fellesloysingar/760#kva_er_ei_nasjonal_fellesloysing
Direktoratet for e-helse. (2020a, 24. januar). Digihelse,. Retrieved from https://ehelse.no/prosjekt/digihelse
Direktoratet for e-helse. (2020b). Normen: Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren. Retrieved from https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren
Direktoratet for e-helse. (2020c). *Strategi for digital sikkerhet i helse- og omsorgssektoren: vurdering av behov og innretning,* (IE-1064). Retrieved from https://ehelse.no/publikasjoner/strategi-for-digital-sikkerhet-i-helse-og-omsorgssektoren-vurdering-av-behov-og-innretning
Direktoratet for forvaltning og ikt. (2018). *Arbeidet med informasjonssikkerhet i statsforvaltningen: Kunnskapsgrunnlag* (2018:4). Retrieved from Oslo: https://www.digdir.no/media/951/download?fbclid=IwAR3GBV6iNgE4swgWiIvOzuWV5jrcFtWtaKdUk3Oc7Nn9D3X5Qq3nm2Lr0qE
Direktoratet for samfunnssikkerhet og beredskap. (2018). *IKT-sikkerhet på regionalt og lokalt nivå,* . Retrieved from
Direktoratet for samfunnssikkerhet og beredskap. (2020). *Risikostyring i digitale verdikjeder*. Retrieved from https://www.dsb.no/globalassets/dokumenter/rapporter/risikostyring-i-digitale-verdikjeder.pdf
Forskrift om elektronisk kommunikasjon med og i forvaltningen, FOR-2004-06-25-988 C.F.R. (2004).
Ejdys, J., Ginevicius, R., Rozsa, Z., & Janoskova, K. (2019). The role of perceived risk and security level in building trust in E-government solutions.
Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative inquiry, 12*(2), 219-245.
Guo, Y. (2010). *E-government: Definition, goals, benefits and risks.* Paper presented at the 2010 International Conference on Management and Service Science.
Halvorsen, K. (2008). *Å forske på samfunnet : en innføring i samfunnsvitenskapelig metode* (5. utg. ed.). Oslo: Cappelen akademisk forl.
Hopkins, A. (2011). Risk-management and rule-compliance: Decision-making in hazardous industries. *Safety science, 49*(2), 110-120.
Ipsos Public Affairs. (2018). *Kartlegging av endrede kompetansebehov i en digitalisert helse- og omsorgssektor,* . Retrieved from https://www.ks.no/contentassets/9d044ddc1e12472b8c3a11fb2f851d85/rapport-ks-dypdykk-ledere-2018---oppdatert.pdf
Jore, S. H. (2015). Challengers of Building Societal Resilience through Organizational Security Risk Management.
Kommunal- og moderniseringsdepartementet. (2014a, 06.12.2014). Digitalisering i offentlig sektor,. Retrieved from https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/digitaliseringen-i-offentlig-sektor/id2340245/
Kommunal- og moderniseringsdepartementet. (2014b, 08. desember). Hva er felleskomponenter?,. Retrieved from https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/felleskomponenter/id2342598/
Kommunal- og moderniseringsdepartementet. (2016). *Digital agenda for Norge - IKT for en enklere hverdag og økt produktivitet*. (Meld. St. 27 (2015-2016)). Retrieved from https://www.regjeringen.no/no/dokumenter/meld.-st.-27-20152016/id2483795/
Kommunal- og moderniseringsdepartementet. (2019). *Én digital offentlig sektor: Digitaliseringsstrategi for offentlig sektor 2019–2025*. Retrieved from https://www.regjeringen.no/no/dokumenter/en-digital-offentlig-sektor/id2653874/

Kommunal- og moderniseringsdepartementet. (2021a, 01. februar). Digitalisering i offentlig sektor . Retrieved from https://www.regjeringen.no/no/dokument/dep/kmd/andre-dokumenter/brev/utvalgte_brev/2021/digitalisering-i-offentlig-sektor/id2830849/

Kommunal- og moderniseringsdepartementet. (2021b). *Vår felles digitale grunnmur — Mobil-, bredbånds- og internettjenester*. (Meld. St. 28 (2020–2021)). Retrieved from https://www.regjeringen.no/no/dokumenter/meld.-st.-28-20202021/id2842784/?ch=1

lov om kommuner og fylkeskommuner (kommuneloven),, LOV-2018-06-22-83 C.F.R. (2018).

Kommunesektorens organisasjon. (2017). *Digitaliseringsstrategi for kommuner og fylkeskommuner 2017-2020*. Retrieved from https://www.ks.no/globalassets/fagomrader/digitalisering/klart-sprak-i-digitale-selvbetjeningslosninger/sprak-og-tekst/ingresser/KS-Digitaliseringsstrategi-hefte-F32.pdf

Kommunesektorens organisasjon. (2018a, 09. oktober). Effektiv digitalisering av offentlig sektor. Retrieved from https://www.ks.no/fagomrader/digitalisering/styring-og-organisering/digitaliseringsstrategien/mal-og-posisjoner2/effektiv-digitalisering-av-offentlig-sektor/

Kommunesektorens organisasjon. (2018b, 13. desember). Hele Rogaland er med. Retrieved from https://www.ks.no/regioner/ks-vest-norge/hele-rogaland-er-med/

Kongsvik, T. Ø. (2013). *Sikkerhet i organisasjoner*. Oslo: Akademika forl.

KS. (2020). Orden i eget hus: Kommunedirektørens internkontroll. Retrieved from https://www.ks.no/globalassets/fagomrader/lokaldemokrati/internkontroll/Kommunedirektorens-internkontroll-veileder-F41-web.pdf

Lindøe, P., Kringen, J., & Braut, G. S. (2012). *Risiko og tilsyn : risikostyring og rettslig regulering*. Oslo: Universitetsforl.

Lindøe, P. H. (2018). *Risiko, tillit og kontroll*. Oslo: Gyldendal.

Mark, M. S., Tømte, C. E., Næss, T., & Røsdal, T. (2019). Leaving the windows open–økt mangel på IKT-sikkerhetskompetanse i Norge. *Norsk sosiologisk tidsskrift, 3*(03), 173-190.

Nasjonal sikkerhetsmyndighet. (2017a). *Helhetlig IKT-risikobilde 2017,* . Retrieved from https://nsm.no/getfile.php/133675-1592831718/Demo/Dokumenter/Rapporter/helhetlig_ikt-risikobilde_2017_orig_enkeltsider_low.pdf

Nasjonal sikkerhetsmyndighet. (2017b). *Risiko 2017: risiko og sårbarheter i en ny tid*. Retrieved from https://nsm.no/getfile.php/133726-1592915950/Demo/Dokumenter/Rapporter/nsm_risiko_2017_lr_0404_enkelts_v3.pdf

Nasjonal sikkerhetsmyndighet. (2019). *Helhetlig digitalt risikobilde 2019*. Retrieved from https://nsm.no/getfile.php/133669-1592830841/Demo/Dokumenter/Rapporter/2019---nsm-helhetlig-digitalt-risikobilde.pdf

Nasjonal sikkerhetsmyndighet. (2020a). Helhetlig digitalt risikobilde 2020. Retrieved from https://nsm.no/getfile.php/134468-1604926904/Demo/Dokumenter/Rapporter/NSM_IKT-risikobilde_2020_enkeltside.pdf

Nasjonal sikkerhetsmyndighet. (2020b). *Risiko 2020,* . Retrieved from https://nsm.no/getfile.php/131421-1587034764/Hermans%20undermappe%20med%20bilder/NSM_Risiko_2020_web_0104.pdf

Nasjonal sikkerhetsmyndighet. (2021). *Risiko 2021: Helhetlig sikring mot sammensatte trusler,* . Retrieved from https://nsm.no/getfile.php/136399-1615402643/Demo/Dokumenter/Rapporter/NSM_Risiko_2021_web_enkeltside_1003.pdf

Njå, O., Sommer, M., Rake, E. L., & Braut, G. S. (2020). *Samfunnssikkerhet : analyse, styring og evaluering*. Oslo: Universitetsforlaget.

Normann, R. S., & Tranvik, T. (2012). *Personvern og informasjonssikkerhet i kommunen : en håndbok i risikovurdering*. Oslo: Kommuneforl.

Norsis. (2017). *Utredning av kommunal sektors felles behov for et kompetansesenter for håndtering av IKT-hendelser (kommuneCSIRT),* . Retrieved from Gjøvik: https://norsis.no/wp-content/uploads/2018/05/Utredning-Kommune-CSIRT.pdf

NorSIS. (2021, 08. april). Dataangrepet i Østre Toten kommune: Minst 9000 dokumenter og store e-postmengder stjålet

. Retrieved from https://norsis.no/dataangrepet-i-ostre-toten-kommune-minst-9000-dokumenter-og-store-e-postmengder-stjalet/?fbclid=IwAR2waBq6NcKunRW4XmEoyQYykkk94gXnLuXsQEMCO2dxK0y_1d5nE3ZHYlc

NOU 2015: 13. (2015). *Digital sårbarhet - sikkerhet samfunn: Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Retrieved from https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

NOU 2018: 14. (2018). *IKT-sikkerhet i alle ledd: Organisering og regulering av nasjonal IKT-sikkerhet*. Retrieved from https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/

Perrow, C. (1999). *Normal accidents: living with high-risk technologies*: Princeton University Press.

Pidgeon, N., & O'Leary, M. (2000). Man-made disasters: why technology and organizations (sometimes) fail. *Safety science, 34*(1), 15-30. doi:10.1016/S0925-7535(00)00004-7

Politiets sikkerhetstjeneste. (2021). Nasjonal trusselvurdering 2021. Retrieved from https://pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/

Roberts, K. H. (1990). Managing high reliability organizations. *California management review, 32*(4), 101-113.

Lov om nasjonal sikkerhet,, LOV-2018-06-01-24 C.F.R. (2019).

Singh, S., & Karaulia, D. S. (2011). *E-governance: Information security issues.* Paper presented at the International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International journal of information management, 36*(2), 215-225.

Statistisk sentralbyrå. (2019). *Digitalisering i kommunene: overblikk over tilstanden i 2018*. Retrieved from https://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/_attachment/388777?_ts=16b457fdd00

Statsforvalteren i Rogaland. (2018). Etablerer Digi Rogaland: Unik digital satsing i rogalandskommunane. Retrieved from https://www.fylkesmannen.no/nb/Rogaland/Kommunal-styring/Kommunal-fornying/etablerer-digi-rogaland-unik-digital-satsing-i-rogalandskommunane/

Sutcliffe, K. M. (2011). High reliability organizations (HROs). *Best Practice & Research Clinical Anaesthesiology, 25*(2), 133-144.

Sutton, D. (2014). *Information risk management : a practitioner's guide* (1st edition. ed.). Wiltshire, England: BCS The Chartered Institute for IT.

Thagaard, T. (2013). *Systematikk og innlevelse: en innføring i kvalitativ metode* Bergen: Fagbokforlaget.

Thompson, N., Mullins, A., & Chongsutakawewong, T. (2020). Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand. *Government Information Quarterly, 37*(1), 101408.

Tjora, A. (2012). *Kvalitative forskningsmetoder i praksis* (Vol. 2): Gyldendal akademisk Oslo.

Turner, B. A. (1976). The organizational and interorganizational development of disasters. *Administrative science quarterly*, 378-397.

Turner, B. A. (1994). Causes of Disaster: Sloppy Management. *British journal of management, 5*(3), 215-219. doi:10.1111/j.1467-8551.1994.tb00172.x

Vogus, T. J., Rothman, N. B., Sutcliffe, K. M., & Weick, K. E. (2014). The affective foundations of high-reliability organizing. *Journal of Organizational Behavior, 35*(4), 592-596.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security, 38*, 97-102.

Weick, K. E. (1998). Foresights of failure: an appreciation of Barry Turner. *Journal of contingencies and crisis management, 5*(2), 72-75.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Processes of collective mindfulness. *Crisis management, 3*(1), 81-123.

Åhlfeldt, R.-M., Nohlberg, M., Söderström, E., Lennerholt, C., & van Laere, J. (2018). CURRENT SITUATION ANALYSIS OF INFORMATION SECURITY LEVEL IN MUNICIPALITIES. *Journal of Information System Security, 14*(1).

Vedlegg

Vedlegg 1: Dokumenter

Utgivelsesår	Utgiver	Tittel
2017	Kommunesektorens organisasjon	Digitaliseringsstrategi for kommuner og fylkeskommuner 2017-2020
2019	Kommunal- og moderniseringsdepatrementet	En digital offentlig sektor: digitaliseringsstrategi for offentlig sektor 2019-2025
2012	Departementene	Nasjonal strategi for informasjonssikkerhet
2019	Departementene	Nasjonal strategi for digital sikkerhet
2020b	Direktoratet for e-helse	Strategi for digital sikkerhet i helse- og omsorgssektoren: Vurdering av behov og innretning.
2017a	Nasjonal sikkerhetsmyndighet	Helhetlig IKT-risikobilde
2017b	Nasjonal sikkerhetsmyndighet	Risiko 2017: risiko og sårbarheter i en ny tid
2019	Nasjonal sikkerhetsmyndighet	Helhetlig digitalt risikobilde 2019
2020b	Nasjonal sikkerhetsmyndighet	Risiko 2020
2020a	Nasjonal sikkerhetsmyndighet	Helhetlig digitalt risikobilde 2020
2021	Nasjonal sikkerhetsmyndighet	Risiko 2021: Helhetlig sikring mot sammensatte trusler
2018	NOU 2018	IKT-sikkerhet i alle ledd: Organisering og regulering av nasjonal IKT-sikkerhet
2015	NOU 2015	Digital sårbarhet - sikkert samfunn: beskytte enkeltmennesker og samfunn i en digitalisert verden
2018	Direktoratet for samfunnssikkerhet og beredskap	IKT-sikkerhet på regionalt og lokalt nivå (Internt dokument)
2020	Direktoratet for samfunnssikkerhet og beredskap	Risikostyring i digitale verdikjeder
2018	Ipsos public affairs	Kartlegging av endrede kompetansebehov i en digitalisert helse- og omsorgssektor

2020	Kommunesektorens organisasjon	Orden i eget hus: kommunedirektørens internkontroll
2016	Kommunal- og moderniseringsdepartementet	Digital agenda for Norge- IKT for en enklere hverdag og økt produktivitet
2018	Direktoratet for forvaltning og IKT	Arbeidet med informasjonssikkerhet i statsforvaltningen: Kunnskapsgrunnlag
2020a	Digitaliseringsdirektoratet	Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner: Kunnskapsgrunnlag- en dokumentstudie
2020b	Digitaliseringsdirektoratet	Internkontroll i praksis- informasjonssikkerhet grunnleggende innføring
2011	Datatilsynet	Kommuneundersøkelsen 2010-2011
U.Å	Digitaliseringsdirektoratet	Kompetansebeskrivelser
2017	Norsis	Utredning av kommunal sektors felles behov for et kompetansesenter for håndtering av IKT-hendelser (kommuneCSIRT)

Tabell 2 Dokumenter brukt i forbindelse med dokumentstudiet

Vedlegg 2: Informanter

Kode	Informantens ansvarsområde	Kommunekategorisering
I-1	IKT-rådgiver	Mellom-stor
I-2	Systemansvarlig	Mellom-stor
I-3	Fagleder digitalisering	Mellom-stor
I-4	Digitaliseringssjef	Stor
I-5	Digitaliseringssjef	Mellom-stor

Tabell 3 Informantoversikt

Vedlegg 3: intervjuguide

Intervjuguide

Introduksjonsspørsmål:

Før vi begynner, har du noen spørsmål til oss etter å ha lest gjennom intervjuguiden og informasjonsskrivet?

Sikkerhetsutfordringer knyttet til informasjonssikkerhet:

(Når vi spør om sikkerhetsutfordringer er vi opptatt av uintenderte hendelser)

1. Kan du gi en kort forklaring på hvordan utviklingen med digitalisering av helsetjenester har vært de siste årene i deres kommune?
2. Bruk av fellestjenester nevnes som et viktig verktøy for å oppnå gevinster ved digitalisering ifølge KS sin digitaliseringsstrategi. Hvilke fellestjenester mener dere er de mest sentrale for helsesektoren i deres kommune?
3. Digi helse er en fellestjeneste som blir brukt av en rekke kommuner i Rogaland, bruker dere denne tjenesten?

- Hvis ja, hvor lenge har den vært i drift?

4. Hvordan påvirker bruk av fellestjenester i helsesektoren informasjonssikkerheten i kommunen deres?
    - Hvilke typer uintenderte hendelser kan ramme digitale fellestjenester?
    - Medfører bruk av fellestjenester særegne sikkerhetsutfordringer (hendelser som kan inntreffe, sårbarheter eller andre organisatoriske utfordringer)?
    - Hva er etter deres mening de største utfordringene ved bruk av fellestjenester?

Organisering av informasjonssikkerhetsarbeidet:

5. Lovverket som regulerer informasjonssikkerhetsarbeidet er i stor grad risikobasert og legger ansvaret for å analysere risiko og finne passende tiltak til virksomhetene selv. Hvordan opplever dere regelverket?
    - Gir regelverket dere gode forutsetninger for arbeidet med informasjonssikkerhet?
    - Hva opplever dere som de største fordelene og ulempene med et risikobasert regelverk?
    - Opplever dere fleksibiliteten som ligger i regelverket som en fordel eller hadde det vært behov for mer klare rammer i arbeidet med informasjonssikkerhet i kommunen?
    - Er det områder hvor myndighetene burde bistå mer (eksempelvis områder hvor det hadde vært behov for veiledningsmateriell)?

6. Hvordan er rollefordelingen med tanke på ansvaret for informasjonssikkerhet i fellestjenester i kommunen deres?
    - Hvem er ansvarlige for informasjonssikkerheten i de digitale fellestjenestene innenfor helsesektoren, eksempelvis digi helse?
    - På hvilken måte er ledelsen involvert i informasjonssikkerhetsarbeidet i tilknytning til fellestjenester?
    - Hvilke vurderinger ligger bak den valgte organiseringen, og hvilke faktorer kan eventuelt ha påvirket disse valgene?
7. Hvordan fungerer samarbeidet med digi Rogaland?
    - Hvilken rolle har Digi Rogaland i forhold til informasjonssikkerhet og fellestjenester?
    - Hvilken betydning har det interkommunale samarbeidet hatt for ivaretakelsen av sikkerheten i digitale fellestjenester som digi helse.

Risikostyring:

8. Hva vil dere si er hovedutfordringene i forbindelse med risikostyring av digitale fellestjenester?
    - Er tiltakene dere bruker hovedsakelig proaktive (reduserer sannsynlighet for at hendelser inntreffer) eller reaktive (redusere konsekvensene når en hendelse først inntreffer)?
    - Har bruk av fellesløsninger ført til endringer i risikostyringen?
9. Direktoratet for e-helse og NSM tar opp utfordringene ved lange verdikjeder og avhengigheter på tvers av sektorer som følge av økende digitalisering, er dette problemstillinger som er gjeldene for deres kommune?

Hvis ja:

- Hvorfor er dette en utfordring?
- Hvordan arbeider dere for å kartlegge egne avhengigheter og sårbarheter
- Hvordan arbeider dere for å håndtere disse utfordringene?
- Opplever dere å ha oversikt og kontroll over egne avhengigheter og sårbarheter?

Hvis nei:

- Hvorfor mener dere dette ikke er relevant for dere?

10. Hvordan er ansvarsfordelingen på informasjonssikkerhetsområdet mellom de som utvikler og drifter fellestjenester og kommunene som bruker dem?
    - Opplever dere ansvarsfordelingen slik den er i dag som naturlig? Hvorfor og eventuelt hvorfor ikke?
    - Hvordan opplever dere kommunikasjonen om risiko, sårbarhet og avhengigheter i forbindelse med bruk av digitale fellestjenester?

Vedlegg 4: Samtykkeskjema

Samtykke for behandling av personopplysninger i forskningsprosjekt

Universitetet i Stavanger

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet "*digitalisering og sårbarhet i kommunal sektor*", og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju hvor det benyttes lydopptaker
- ☐ Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. 15.06.2021

(Prosjektdeltakers navn med blokkbokstaver)

---/---/---
(Sted /dato /prosjektdeltakers signatur)

Vedlegg 5: NSDs godkjenning om at databehandlingen kan starte

Melding
22.01.2021 10:21

Behandlingen av personopplysninger er vurdert av NSD. Vurderingen er:

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 22.01.2021. Behandlingen kan starte.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde:
nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/melde-endringer-i-meldeskjema

Du må vente på svar fra NSD før endringen gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 15.06.2021.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles til nye uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).
NSD vurderer at informasjonen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og eventuelt rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET
NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Kontaktperson hos NSD: Anne Marie Try Laundal
Tlf. Personverntjenester: 55 58 21 17 (tast 1)