God digitalisering

Å bygge inn personvernet – fra politisk visjon til IT-praksis

Stian Gullner Klasbu

Masteroppgave ved

TIK - Senter for teknologi, innovasjon og kultur

UNIVERSITETET I OSLO

Vår 2020

God digitalisering

Å bygge inn personvernet – fra politisk visjon til IT-praksis

Av Stian Klasbu

2020

God digitalisering: Å bygge inn personvern

Masteroppgave, TIK Senter for Teknologi, Innovasjon og Kultur, Samfunnsvitenskapelig fakultet, Universitetet i Oslo

http://www.duo.uio.no

Til Eirik. En god venn og inspirasjonskilde som gikk bort alt for tidlig. Denne oppgaven hadde ikke blitt til uten ham.

Sammendrag

Denne oppgaven handler om hvordan en visjon om et nytt personvern gjøres til lov, og hvordan denne visjonen gjøres til del av infrastruktur, teknologi og organisasjon. Oppgaven tar utgangspunkt i Personvernforordningen, som ble innført i 2018, og undersøker den teknologipolitiske visjonen som gir opphav til forordningen og hvordan loven gjøres til et verktøy for å realisere en visjon om det jeg har kalt for «god digitalisering». I arbeidet med oppgaven har jeg utviklet dette begrepet for å vise frem verdsettingspraksisen som kommer til uttrykk i lovverket og arbeidet med å «bygge inn» personvernet fra visjon til teknologi. Jeg har brukt begrepet «å bygge inn» for å vise hvordan visjonen blir gjort til en del av lov og IT-praksis gjennom oversettelsesarbeid og grensedragninger. På denne måten viser også analysen hvordan en teknologipolitisk visjon for digitalisering utøves og bygges inn i infrastruktur i praksis.

Problemstillingen jeg svarer på i oppgaven er *Hvordan bygges en visjon om et nytt personvern inn i lov og IT-praksis?* For å tilnærme meg dette spørsmålet har jeg fulgt det jeg har kalt en «implementeringskjede», inspirert av Bruno Latours (1999) begrep «oversettelseskjede» og Hilde Reinertsens (2016) begrep «dokumentkjede», fra visjon til «implementering» i en organisasjon og i en digital tjeneste. Jeg starter i EUs lovarkiv, EUR-Lex. Der analyserer jeg dokumentet «A comprehensive approach on personal data protection in the European Union», som jeg har kalt for «visjonsdokumentet», der Europakommisjonen tegner opp en visjon for en ny personvernlovgivning. Deretter gjør jeg en nærlesning av noen av Personvernforordningens artikler. Jeg beveger meg videre til to av forordningens verktøy for å bygge inn visjonen i organisasjoner og teknologi: «Innebygget personvern» og «Prinsippet om ansvarlighet». Datatilsynets veileder «Programvareutvikling med innebygd personvern», sammen med intervju med en av veilederens forfattere er det empiriske hovedfokuset for denne delen. Til slutt analyserer jeg møtet mellom personvernet og en digital tjeneste og en IT-organisasjon: Universitetets senter for informasjonsteknologi, og deres plattform for datainnsamling via internett «Nettskjema».

Jeg har tatt i bruk praksis-orientert dokumentanalyse og kvalitative intervjuer som metodiske verktøy for å besvare problemstillingen. Ved å ta i bruk denne formen for dokumentanalyse har jeg kunnet vise frem den performative funksjonen dokumentene har i å «bygge inn» en visjon i infrastruktur. Oppgaven er skrevet innenfor vitenskap- og teknologistudier (STS), og jeg har tatt i bruk ulike verktøy fra denne tradisjonen. Aktør-

nettverk-teori, verdsettingsstudier og infrastruktur-perspektivet utgjør oppgavens sentrale teoretiske rammeverk.

Forord

Miljøskadet av aktør-nettverk-teori som jeg er, vil jeg understreke at jeg umulig kunne skrevet denne oppgaven uten et stort heterogent nettverk av aktører. Som veileder har Hilde Reinertsen har vært en enorm ressurs og inspirasjon i arbeidet med denne oppgaven. Kjetil Rommetveit har som bi-veileder bidratt med uvurderlige kommentarer. Jeg vil rette en stor takk til Sylvia Irene Lysgåd som stilte opp med gode tilbakemeldinger i oppgavens sluttfase. Takk til Frans for gode innspill og samtaler, og takk til Titti for korrekturlesning. Jeg vil også takke TIK-studentenes masterlesesal og menneskene i den for godt selskap.

En minst like viktig del av nettverket er de som har bidratt med nødvendig omsorgspraksis – for det fortjener de klemmer, heder og ære: En tålmodig kjæreste og støttende venner og familie.

Jeg vil ikke takke covid-19.

Innholdsfortegnelse

1 Innledning

Det er en kjensgjerning at vi i Europa i dag lever i et samfunn gjennomsyret av digital teknologi og digitale nettverk. For de fleste av oss er store deler av dagen viet til digitale flater, og omfanget bare øker. Smarttelefoner, datamaskiner, og i økende grad et hav av dingser, «internett av ting», kobler oss til store nettverk som både gir tilgang til informasjon og som samler informasjon om den enkelte. Slik blir vi både mottakere av og kilde til enorme digitale datastrømmer.

Til tross allestedsnærværet av det digitale, synes det som om sentrale samfunnsinstitusjoner har utfordringer med å forholde seg til og å ta inn over seg digitaliseringen og datafiseringen av samfunnet. Samfunnsvitenskap er intet unntak. Det mangler ikke på mengden av tekst om digitalisering, internett, personvern og overvåkning, men min egen erfaring fra arbeidet med denne oppgaven er at det er langt mellom tekster som mestrer å snakke godt om noen av disse fenomenene.

Den korte beskrivelsen av det moderne digitale liv jeg her gir nærmer seg en klisje, og glir lett inn i en polariserende teknologideterministisk diskurs, enten den heller mot det teknologioptimistiske eller det teknologipessimistiske. Nettopp dette underbygger poenget: Det er så utfordrende å snakke om digitalisering fordi vi befinner oss midt i den, og denne mangelen på distanse, sammen med kompleksiteten i fenomenet, gjør at vi mangler både gode ord og gode beskrivelser for disse fenomenene.

Store teknologiske endringer er ikke noe nytt. Måten den «digitale revolusjonen» beskrives, har ofte et preg av ahistorisk teknologideterminisme. Teknologisk utvikling faller lett inn i kategorier av et iboende onde, gjerne langs en akse mellom menneske og maskin, eller et iboende gode, som en «teknologisk innovasjon». I slike beskrivelser er det som om samfunn og demokrati ikke har noe de skulle sagt i den teknologiske utviklingen: Enten fordi teknologien implisitt tillegges en selvstendig kraft og logikk eller med bakgrunn i et slags teknologisk «laissez-faire»-prinsipp. Ziewitz påpeker at fortellinger om algoritmer og digitalisering har en tendens til å føye seg inn i en reduktiv fortelling som plasserer algoritmene inn i et «ready-made system of conventional politics with its establisth cast of acors and long-standing conserns ablout agency, transparnecy and normativity» (2016, s. 6). Poenget er ikke at denne fortellingen uten videre bør avvises, men digitalisering og algoritmer bør studeres på en måte som ikke tar en slik fortelling for gitt, og som genererer nye forståelser, både av digitalisering og samfunnet.

Jeg startet å skrive denne oppgaven med en sterk interesse for teknologipolitikk, slik Francis Sejersted brukte ordet. Sejersted ønsket å studere relasjonene mellom teknologi og samfunn på en måte som beveget seg utover teknologideterminisme og teknologipessimisme, og utvikle kunnskap som gjør det mulig å ta kontroll over utviklingen (Sejersted, 1998). I denne oppgaven angriper jeg denne tematikken ved å starte med en teknologipolitisk visjon for et nytt lovverk. Hvordan styres teknologi gjennom lov, og hvordan gjøres den styrbar? Et overordnet spørsmål i denne oppgaven er: Hvordan utøves teknologipolitikk gjennom lov?

Da jeg begynte å skrive denne oppgaven hadde nettopp Personvernforordningen - GDPR (General Data Protection Regulation) på engelsk – gjort sin entré, først vedtatt av EU i 2016 og deretter vedtatt som norsk lov og iverksatt i 2018. Personvernforordningen har blitt beskrevet som den mest innflytelsesrike personvernsreguleringen som er laget. Kuner et al. (2017) kaller Personvernforordningen en ny «gullstandard» for personvern, og mange andre land utenfor EU har vedtatt lover inspirert av forordningen.

Europakommisjonen beskriver lovverket som et svar på utfordringer knyttet til innføring av ny teknologi. Personvernforordningen er også en del av en større visjon for digitalisering i EU (jf. Europakommisjonen, 2015). Lovverket går langt i å harmonisere personvernlovgivningen i Europa og tar i bruk nye instrumenter for å verne personopplysninger. Forordningen skal på denne måten sikre grunnleggende rettigheter, knyttet til personvern, for Europas borgere. Samtidig skal forordningen sikre fri flyt av personopplysninger og bidra til å styrke det indre marked (Europakommisjonen, 2010). Personvernforordningen kan på denne måten beskrives som en visjon om å skape det jeg i denne oppgavens tittel har kalt for «god digitalisering»: digitalisering som skal sikre verdiene knyttet til personopplysningers verdi for kunnskapsproduksjon og marked, samtidig som den skal håndtere risiko som behandlingen av personopplysninger utgjør ovenfor borgeres rettigheter. I denne oppgaven undersøker jeg hvordan en slik visjon om «god digitalisering» utøves. Som jeg vil komme tilbake til, har jeg på dette punktet latt meg inspirere av verdsettingsstudier, og mer spesifikt av forskningsprosjektet *Enacting the good econnomy,* ledet av Kristin Asdal og tilknyttet Senter for teknologi, innovasjon og kultur, der denne oppgaven er skrevet.

I perioden jeg skulle bestemme meg for hva jeg skulle skrive oppgave om, var det mye diskusjon om dette nye lovverket som skulle tre i kraft. Lovverket ga opphav til mange offentlige diskusjoner om digital teknologi, personopplysninger og i hvilken forskjell et lovverk fra EU kan gjøre. Disse diskusjonene fanget min interesse, og jeg ble nysgjerrig på relasjonen mellom lov og digital teknologi. Som en med en sterk interesse for digital

teknologi og programmering, undret jeg over hvordan et lovverk for personvern kommer til uttrykk i digitale løsninger, og hvordan lovverket gjøres til en del av praksisen til de som lager disse løsningene. Spesielt begrepet «innebygget personvern» fanget min interesse. Hva betyr dette i praksis? Hvordan «bygges personvernet inn»?

Spørsmålet er både hvordan visjonen bygges inn i lovgivningen og inn i det jeg har kalt IT-praksis. Med dette sistnevnte begrepet mener jeg å inkludere både teknologien, den digitale infrastrukturen og menneskene som arbeider med og utvikler teknologien. For å operasjonalisere spørsmålet har jeg formulert problemstillingen slik:

Hvordan bygges en visjon om et nytt personvern inn i lov og IT-praksis?

For å svare på dette spørsmålet har det vært nødvendig å undersøke flere empiriske steder. Fra visjonen og lovgivningen til «implementeringen» i organisasjon og teknologi. Jeg har tatt i bruk praksis-orientert dokumentanalyse og kvalitativt intervju som metodiske verktøy i innsamlingen og analysen av oppgavens empiri. Analysen har jeg delt inn i tre deler som tar for seg hver sine empiriske steder og empiriske materialer, og på den måten har jeg kunnet følge en konkret kjede.

Denne oppgaven springer ut av STS-fagfeltet (Science and Technology Studies), og jeg har hentet verktøy fra fagfeltet for å besvare problemstillingen. Da jeg begynte å skrive på oppgaven var STS-feltet og disse verktøyene helt nytt for meg, og en viktig motivasjon underveis i oppgaven har vært å undersøke hvordan STS-feltets analytiske verktøy kunne anvendes og komme til nytte i møtet med en slik tematikk. Jeg har spesielt latt meg inspirere av begreper og verktøy fra aktør-nettverk-teori, som jeg vil komme tilbake til i teori-kapitlet. Slik sett har denne oppgaven også vært en utforskning av hvordan disse verktøyene kan anvendes for å studere relasjonen mellom lov og digitalisering.

1.1 Oppgavens struktur og empiri

I oppgavens andre kapittel presenterer jeg oppgavens teoretiske og metodiske tilnærming. Jeg starter med å gjøre rede for aktør-nettverk-teori og de ulike begrepene som jeg har latt meg inspirere av og tar i bruk fra denne tradisjonen. Så gjør jeg redde for de ulike konseptene som utgjør rammeverket for oppgaven, og som jeg vil ta i bruk for å besvare problemstillingen. Deretter beskriver jeg den metodiske tilnærmingen og hvordan jeg har gått frem arbeidet i med oppgaven.

Jeg starter i EUs lovarkiv, EUR-Lex, i første analysekapittel (kapittel 3). Her beskriver jeg først selve arkivet og kjeden av dokumenter som dannes i arkivet. Deretter analyserer jeg dokumentet «A comprehensive approach on personal data protection in the European Union» fra Europa-kommisjonen, som jeg kaller for «visjonsdokumentet». Dette dokumentet er interessant for denne oppgaven ettersom det er her Europakommisjonen tegner opp sin visjon for et nytt europeisk personvern. I tillegg gir dette dokumentet innsikt i den juridiske, byråkratiske og politiske infrastrukturen som ligger «bak» et lovdokument som Personvernforordningen. Til slutt analyserer jeg Personvernforordningen. Jeg trekker spesielt frem artikkel 4 og 5, henholdsvis «Definisjoner» og «Prinsipper for behandling av personopplysninger».

I det andre analysekapitlet (kapittel 4) følger jeg to av Personvernforordningens «verktøy»: Innebygget personvern og prinsippet om ansvarlighet. Datatilsynets veileder «Programvareutvikling med innebygd personvern», samt intervju med en av veilederens forfattere utgjør kjerne-empirien i kapitlet. Jeg analyserer hvordan disse verktøyene forsøker å oversette juridisk praksis til organisasjon og teknologi.

I det siste analysekapitlet (kapittel 5) undersøker jeg personvernet i møte med en digital tjeneste, «Nettskjema» og en IT-organisasjon, USIT, Universitetets senter for informasjonsteknologi. Nettskjema er en «Sikker løsning for datainnsamling via nett» (USIT, u.å.-a), og var i 2018 en av finalistene i Datatilsynets konkurranse for «innebygget personvern i praksis», og utgjør slik sett en interessant «case» for å undersøke hvordan personvernet «bygges inn». Her analyserer jeg hvordan kravene fra personvernet møter IT-praksis, hvordan personvernet gjøres til en del av organisasjon og teknologi.

Kapitlene tre til seks består av oppgavens analysedel som jeg allerede har beskrevet. Jeg avslutter oppgaven ved å oppsummere hovedfunnene mine og svarer på problemstillingen. Jeg gjør også noen refleksjoner rundt arbeidet med oppgaven og hvordan denne tematikken kan studeres videre.

2 Teoretisk og metodisk tilnærming

I dette kapitlet vil jeg vise frem de teoretiske perspektivene og begrepene jeg har hentet fra STS-feltet, før jeg beskriver hvordan den metodisk tilnærmingen jeg har tatt i bruk og hvordan jeg har gått frem for å besvare oppgavens problemstilling. Det er ofte en glidende overgang mellom teori og metode i STS, og det er også tilfellet i dette kapitlet. Jeg har likevel forsøkt å dele kapitlet i to deler for å gjøre materialet mer oversiktlig.

2.1 Teoretisk tilnærming

Jeg har spesielt hentet ressurser og inspirasjon fra aktør-nettverk-teori (ANT), og denne tilnærmingen utgjør en viktig del av mitt blikk i møte med oppgavens empiri. Derfor vil jeg starte med å trekke frem noen viktige trekk ved ANT som har hatt innvirkning på analysen.

2.1.1 Aktør-nettverk-teori

ANT har sitt utgangspunkt innenfor vitenskap og teknologi-studier, og kan beskrives som en samling av verktøy, sensibiliteter og metoder (Law, 2007). ANT rettet fokuset mot relasjoner i nettverk, og betraktet kunnskap som et resultat av relasjonene, sammensetningen og arbeidet i heterogene nettverk heterogene nettverk av både mennesker og ting. John Law kaller skapelsen av slike nettverk for heterogen konstruksjon (heterogenous engineering) og ser slike nettverk som sentralt ved ANTs måte å betrakte verden:

> [The metaphor of heterogenous networks] lies at the heart of actor-network theory, and is a way of suggesting that society, organisations, agents and machines are all effects generated in patterned networks of diverse (not simply human) materials" (Law, 1992, s. 2).

Slike nettverk er altså ikke bare et kjennetegn ved kunnskap, men også en rekke andre sosiale fenomener. Sett med ett ANT-blikk, er det gjennom ordningen, relasjonene og arbeidet som gjøres i slike nettverk av ting og mennesker som gjør muliggjør handlinger.

På denne måten fremhever også ANT tingene og teknologienes rolle. Samtidig motsetter ANT seg både teknologisk og sosial reduksjonisme eller determinisme. Det antas ikke at det ene driver det andre, eller det ene kan reduseres eller utelukkende forklares av det andre. Sosiale relasjoner kan gi opphav til teknologi, og i enkelttilfellet kan teknologi skape sosiale relasjoner, men dette kan ikke antas *a priori*, det er et empirisk spørsmål (Law, 1992). Fra ANTs perspektiv er dermed heller ikke «det sosiale» og «det tekniske» separate, men to sider av samme sak.

Begrepet «translasjonssosiologi» eller «oversettelsessosiologi»[1] brukes ofte synonymt med ANT. Latour beskriver en *oversettelsesskjede* som «the work through which actors modify, displace, and translate their various and contradictory interests» (Latour, 1999, s. 311). For Latour er oversettelser av interesser et sentralt studieobjekt for i ANT, og slike oversettelser innebærer ofte både mennesker og ting. Latour bruker en fartsdump som eksempel på en bestemt oversettelseskjede. Fartsdumpen kan beskrives som *programmet* «å få bilister til å senke farten i skoleområdet» *artikulert* i asfalt. Latour kaller dette for en *delegering*: fartsdumpen *står inn for* ingeniørene eller politiet, og dermed har selve uttrykket for interessen endret materialitet. «Program» referer her til det Latour kaller for et *handlingsprogram*, det vil si et sett av mål, steg og intensjoner som settes sammen til en fortelling, altså en formulering av aktørens interesser. Latour bruker begrepet *artikulering* i stedet for «materialisert» eller «tingliggjort» for å understreke at vi har å gjøre med en samhandling. Det er ikke *egentlig* ingenørene, politiet eller loven som utøver målet om å få bilistene til å senke farten, og det er heller ikke fartsdumpen som gjør dette på egenhånd, det er nettverket av aktører som muliggjør handlingen (Latour, 1999, s. 178–187).

I sin klassiske artikkel om domestisering av kamskjell, tar Michel Callon (1984) i bruk noen begreper som også kan relateres til Latours beskrivelse over. I artikkelen beskriver Callon en gruppe forskeres forsøk på å etablere en ny form for kamskjellsoppdrett i Frankrike. Callon beskriver dette som en oversettelsesprosess. For denne oppgavens vedkommende, vil jeg trekke frem tre begreper som Callon bruker i sin analyse.

> [The researchers] determined a set of actors and defined their identities in such a way as to establish themselves an obligatory passage point in the network of relationships they were building. This double movement, which renders them indispensable in the network, is what we call problematization. (Callon, 1984, s. 6)

Callon bruker altså begrepet *problematisering* for å beskrive prosessen der en aktør - i dette tilfellet forskerne - definerer et nettverk av aktører og forbindelsene mellom dem. Parallelt tegnes dette nettverket opp på en slik måte at forskerne er uunnværlige for programmet som tegnes opp. De utgjør dermed det Callon kaller for *obligatorisk passasjepunkt*. For at en slik problematisering skal bli vellykket, må aktørene *innrulleres* inn i de rollene som er blitt tegnet opp. Det er nemlig ikke gitt at aktørene uten videre aksepterer disse rollene, aktørene kan «kjempe mot» programmet, og det må ofte «forhandlinger» til for å gjennomføre programmet (Callon, 1984, s. 10–11).

[1] Heretter i oppgaven bruker jeg «oversettelse» i stedet for «translasjon».

ANT har et ikke-essensialistisk og prosess-orientert perspektiv. Fakta er ikke noe som allerede finnes ferdig «der ute», men noe som blir til som en del av og i interaksjon med ulike kunnskapspraksiser (Law, 2004, s. 31). Ulike kunnskapspraksiser kan også skape ulike, og ofte omstridte objekter. I *The Body Multiple* beskriver Annemarie Mol (2003) for eksempel om hvordan ulike versjoner av åreforkalkning «utøves» på ulike avdelinger på et sykehus. Heller ikke objekter er der allerede som «ferdige pakker», men blir *utøvet* gjennom ulikepraksiser og i samspill med nettverk av mennesker og ting.

Madeleine Akrich beskriver det hun kaller for teknologiske «script». Det er ikke bare teknologier som lager inskripsjoner. Også teknologier er inskribert med bestemte forestillinger om verden, og implisitte antagelser om teknologiens brukere. Ofte legger teknologiens designere føringer for hvordan teknologien skal brukes og hvem som er teknologiens brukere. Det er ikke dermed sagt at teknologiens brukere nødvendigvis inntar den rollen de blir tillagt, brukeren kan «avvise» skriptet eller lage sitt eget antiprogram (Latour, 1999), altså bruke teknologien på en annen måte enn tiltenkt.

2.1.2 Politiske teknologier og politikkens teknologier

Personvernsforordningen er ikke bare juridisk, den er også politisk. Med et ANT-blikk blir det imidlertid tydelig at politikk og teknologi vanskelig lar seg skille fra hverandre. I denne oppgaven kommer også det helt konkret til uttrykk når politikken – i klassisk forstand, uttrykt gjennom lov – skal bygges inn i teknologien.

Asdal bruker begrepet «politikkens teknologier» for å betegne de teknologier som tas i bruk innen politikk: «Dette er teknologier som til dels er strategier for å styre (direkte eller indirekte) *over* en befolkning, ting og områder. Men dette er også strategier for å styre *med*, for å muliggjøre deltagelse og det å samle og sannsynliggjøre sammenhenger og realiteter» (Asdal, 2011, s. 211, min uthevelse). På denne måten anlegger Asdal et perspektiv på politikk som fremhever teknikker og praksiser for å styre, fremfor å kun fokusere på overtalelse, som har vært vanlig innen klassiske politiske analyser. Politikkens teknologier er ikke rent instrumentelle verktøy som tas i bruk for å oppnå forhåndsdefinerte formål. Politikk kan ikke reduseres til klart definerte intensjoner som påføres ovenfra og ned. Den blir til i et samspill mellom en rekke ulike aktører, inkludert politikkens ting, slik som dokumentene som analyseres i denne oppgaven.

Asdal bruker også begrepet «styringspraksiser» for å betegne praksisene slike teknologier inngår i. Måten Asdal bruker dette begrepet er inspirert av både Foucault,

samtidig som det bygger videre på ANT (Asdal, 2011, s. 215). Foucault brukte begrepet governmentalité blant annet for å beskrive en historisk endring i synet og utøvelsen av styring, og de teknikker som gjør det mulig å utøve denne spesifikke formen for makt (Foucault, 2007, s. 108). I Foucaults maktanalyse er det ikke mulig å skille det som muliggjør styringen, dets teknikker og diskurser, fra styringen selv. Foucault kritiserte tradisjonelle politiske analyser for å utelukkende fokusere på institusjoner og staten. I stedet mente han at et fokus på styringspraksis og styringsteknologier er mer fruktbart: «Det handler om styringspraksiser i form av det vi kunne kalle statens lange arm; kunnskapspraksiser som strekker seg utover og fanger og former forvaltningsobjekter» (Asdal, 2011, s. 216–217). Også ANT har interessert seg for styring. John Law tar i bruk begrepet «handling på distanse» for å beskrive teknologier som muliggjør styring på avstand (Law, 2015). Denne tradisjonen har imidlertid hatt et større fokus på materielle praksiser fremfor rent diskursive eller språklige aspekter som ofte assosieres med Foucault-inspirerte studier (Asdal, 2011, s. 218).

2.1.3 Juridiske teknologier

Lov kan ses som en av politikkens teknologier. Asdal og Druglitrø (2017) beskriver loven som en moralsk teknologi, inspirert av Foucault. Foucault (1991) brukte begrepet i sin historiske studie av avstraffelse, og var interessert i hvordan ulike kunnskapspraksiser har bidratt til og interagert med ulike regimer for avstraffelse. Asdal og Drulitrø undersøker hvilken rolle lov har spilt i å skape relasjoner og grenselinjer mellom mennesker og dyr, og viser hvordan slike relasjoner blir skapet gjennom en rekke lov-praksiser. I relasjon til personvern kan loven også i denne oppgaven ses som en moralsk teknologi i den forstand at det dras opp nye grenselinjer for hva hvilke opplysninger som skal vernes, og hvordan de skal vernes.

I *The Making of Law* gjør Latour (2009) en etnografisk studie av det franske rettsapparatet og fremhever dokumentenes sentrale rolle i juridisk praksis (mer spesifikt Conseil d'État). I artikkelen «Making Order», beskriver Jasanoff (2008) rollen vitenskap har i møtet med Rettssystemet. Denne oppgaven tar en annen tilnærming. I stedet for å undersøke rettssystemet har jeg studert loven som teknologi ved å undersøke hvordan loven blir anvendt, oversatt og bygget inn i et annet praksisfelt. Fra min litteraturgjennomgang synes det som det har vært gjort lite studier av denne typen, og jeg mener derfor min oppgave også på denne måten kan være et bidrag til STS-feltet.

2.1.4 Infrastruktur og infrastrukturering

I visjonsdokumentet fra Europakommisjonen, som jeg beskriver i analysen, kommer det frem at det som skal bli til personvernsforordningen kommer som et svar på teknologiske utviklinger og økt flyt av informasjon. I dag foregår behandlingen av personopplysninger først og fremst gjennom ulike digitale informasjonsteknologier og IT-organisasjoner. Dette er derfor et sentralt objekt for Personvernforordningen. I denne oppgaven ser jeg denne sammensetningen, og objektet for Personvernforordrningen som informasjonsinfrastruktur. Begrepet brukes innen studier av informasjonssystemer for å betegne sammensetningen av slike komplekse heterogene nettverk, inspirert av aktør-nettverk-teori (Geirbo, 2017, s. 7). USIT og deres nettskjema, både bygger på og utgjør en utgave av denne infrastrukturen. Som jeg vil komme tilbake til, kan også loven ses som en del av en juridisk infrastruktur.

Geoffrey Bowker og Susan Leigh Star (1999) har utviklet analytiske verktøy for å studere infrastrukturer, og viser samtidig hvorfor infrastrukturer er et utfordrende studieobjekt. Når en infrastruktur fungerer godt, blir den nærmest per definisjon usynlig, og ofte blir de også vanskeligere å få øye på jo større de er. Det er ofte først når infrastrukturen bryter sammen, at vi blir bevisst infrastrukturen og dens funksjoner. (Bowker & Star, 1999, s. 33). Å se og forstå infrastruktur krever ofte egne ekspertiser, og jo mer de skalerer opp, jo vanskeligere er de å forstå for utenforstående, til tross for at vi ofte står midt i dem.

Bowker og Star ser infrastrukturer som en type klassifiseringssystem. Sortering, kategorisering og standardisering er alltid involvert i infrastrukturer. Kategorisering gjør på den ene siden aktivt arbeid ved å dele opp. På den andre siden bidrar standardisering til å få infrastrukturen til å henge sammen, og muliggjør skalering av infrastruktur (Bowker & Star, 1999, s. 10, 13–14).

En infrastruktur er ikke en isolert entitet som vokser ut av ingenting, de er innkapslet i andre praksiser, sosiale og teknologiske, som igjen er bygget på toppen av andre infrastrukturer. Infrastrukturen «arver» begrensinger, styrke og inerti fra allerede eksisterende infrastrukturer. Bowker og Star kaller dette for installert base («installed base») (Bowker & Star, 1999, s. 35). Slike infrastrukturer holdes ikke oppe av seg selv. Det krever store mengder med arbeid for å opprettholde infrastrukturer, både av menneskelige og ikke-menneskelige aktører. Selv om infrastrukturen ofte kan forsvinne ut av syne, er den på ingen måter

«uskyldig», og har ofte store konsekvenser for hvordan vi lever livene våre (Jf. Bowker og Star (1999) om helsemanualer og Edwards (2010) om klimamodeller).

Bowker og Star tar i bruk det de kaller «infrastrukturell inversjon» («infrastructural inversion»). Deres metode og perspektiv forsøker å synliggjøre infrastrukturen og få frem arbeidet og praksisen som ligger til grunn for infrastrukturen: «Infrastructural inversion means recognizing the depths of interdependence of technical networks and standards, on the one hand, and the real work of politics and knowledge production on the other» (Bowker & Star, 1999, s. 34).

Infrastruktur, slik Bowker og Star bruker begrepet, minner om heterogene nettverk og heterogen konstruksjon. Selv om Bowker og Star ikke selv bruker dette begrepsapparatet, anser jeg i denne oppgaven infrastrukturer som en spesifikk type heterogent nettverk. Altså et heterogent nettverk av materialiteter som har de egenskapene som beskrevet ovenfor.

Hanne Cecilie Geirbo (2017) bruker begrepet «infrastrukturering» («infractructuring») for å betegne arbeidet og praksisen som er involvert i å skape og opprettholde infrastrukturer. I likhet med Geirbo bruker jeg i denne oppgaven dette begrepet for å fokus på praksis-aspektet ved skapelsen av infrastrukturer (Geirbo, 2017, s. 2).

I oppgaven har jeg brukt begrepet «å bygge inn» for å beskrive prosessen der nye praksiser forsøksvis gjøres til en del av en allerede eksisterende infrastruktur. Begrepet tar utgangspunkt i konseptet «innebygd personvern», som har sin egen artikkel i Personvernforordningen, og som naturligvis spiller en hovedrolle i Datatilsynets «Programvareutvikling med innebygd personvern». Jeg har slik sett brukt begrepet som et sensitiverende konsept, altså et begrep fra oppgavens empiri som også brukes som et analytisk begrep (van den Hoonaard, 2008). «Å bygge inn» er beslektet med infrastrukturering fordi det handler om praksisen i dannelse og modifikasjon av infrastruktur, men «å bygge inn» peker eksplisitt mot å bygge inn ny praksis, og utgjør slik sett en intervensjon i infrastrukturen.

2.1.5 Verdsetting og «god digitalisering»

Verdsettingsstudier («valuation studies») er et relativt nytt felt som har sitt opphav mellom økonomisk sosiologi og STS. Studier av verdi er ikke noe nytt, men verdsettingsstudier forsøker, i likhet med dokumentanalyse, å nærme seg verdier fra et mer pragmatisk og praksis-orientert perspektiv. Denne tilnærmingen til verdier er inspirert av John Deweys filosofi, som bidro til en pragmatisk vending innen studier av verdsetting gjennom den tidligere nevnte «flanke-manøveren» (Muniesa, 2011). I tråd med sin pragmatistiske filosofi

mente Dewey at verdier verken finnes i tingene i seg selv (realisme) eller kun er noe som tilskrives dem (idealisme). Verdier oppstår derimot i møtet mellom de som tilskriver og tingene selv. I stedet for å bli stående fast i kontroversen mellom realisme og idealisme, foreslår Dewey en «flankemanøver» (Dewey, 1913, s. 268). Denne flankemanøveren innebærer å angripe fra en annen side, et skifte fra verdi som iboende eller tilskrevet, til verdsetting som handling (Muniesa, 2011, s. 25). I verdsettingsstudier blir verdi sett som noe som aktivt gjøres, og en bestemt form for praksis (Asdal, 2015a, s. 170; Muniesa, 2011). Denne praksisorienterte tilnærmingen åpner også opp for en mer agnostisk innstilling til hva verdi er og hvor verdsetting gjøres: «Valuation denotes here any social practice where the value or values of something are established, assessed, negotiated, provoked, maintained, constructed and/or contested» (Doganova et al., 2014, s. 87). Økonomisk verdi har vært verdsettingsstudiers primære objekt, men verdsetting kan altså også inkludere andre former for verdsetting av kvaliteter, slik som estetisk eller moralsk verdsetting. Dette perspektivet åpner også opp for å se økonomi som et mangefasettert fenomen som skapes av og i forskjellige praksiser, i stedet for «økonomien» som én enkelt entitet, med én bestemt iboende logikk (Asdal, 2015a, s. 173). Som vi skal se er også dette poenget relevant for mitt materiale.

Inspirert av verdsettingsstudier, har jeg utviklet begrepet «god digitalisering». Ordet «god» brukes ikke eksplisitt i oppgavens empiri, men er ment som en analytisk prisme for å få tak i de verdsettingspraksisene som tas i bruk i oppgavens materiale. På denne måten operasjonaliserer jeg verdsettingspraksisene gjennom et analytisk begrep. Denne bruken av «god» er inspirert av forskningsprosjektet «Little Tools: Enacting the good economy» (Asdal et al., 2019) og Charis Thompsons (2013) bok «Good Science: The Ethical Choreography of Stem Cell Research». Bruken av ordet i denne oppgaven peker ikke bare på «god» i en moralsk forstand, men også i en økonomisk og funksjonell forstand, som noe som skal skape verdi og skape noe godt og noe som skal fungere godt. Denne måten å bruke begreper på passer inn i en tradisjon i STS for å bruke språk som analytisk verktøy.

2.1.6 Personopplysninger som risiko

Denne oppgaven tar for seg noen ganske forskjellige studieobjekter: et «visjonsdokument», en lov, arkivet der loven og visjonsdokumentet befinner seg, en veileder og en digital tjeneste for innhenting av opplysninger. Noe av det som alle disse har til felles er at de alle, om enn på ulike måter, tar for seg eller utfører behandling av personopplysninger. Som jeg har vært inne på, kommer Personvernforordningen som en reaksjon på en teknologisk utvikling som

medfører en økt spredning av personinformasjon. Personvernforordningen kan slik sett også ses som en måte å håndtere risikoen knyttet til denne utviklingen. I oppgavens analyse vil jeg vise hvordan behandlingen av personopplysninger kan ses som det Stephen Hilgartner (1992) kaller for et risiko-objekt.[2]

Konseptuelt består risiko av tre komponenter: et objekt som «utgjør» en risiko, en antatt skade og en kausal forbindelse mellom objektet og skaden (Hilgartner, 1992, s. 40). Hilgartner argumenterer for at denne strukturen skapes, og at akkurat hvordan den settes sammen er kontingent og må analyseres. Ofte er også konstruksjonen av forbindelsen mellom objektet og antatt skade tett forbundet med selve artikulasjonen av objektet. «Objekt» brukes her i en ikke-essensialistisk forstand, altså ikke som et objekt som allerede finnes «der ute» som en ferdig artikulert enhet, men som objekt som kontinuerlig artikuleres og skapes. Risiko kommer sjelden alene knyttet til et objekt, men er knyttet sammen med mange ulike objekter i nettverk av risiko-objekter.

Hilgartner ser utviklingen av et slikt nettverk som en retorisk prosess, og som i det postindustrielle samfunnet ofte gjøres av spesialiserte tekster og organisasjoner som knytter sammen ulike objekter og risiko (Hilgartner, 1992, s. 46). Det er ofte tekniske eksperter som spiller den viktigste rollen i utformingen og opprettholdelsen av risiko-objekter. Han oppfordrer derfor forskere som studerer risiko til å undersøke de stedene der slike spesialister arbeider, heller enn offentligheten og media, der risiko ofte er blir studert. I denne oppgaven utgjør dokumentene som jeg analyserer, nettopp slike spesialiserte tekster som gjør et retorisk arbeid. Hilgartner peker også spesifikt på lov og regulering som områder som kan spille en viktig rolle i artikulasjonen av risiko-objekter. Som jeg vil vise, spiller dokumentene jeg analyserer alle viktige roller i utformingen og modifikasjonen av behandling av personinformasjon som risiko-objekt.

Ofte skjer utformingen av risiko-objektene parallelt og i samspill med kampen om å kontrollere risiko. Hilgartner viser hvordan det bygges et «kontrollnettverk» rundt risikoobjektene: et sosioteknisk nettverk bestående av et stort antall heterogene aktører, og tar i bruk John Laws begrep heterogen konstruering for å vise hvordan et slikt nettverk bygges (48).

Artikuleringen av risikoobjektene har også implikasjoner for hvem som har ansvar, plikt og rett til å gjøre noe med risikoen som objektene utgjør (Hilgartner, 1992, s. 47). Ved å

[2] Hilgartner (1992) bruker begrepet «risk objects». Andre forskere innenfor STS-feltet bruker senere begrepet «risky objects» (Latour, 2004, s. 256; Marres, 2007, s. 762).

ta i bruk dette teoretiske og metodiske apparatet som tar utgangspunkt i aktør-nettverk-teori, kan nettverket av risiko åpnes opp. Formålet er å undersøke hvordan risiko skapes, kontrolleres og distribueres (Hilgartner, 1992, s. 52).

Hilgartner beskriver ulike strategier for å håndtere risiko-objekter. En kan forsøke å plassere inn objektene inn i det sosiotekniske nettverket eller forsøke å flytte objektene ut av nettverket. Å flytte inn objektene innebærer å modifisere nettverket slik at risiko-objektet kan bli en del av nettverket. Å flytte objektene ut vil si å fjerne objektene eller nøytralisere forbindelsen mellom objektet og skade, slik at objektet ikke vil ha noen innvirkning på det sosiotekniske nettverket (Hilgartner, 1992, s. 48–49).

2.1.7 Digitalisering og algoritmer

De senere årene har det vært et økende fokus på «det digitale» innenfor STS. I introduksjonen til *digitalSTS: A field Guide for Science and Technology Studies*, beskriver forfatterne digital STS, ikke som et nytt felt, men som en utvidelse av STS (Vertesi et al., 2019). STS har et stort sett av verktøy som er godt egnet til å møte kompleksitet og endring. «Det digitale», både som studie objekt og som metode, skaper likevel nye utfordringer og krever nye tilnærminger. Forfatterne påpeker også at STS har vært trege til å ta i bruk nye teknikker i møte med digitale objekter og digital metode.

«Det digitale» er et sentralt tema i denne oppgaven. Når Europakommisjonen beskriver behovet for et nytt lovverk for personvern, pekes det mot digital teknologi (først og fremst i form av internett-teknologier) som den viktigste årsaken. Samtidig er også arkivet som loven befinner seg i og dokumentene jeg undersøker digitale. Digitalisering og digital teknologi er slik sett allestedsnærværende i oppgavens.

Algoritmer har innen samfunnsvitenskapen ofte blitt tilnærmet som en mystisk og mektig svart boks. Ziewitz (2016) kaller dette for et algoritmisk drama: en forførende fortelling om en mektig og ukjent aktør som blir satt inn i et allerede etablert språk om agens, gjennomsiktiktighet og normativitet. «There also is a striking similarity between algorithms and the language of politics, which tends to privilege the figure of the lone decision maker at the expense of more complex realities» (Ziewitz, 2016, s. 6). Dette algoritmiske dramaet blir altså reduktivt og konservativt i sin måte å tilnærme seg algoritmen som studieobjekt. Ziewitz sier ikke at dette bildet skal avvises, men at det bør nyanseres. Algoritmer bør tilnærmes som et analytisk objekt på en måte som åpner opp for en produktiv og rik analyse. Ziewitz foreslår

derfor å bruke algoritme som et sensitiverende konsept, og på den måten være åpen for hvordan begrepet brukes og utøves, heller enn å operere med en ferdig definisjon.

I artikkelen «Knowing algorithms» påpeker Nick Seaver (2019) at det ofte ligger en stor mengde tolkningsarbeid bak for å oversette de karakteristikkene man er interessert i inn i algoritmen. Algoritmene som samfunnsvitere er interessert i er sjeldent «enkle» algoritmer, slik de blir definert innen informatikk. De er derimot det Seaver kaller for «algoritmiske systemer»: intrikate, dynamiske arrangementer av mennesker og kode.

> These algorithmic systems are not standalone little boxes, but massive, networked ones with hundreds of hands reaching into them, tweaking and tuning, swapping out parts and experimenting with new arrangements ... We need to examine the logic that guides the hands, picking certain algorithms rather than others, choosing particular representations of data, and translating ideas into code (Nick Seaver, 2019, s. 419).

Seaver argumenterer altså for at algoritmene bør ses i sammenheng med et større nettverk, og det tolkningsarbeidet og oversettingsarbeidet som inngår i det algoritmiske systemet. I denne oppgaven er Personvernet en slik «logikk» som potensielt leder hendene.

2.1.8 «Accountability»

«Accountability» er en annen tematikk som har vært utforsket innen STS som er relevant for denne oppgaven. I denne oppgaven kommer «accountability» direkte til uttrykk i Personvernforordningens «prinsipp om ansvarlighet». «Accountability» blir ofte oversatt til norsk som «ansvarlighet», og i Personvernforordningen, men mange nyanser forsvinner i denne oversettelsen. Ordet har sitt opphav i betydningen «state of being answerable» («Accountability», u.å.). Begrepet har sammenheng med en moralsk forpliktelse til å svare og den praktiske evnen til å gi svar. Kravet om å være «accountable» innebærer slik sett både et moralsk og et praktisk aspekt (Hogle, 2019). «Accountability» knyttes til retorikk om åpen styring, og i økende grad gjøres dette gjennom digitalisering (Hoeyer et al., 2019, s. 463). Hoyer et al. foreslår å studere «accountability» ved å åpne opp det de kaller for «accountability assemblages»: «arrangements of practices, technologies, and theories that configure action in a sociotechnical space» (Hoeyer et al., 2019, s. 460). Dette gjør de ved å stille spørsmål ved hva som teller og hva som skal telles, eller dokumenteres, og for hvem. Alison Cool (2019) har også studert «accountability» i relasjon til Personvernforordningen. Cool viser hvordan kravene fra Personvernfordningens, med fokus på prinsippet om ansvarlighet, skaper usikkerhet og bekymring for forskere som blir underlagt reglene. Denne empirien minner om min egen empiri, men der kravene fra Personvernforordningen også

møter en ekspertgruppe: utviklerene. I «Following the algorithm: How epidemological risk-scores do accountability» undersøker Amelang og Bauer (2019) hvordan «accountability» gjøres gjennom et sett av algoritmer som forsøker å predikere helserisiko. Også i denne oppgaven møtes algoritmer og accountability, men som vi skal se brukes «accountability» også som et verktøy for å oversette personvern inn i IT-praksis.

2.2 Fremgangsmåte og metodiske verktøy

Da jeg startet arbeidet med denne oppgaven visste jeg at jeg ønsket å undersøke Personvernforordningen, og hvordan et «nytt personvern» blir gjort til del av IT-praksis. Utover det visste jeg ikke hva som skulle utgjøre mitt datamateriale og hvilke metoder jeg skulle ta i bruk. Det ble raskt tydelig at det ville gi en bedre innsikt i fenomenet jeg ønsket å undersøke, dersom jeg kunne studere flere steder og ulike empiriske materialer. Jeg har hatt en utforskende og åpen innstilling til mitt empiriske materiale, noe som har gjort at utvalget av empiri som til slutt har blitt en del av oppgaven og tilnærmingen til denne empirien har blitt til underveis. Dette er også karakteristisk for studier innen STS og ANT (Skjølsvold, 2015, s. 71). Jeg starter denne delen med å beskrive hvordan jeg har gått frem og hvordan oppgaven har blitt til.

2.2.1 Fremgangsmåte

Da jeg hadde bestemt meg for at jeg ønsket å undersøke den nye Personvernforordningen og hvordan personvern bygges inn i teknologi, stod jeg ovenfor en utfordring: Hvordan skulle jeg tilnærme meg et så stort område? På den ene siden utgjør juss og juridiske tekster om personvern et enormt felt som jeg hadde begrenset innsikt i, og på den andre siden angår personvern absolutt alle som kan tenkes å skulle håndtere enhver form for personinformasjon. Min løsning på utfordringen var å konsentrere meg om et lite knippe ulike «steder» som alle var knyttet til hverandre og bygger på hverandre i det som kan kalles en implementeringskjede. På den måten ønsket jeg å følge en konkret kjede fra visjonen om et nytt personvernregime til en konkret anvendelse av dette personvernregimet i en teknisk løsning. Min løsning på utfordringen var å undersøke et lite knippe steder som er relatert til hverandre i det som jeg vil kalles en «implementeringskjede», som i dette tilfellet er et knippe av steder som leder fra visjonen om et nytt europeisk personvern til implementeringen av personvern i en konkret digital løsning. Her tok jeg inspirasjon fra Hilde Reinertsens begrep «dokumentkjede», som jeg straks kommer tilbake til. På denne måten ønsker jeg å kunne vise

hvordan en slik politisk og juridisk personvern gjennom en rekke oversettelser til slutt blir til konkrete utøvelser av personvern i teknologi og organisasjon. Det må imidlertid med en gang understrekes at den kjeden jeg til slutt valgte ut, på ingen måte er så lineær og ukomplisert som det her kan virke som. Det er jeg som forsker som har *valgt ut* akkurat denne kjeden av steder og viser frem forbindelsene mellom akkurat disse. Det tok dessuten lang tid å bestemme meg for at det var akkurat *disse* stedene jeg skulle fokusere på og trekke forbindelser mellom.

Personvernforordningen utpekte seg umiddelbart som stedet jeg ville begynne, ettersom forordningen utgjør kjernen i EUs nye personvernregime. Da jeg begynte å lese Personvernforordningen opplevde jeg den som ugjennomtrengelig. Det var vanskelig å forstå hva disse abstrakte formuleringene egentlig betydde. Derfor begynte jeg å undersøke tidligere dokumenter i beslutningsprosessen som ledet frem til forordningen. Dette gjorde jeg både for å forstå forordningen bedre, og for å forstå hvordan den ble til. Et stort antall dokumenter er relevante i dette henseendet, men et dokument som utpekte seg som sentralt, var Europakommisjonens dokument «A comprehensive approach on personal data protection in the European Union» (2010). Her beskriver Europakommisjonen utfordringene knyttet til personinformasjon på daværende tidspunkt, og hvordan de mener at EU bør løse disse problemene. De tegner slik opp en visjon for et nytt personvern-lovverk. Jeg valgte å analysere dette dokumentet fordi det gir innsikt i argumentene Europakommisjonen tar i bruk for hvorfor de mente det var behov for en ny personvernlovgivning, og hvordan kommisjonen tegner opp denne visjonen.

Når jeg oppsøkte andre lovdokumenter knyttet til personvern og prosessen som ledet frem til Personvernforordningen, ble jeg oppmerksom på at alle slike dokumenter befant seg i EUR-Lex, EUs arkiv for lover og dokumenter knyttet til EUs beslutningsprosesser. Med blikket for steder, teknologier, praksiser og forbindelser fra ANT, ble jeg bevisst arkivet som stedet der dokumentene kunne utspille sin rolle, og jeg ble interessert i hvilken rolle arkivet selv hadde i utøvelsen av lovverket. Derfor bestemte jeg meg for å også beskrive arkivet som et sted, og den rollen som arkivet selv spiller.

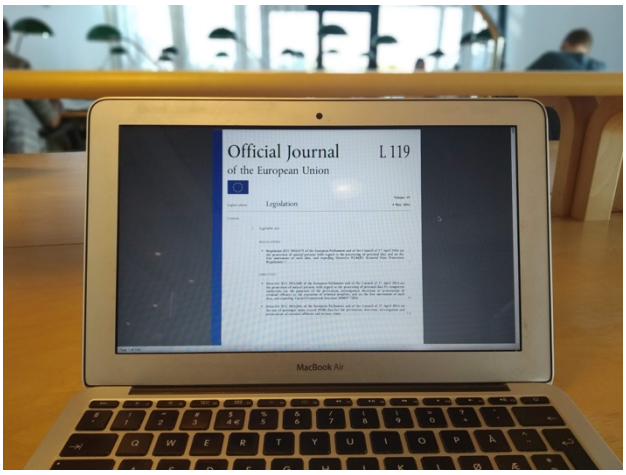
Fordi jeg nettopp ønsket å undersøke det jeg har kalt en «implementeringskjede» - hvordan personvern går fra visjon, til lov og deretter blir til en del av en digital plattform - ble jeg raskt interessert i Personvernforordningens begrep «innebygd personvern». For å finne ut mer om dette oppsøkte jeg Datatilsynet i Norge. Datatilsynet er et norsk offentlig kontrollorgan, med personvern som ansvarsområde («Datatilsynet», 2019). Deres oppgave «er å føre kontroll med personvernregelverket og medvirke til at enkeltpersoner ikke blir krenket

gjennom bruk av opplysninger som kan knyttes til dem» (Datatilsynet, u.å.-b). De hadde nylig gitt ut en veileder om innebygd personvern for programvareutvikling (Datatilsynet, u.å.-c), og denne pekte seg ut som en relevant for oppgaven. I tillegg hadde de hatt en konkurranse for «innebygd personvern i praksis». En av finalistene i konkurransen var USIT, med deres løsning for innsamling av informasjon, primært for forskere, «Nettskjema». Jeg er selv hobby-utvikler, og har derfor også tatt i bruk min egen kompetanse og forståelse knyttet til programmering og utvikling i analysen av USITs Nettskjema.

I Datatilsynet gjennomførte jeg intervjuer med to ansatte som hadde arbeidet med veilederen, og som ville stille opp til intervju. I USIT intervjuet jeg en utviklingsleder. I tillegg ønsket jeg å snakke med noen av utviklerne som jobbet med programmering i Nettskjema, eller utført deltagende observasjon på noe av arbeidet eller møteaktiviteter, men dette forslaget ble avslått. Senere intervjuet jeg en jurist som hadde arbeidet med personvern hos USIT. Ikke alle disse intervjuene har blitt med i empirien som jeg presenterer eksplisitt i oppgaven. De har likevel vært med på å informere og forme analysen.

2.2.2 Å studere dokumenter

Som det kommer frem i beskrivelsen av fremgangsmåten over, utgjør dokumenter en sentral del av oppgavens empiri. Dokumentene som jeg har analysert kan grovt sett deles inn i to typer: offentlige dokumenter og nettsider. Denne distinksjonen er imidlertid ikke så tydelig som den umiddelbart kan fremstå som. Alle de offentlige dokumentene er digitale, og flere av dem presenteres også som nettsider. Som jeg vil komme tilbake til i oppgaven, er de ikke bare digitale i den forstand at de *også* finnes i digitale utgaver, men at de er bygget inn i digital infrastruktur. For å studere disse dokumentene har jeg tatt i bruk ressurser fra praksis-orientert dokumentanalyse. Ettersom praksis-orientert dokumentanalyse spiller en så sentral del av denne oppgavens tilnærming, vil jeg først presentere denne formen for dokumentanalyse, og deretter knytte den til oppgavens empiri.



Figur 1 Digital dokumentanalyse i praksis – General Data Protection Regulation i Official Journal of the European Union

I arbeidet med oppgaven har jeg ønsket å vise frem dokumentene som en del av et større praksisfelt, og som samtidig er med på å skape og moderere bestemte objekter og

praksiser. Dokumentene er ikke bare en kilde til informasjon om EUs personvern, de er også handlende dokumenter som er med på å utøve en bestemt versjon av personvernet. For å anvende et slikt praksis-orientert og ANT-inspirert blikk, har jeg tatt i bruk praksis-orientert dokumentanalyse.

Praksis-orientert dokumentanalyse er en tverrfaglig tilnærming til studiet av dokumenter, som kombinerer innsikter fra STS, historisk metode og hermeneutikk (Asdal & Reinertsen, 2020)[3]. Asdal og Reinertsen viser hvordan dokumenter kan være studieobjekter på flere ulike måter, ikke bare som inngang til det en egentlig vil studere, men også som interessante studieobjekter i seg selv. Dokumenter er ikke bare tekst om noe og objekter som kan studeres, dokumenter kan også være med på å aktivt transformere og modifisere virkeligheten de er en del av (Asdal, 2015b). På denne måten er dokumenter være med-handlende, og bidrar til å skape og moderere saker, og kan på den måten bidra til å endre samfunn.

Dokumenter er ikke isolerte entiteter, de utgjør alltid en del av større praksisfelter. Det finnes ikke et prinsipielt skille mellom dokumentene og omverden, Dokumenter «er allerede en integrert del av den virkeligheten og det samfunnet vi studerer» (Asdal & Reinertsen, 2020, s. 10). Praksis-orientert dokumentanalyse er en form for materiell-semiotikk, en tradisjon som overlapper med ANT. Dokumenter behandles som materiell-semiotiske objekter. Et dokument er altså både et materielt objekt (fysisk eller digitalt) og et semiotisk objekt bestående av meningsbærende tegn. Dette kan virke som en triviell påstand, men dette synet på dokumenter får direkte konsekvenser for hvordan dokumenter kan og bør studeres. Dokumenters innhold, form og relasjoner må ses i sammenheng, og dokumentene må ses som en del av større praksisfelt (Asdal & Reinertsen, 2020).

Et dokument befinner seg alltid på et sted og er en del av disse stedene. Samtidig kan et dokument også være et sted for å gjøre feltarbeid. Asdal og Reinertsen beskriver tre ulike måter dokumenter kan inngå som feltarbeid: 1) Feltarbeid med dokumenter, 2) feltarbeid i arkiver og 3) feltarbeid i dokumenter (Asdal & Reinertsen, 2020, s. 118). Måten jeg har tilnærmet meg dokumentene som empiri reflekteres i disse tre måtene dokumenter kan inngå som feltarbeid:

1) I denne oppgaven følger jeg personvern i det Reinertsen beskriver som en dokumentkjede (Reinertsen, 2016). I mitt tilfelle utgjør visjonsdokumentet fra

[3] Boken er under utgivelse 2020. Sidetallene i de kommende referansene refererer til siste utgave (mottatt 10.6.2020).

Europakommisjonen, personvernsforordningen og dokumenter knyttet til implementeringen av Nettskjema en slags analytisk «hovedkjede», omgitt av et stort antall andre dokumenter. Dette blir en måte å følge dokumentene i feltet. Samtidig er det også en måte å følge dokumentenes bevegelse, og dermed å studere dokumentene over tid.

2) Det er mange dokumenter som utspiller en rolle i oppgaven, men det legges spesielt vekt på Personvernforordningen og Europakommisjonens kommunikasjonsdokument. Disse dokumentene behandles ikke bare som kilde til informasjon, men også som sentrale objekter i seg selv. Dette har jeg gjort ved å gå dypt inn i noen deler av dokumentene og vise frem akkurat hvordan de «utøver» personvern, og samtidig hvordan de er del av et større praksisfelt.
3) Arkiv inngår nettopp i dette praksisfeltet, og arkiver utgjør viktige etnografiske steder i denne oppgaven: Loven befinner seg i EUR-lex-arkivet, og også Nettskjema, et verktøy for å hente, lagre og hente ut informasjon, kan også betraktes som et slags arkiv. Jeg har tilnærmet meg arkivet som mer enn en passiv beholder for dokumenter og opplysninger, arkivene er aktive deler av praksisfeltene de inngår i.

2.2.3 Oppgavens empiri og tilnærming

I det første analysekapitlet er det to dokumenter som utgjør hoved-empirien: Europakommisjonens visjonsdokument og Personvernforordningen. Visjonsdokumentet gir innsikt i hvilke utfordringer lovverket er ment å løse og hvordan den skal løse disse utfordringene. Samtidig representerer dokumentet en juridisk/byråkratisk sjanger og praksis som spiller en sentral rolle for å materialisere visjonen Europakommisjonen tegner opp. Personvernforordningen utgjør det empiriske dreiningspunktet i oppgaven. Først og fremst det første analysekapitlet fokuserer på lovverket, men det er også til stede i de andre kapitlene. Store deler av lovverket har informert min lesning, men jeg har valgt å trekke frem noen korte utsnitt fra loven som er relevante for å besvare mine forskningsspørsmål: Artikkel 4 med definisjoner, artikkel 5 «Prinsipper for behandling av personopplysninger», samt noen korte utdrag fra lovens fortale. Disse utsnittene spiller en avgjørende rolle i konstruksjonen av personinformasjon som risiko- og verdiobjekt.

Visjonsdokumentet og Personvernforordningen befinner seg i EUR-Lex. Dette har også utgjort et viktig etnografisk sted for oppgaven. Jeg har derfor også satt av plass til å beskrive arkivet som sted og dets rolle som en del av en juridisk infrastruktur. En annen grunn

til at jeg har valgt å fremheve arkivet er at det, som digitalisert arkiv, viser frem hvordan digitale infrastruktur allerede er en del av, og virker inn på, den juridiske infrastrukturen.

Det andre analysekapitlet består av to deler. Den første delen dreier seg om prinsippet om ansvarlighet, og der har jeg tatt utgangspunkt i Artikkel 29-gruppens uttalelse om prinsippet om ansvarlighet fra 2010 (Artikkel 29-gruppen, 2010). Artikkel 29-gruppen var EUs arbeidsgruppe for personvernspørsmål, og var sammensatt av medlemsstatenes datatilsynsmyndigheter. Den andre delen av kapitlet handler om innebygget personvern. I denne delen har jeg gjort en dokumentanalyse av Datatilsynets veileder «Programvareutvikling med innebygd personvern». Dette dokumentet er interessant fordi det tar «innebygd personvern» et skritt videre, og gir konkrete anbefalinger og verktøy til personer og organisasjoner som jobber med programvareutvikling. Dokumentet er et verktøy for programvareutviklere som skal håndtere behandling av personinformasjon. Sett fra perspektivet til EUs visjon kan det samtidig ses som et verktøy for å bygge inn personvernet. Derfor er det også et tydelig relevant dokument med tanke på min problemstilling.

I det tredje og siste analyse kapitlet, «Å bygge inn personvern i IT-praksis: Nettskjema», undersøker jeg USITs «Nettskjema». For å undersøke hvordan Personvern møter IT-praksis, har jeg studert denne digitale tjenesten, og analyser hvordan personvernet bygges inn i nettskjema og organisasjonen. For å gjøre det har jeg både studert den tekniske løsningen og intervjuet en utviklingsleder som arbeider med Nettskjema. I tillegg har jeg brukt en video-presentasjon fra den samme utviklingslederen og USITs nettsider som empiri.

Metoden og den utforskende tilnærmingen til materialet i denne oppgaven har også medført at jeg har samlet inn langt mer datamateriale enn jeg har endt opp å trekke frem i den ferdige oppgaven. For det første har jeg gjort flere intervjuer som ikke har endt opp med å fokusere på: Et med en jurist i Datatilsynet, en teknolog i Datatilsynet og en tidligere jurist ved Universitetet i Oslo. Jeg deltok også på konferansen Computers, Privacy and Data Protection (CPDP) 2019 i Brussel. Konferansen er et møtepunkt for de som jobber med personvern i Europa, i akademia, bedrifter, statlig byråkrati og for jurister. Dette ga meg en bedre forståelse for de mange utfordringene knyttet til personvern fra mange ulike perspektiver. Ikke minst har jeg lest og studert et stort antall lovdokumenter og nettsider som ikke ble en del av empirien jeg aktivt bruker. Likevel har mye av dette materialet informert, veiledet og formet den oppgaven jeg har skrevet. Når jeg ikke har valgt å ta med alt dette materialet, er det fordi jeg har ønsket å kunne gå i dybden på et mindre empirisk materiale, og virkelig vise frem den praksisen som dette utgjør, i stedet for å skrape i overflaten på et større materiale.

Vitenskap- og teknologistudier har en tradisjon for å undersøke komplekse fenomener ved å studere konkrete praksiser. Det har jeg også gjort i denne oppgaven ved å angripe en nokså bred tematikk med en eksplorerende tilnærming, men til gjengjeld snevret inn oppgaven gjennom det empiriske utvalget. Med «eksplorerende tilnærming» mener jeg at jeg underveis i oppgaven har hatt en agnostisk og åpen innstilling til det empiriske materialet (jf. Callon, 1984). Jeg har behandlet de ulike stedene i oppgaven ikke bare som en kilde til informasjon, men som et sted med forbindelseslinjer til praksis og materialer i nettverk som virker sammen for å skape handling, endring eller stabilitet. I dokumentene, arkivet og i den tekniske løsningen, har jeg forsøkt å vise frem komponentene og forbindelseslinjene som setter de i stand til å handle. Samtidig har jeg under arbeidet etterstrebet å la sentrale objekter, slik som «personvern» og «personopplysninger», forbli åpne uten at jeg som forsker påtvinger min egen definisjon, men heller undersøker hvordan disse begrepene blir til i praksis og endrer karakter fra sted til sted.

2.2.4 Kvalitative intervjuer

Som jeg har nevnt utførte jeg til sammen fire intervjuer i Datatilsynet og USIT. Jeg bruker bare to av disse eksplisitt i analysematerialet. De resterende intervjuene har likevel informert oppgaven og hjulpet meg med å sirkle inn det jeg vil løfte frem i materialet. Jeg gjennomførte disse intervjuene for å få innsikt i praksisen knyttet til dokumentene jeg undersøkte, og i tilfelle med intervjuene i USIT for å undersøke IT-praksisen knyttet til å gjøre personvern til en del av Nettskjema. Jeg valgte å bruke kvalitative intervjuer for å få fyldigere beskrivelser og for å få frem de konkrete praksisene som utøves knyttet til dokumentene og infrastrukturen jeg har undersøkt (Hay, 2016, s. 150).

Intervjuer utført for oppgaven

Dato	Posisjon	Relevans
5.12.2018	Jurist, Datatilsynet	Arbeidet med personvern i relasjon til Europeisk samarbeid.
24.1.2019	Fagleder, Datatilsynet	Arbeidet med Datatilsynets veileder, «Programvareutvikling med innebygd personvern».
27.3.2019	Utviklingsleder, USIT	Arbeidet med Nettskjema og implementering av personvern

20.5.2019	Tidligere jurist ved Universitetet i Oslo og USIT	Personvern som ekspertisefelt og veiledet USIT i personvernspørsmål.

Intervjuene hadde en semi-strukturert form. Det vil si at jeg hadde skrevet en intervjuguide på forhånd, men at jeg var åpen for å komme inn på andre relevante temaer (Hay, 2016, s. 158). Jeg fokuserte på å stille åpne spørsmål og fleksible spørsmål. Dette gjorde jeg for å ikke legge for sterke føringer og for åpne opp for andre innfallsvinkler (Weiss, 1994, s. 74). Ettersom mine informanter hadde langt mer kunnskap om feltet enn meg, viste denne fleksibiliteten seg spesielt gunstig, ettersom informantene bidro med informasjon eller perspektiver som gjorde at intervjuene tok en annen vending enn forventet. Av samme grunn brukte jeg mye tid på å skrive fleksible intervjuguider slik at jeg kunne få mest mulig ut av intervjuene.

Intervjuene ble tatt opp på lydopptaker og transkribert i etterkant. Jeg kodet deretter intervjuene i analyseprogrammet NVivo. Jeg valgte å kode intervjuene som en del av analysearbeidet som en metode for å se forbindelser og gjennomgående tematikk i intervjuene (Corbin & Strauss, 2008, s. 66). Dette var også svært nyttig for å kartlegge relevant tematikk som dukket opp i intervjuene.

2.2.5 Etikk

Ettersom jeg skulle bruke intervjuer i oppgaven, sendte jeg inn prosjektet til Norsk senter for forskningsdata (NSD), som godkjente prosjektet (referanse 156326). I henhold til NSDs retningslinjer, sendte jeg brev til informantene i forkant av intervjuene med informasjon om prosjektet og hvordan informasjonen ville bli behandlet. I tråd med informasjonsskrivet som ble gitt til informantene, gjennomførte jeg tiltak for å anonymisere informantene. Det innebærer at all intervjuene ble anonymisert etter transkribering, at all intervjudata vil bli slettet når prosjektet avsluttes og at kun arbeidstittel brukes for å referere til de respektive informantene i oppgaven.

3 Visjonen og loven

I dette kapitlet analyserer jeg visjonen om et nytt europeisk personvern, og hvordan loven gjøres til et verktøy for å bygge inn denne visjonen. Jeg starter starter i EUs lovarkiv der Personvernforordningen og «*A comprehensive approach on personal data protection in the European Union*» dokumentet der Europakommisjonen tegner opp visjonen for et nytt personvernlovgivning, befinner seg. I visjonsdokumentet fokuserer jeg på hvordan det artikuleres en problematisering med loven som løsning, og hvordan verdi og risiko spiller inn i denne problematiseringen. Jeg fortsetter til Personvernforordningen, der jeg gjør en nærlesning av artikkel 4 «Definisjoner» og artikkel 5 «prinsipper». Til slutt undersøker jeg hvordan visjonen og loven bygger videre på EUs målsettinger og hvordan disse smeltes sammen og hvordan personopplysninger gjøres til et forvaltningsobjekt i tråd med disse målsetningene.

Figur 2: To av prosedyrene som ledet frem til Personvernforordningn i EUR-lex. (Hentet 13.6.20 fra https://eur-lex.europa.eu/procedure/EN/199818 og [https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:32016R0679)](https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:32016R0679)

3.1 En dokumentkjede: Fra visjon til lovtekst

I 2009 satte Europakommisjonen i gang en utredning for å besvare hvorvidt den daværende lovgivningen var tilstrekkelig for å hanskes med nye utfordringer knyttet til personvern. En konferanse ble arrangert, en offentlig konsultasjon ble utlyst og flere studier ble satt i gang (Europakommisjonen, 2010, s. 3). Resultatene blir presentert i dokumentet med tittelen *«A comprehensive approach on personal data protection in the European Union»*, COM(2010) 609 final, der Europakommisjonen oppsummerer sitt forslag til en ny europeisk personvernlovgivning.

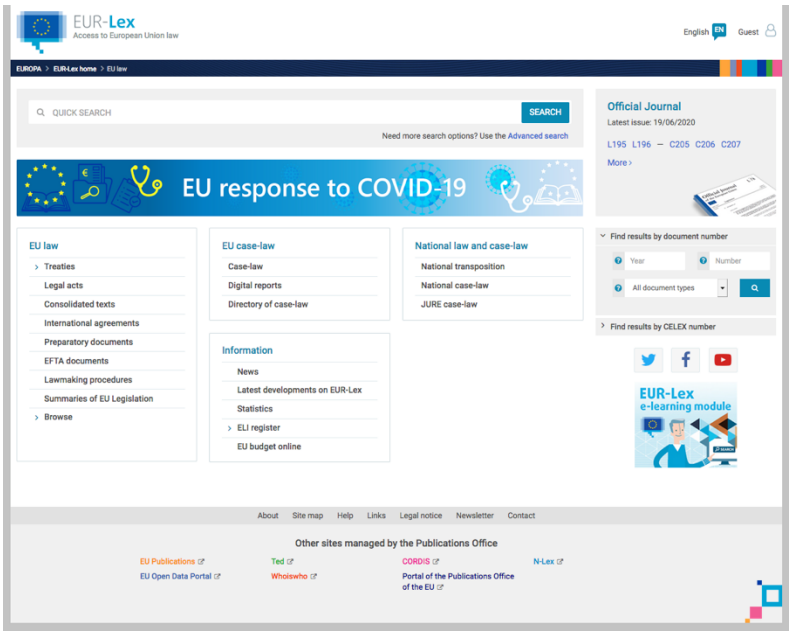
Figur 2 over viser to av prosedyrene i EU som leder frem til Personvernforordningen. Figurene er hentet fra EUR-Lex som jeg vil komme tilbake til senere i kapitlet. Den øverste prosedyren starter med det nevnte dokumentet der Europakommisjonen tegner opp en visjon for loven. Den nederste prosedyren ender med den ferdige utgaven av Personvernforordningen, ferdigstilt i 2016. Hver prikk i figuren representerer et eller flere dokumenter av ulik art, møtereferater, kommunikasjonsdokumenter og utkast til lovtekst. Figurene viser en beslutningsprosess i et moderne politisk byråkrati, men det viser også frem en kjede av dokumenter og tekstarbeid som spiller en sentral rolle i å skape en ny personvernlovgivning.

Av EUs mange institusjoner er det tre av de som utgjør kjernen i EUs beslutningsprosess, som også kommer til uttrykk i figuren ovenfor: Europakommisjonen, Europaparlamentet og Rådet for Den europeiske union. Europaparlamentet er EUs direkte demokratiske institusjon, bestående av 751 representanter som blir direkte valgt av innbyggere i EUs medlemsstater (Olsen et al., 2017, s. 125–126). Rådet for Den europeiske union er sammensatt av ministre fra EUs 28 medlemsstater, og representerer grovt sett medlemsstatenes interesser (Olsen et al., 2017, s. 83). Europakommisjonen er den utøvende myndighet i EU, og det er denne institusjonen som er mest relevant for denne oppgaven. Kommisjonens hovedoppgaver er å utvikle forslag til vedtak og tiltak (altså rettsakter, inkludert lovtekst), håndheve EU-traktatene, forberede dagsordenen for EUs lovgivende organer og administrere EUs sentrale administrasjon. Det skal ikke tas nasjonale hensyn i kommisjonens arbeid, men den er ikke politisk nøytral. Kommisjonen skal arbeide for EUs interesser, politisk og byråkratisk, som i praksis betyr å utøve og håndheve EUs traktater (Olsen et al., 2017, s. 104–105).

Før jeg går videre til å analysere dokumentet der Europakommisjonen tegner opp sin visjon for et nytt europeisk personvern, vil jeg se litt nærmere på EUs lov-arkiv, EUR-Lex, der både «visjonsdokumentet» og Personvernforordningen befinner seg.

3.1.1 EUR-Lex

EUR-Lex er EUs arkiv for lover og dokumenter knyttet til EUs beslutningsprosesser. Mitt eget møte med EUR-Lex ga en overveldende opplevelse av å trå inn i et system som er for stort for enkeltmennesket. Her finnes millioner av dokumenter, fra 1951 og fremover (EUR-Lex, u.å.-a).



Figur 3: Skjermdump, EUR-Lex forside (Hentet 22.6.20 fra https://eur-lex.europa.eu/homepage.html)

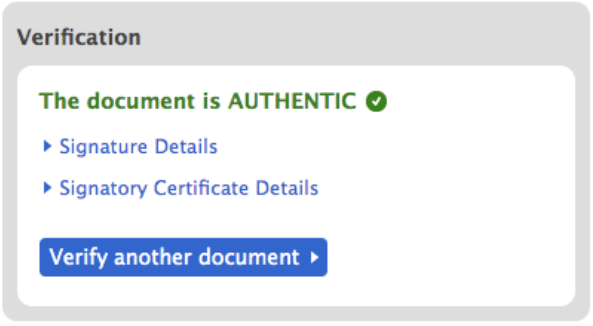
Et arkiv er et sted for oppbevaring og lagring av informasjon, men også ordningen av den informasjonen som arkivet innehar. I EUR-Lex ordnes og kategoriseres dokumentene på mange ulike måter. Hvert dokument er kategorisert i flere forskjellige systemer og det digitale brukergrensesnittet gjør det også mulig for brukeren å ordne dokumentene for eksempel etter prosedyre eller gjennom avanserte søkefunksjoner. Mest overordnet er Celex-koden. Alle dokumenter i arkivet er tildelt en egen slik kode. Denne består av hvilken sektor dokumentet hører inn under, årstall, type lovdokument og dokument-tall («Frequently asked questions», eurlex.eu, udatert). Personvernforordningen har for eksempel koden 32016R0679. Ut av koden kan en lese at vi har med en lovgivning å gjøre (3) vedtatt i 2016, det er en regulering (R) med dokumentnummer 0679. Mange av dokumentene kan også spores til hvor de hører til i den juridisk-politiske prosedyren de tilhører. Denne koden er en av måtene EUR-Lex utøver en av arkivers kjerneaktiviteter: Å kategorisere, standardisere og ordne informasjonen som arkivet innehar.

EUR-Lex beskriver seg selv som «your online gateway to EU Law. It provides the official and most comprehensive access to EU legal documents» (EUR-Lex, u.å.-a). Gjennom det nevnte digitaliserte brukergrensesnittet skal EUR-Lex oppfylle sin målsetning om å gi

«online» tilgang. For EU, som en liberaldemokratisk overnasjonal union, utgjør borgeres tilgang til lovene og prosedyrene en vesentlig funksjon. Som nevnt er det ikke bare lovene som er tilgjengelig i EUR-Lex, men også dokumentene som dokumenterer beslutningsprosessen frem til loven blir vedtatt. På dette måten utgjør også arkivet en sentral «accountability»-funksjon. Dette begrepet vil jeg komme tilbake til senere i oppgaven, men det er også relevant her. Vi mangler en god oversettelse av dette begrepet på norsk. Som jeg kommer tilbake til i neste analysekapittel dekker dette begrepet både det å være ansvarlig og det å være i stand til å svare for seg. Ved å vise frem og sette Personvernforordningen i forbindelse med en kjede av dokumenter, slik som blir gjort i figur 3 dokumenteres beslutningsprosessen som har gitt opphav til forordningen. På denne måten gir arkivet og dokumentene i kjeden økt legitimitet til hverandre.

EUR-Lex inneholder et stort antall type dokumenter og verktøy. «Lov» slik det blir presentert i arkivets undertittel, inkluderer også «forberedende dokumenter», rettspraksis (case law), internasjonale avtaler, EØS-dokumenter og sammendrag av lovgivning (EUR-Lex, u.å.-a).[4] Offisielle dokumenter publiseres i dag på alle de 24 offisielle EU-språkene, i flere forskjellige digitale formater. En viktig rekke av dokumenter som EUR-Lex gir tilgang til er «the authentic Official Journal of the European Union», forkortet til «OJ» (EUR-Lex, u.å.-a). Dette er EUs offisielle tidsskrift som publiseres alle hverdager. Tidsskriftet inneholder primært juridiske tekster - lovgivning, regulering, rettspraksis og prosedyrer – men også offisiell informasjon og merknader (EUR-Lex, u.å.-b). OJ publiseres i dag digitalt, forkortet til «e-OJ». Kun lovtekst som publiseres i OJ har juridisk verdi («legal value»), og siden 2013 er det kun den digitale versjonen som har rettsvirkning. Det er altså kun i den digital utgaven av «e-OJ» at Personvernforordningen er rettskraftig, nærmere bestemt i *Official Journal of the European Union*, L119, volum 59, utgitt 4. mai 2016.

EUR-Lex har en egen tjeneste for å bekrefte en e-OJs autentisitet: «CheckLex». En e-OJ, kan lastes opp, eksempelvis PDFen som inneholder Personvernforordningen, sammen med en korresponderende e-signatur, og



Figur 4: Skjermdump. Bekreftelse på at PDFen med Personvernfoordningen er autentisk (dokumentet i figur 1). Official Journal of the European Union, Online verification of the certified electronic edition. (CheckLex)

[4] EUR-Lex' interne nettside om arkivet ramser opp disse dokumenttypene, i tillegg til det vage «other public documents». Selv det mest byråkratiske og ordnede arkiv kan ikke få «alt» til å passe inn i sine kategorier.

CheckLex kan bekrefte (eller avkrefte) at dokumentet er autentisk. E-signaturen kommer i form av en fil som kan lastes ned fra samme oppføring i EUR-Lex der PDFen av OJ kan lastes ned sammen med en PDF av loven. For å bekrefte dokumentets «authenticity, integrity and inalterability» (EUR-Lex, u.å.-c) lastes PDFen og e-signaturen opp i CheckLex, og dokumentets autentisitet bekreftes (eller avkreftes). Autentifiseringen bekrefter mer enn at dokumentet er ekte. Autentifiseringen bekrefter at Personvernforordningen er rettskraftig. Dette er slik sett et verktøy som også bekrefter dokumentets juridiske verdi som et dokument som skal utøves i juridisk praksis.

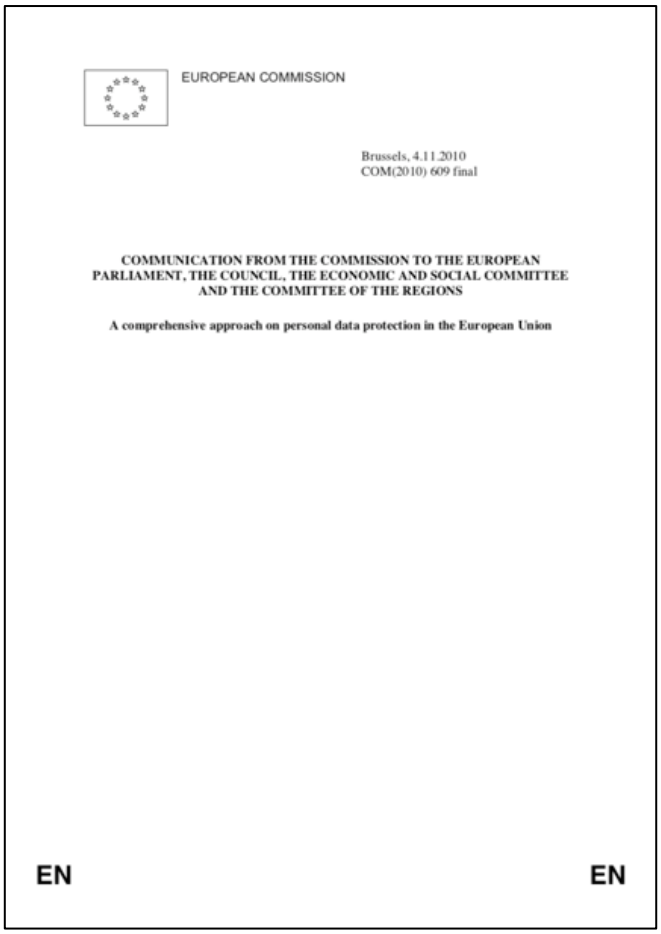
De mange ulike digitale verktøyene spiller en sentral rolle i EUR-Lex' virkemåte. Et avansert digitalt brukergrensesnitt gir en lang rekke funksjoner til arkivets besøkende (Noen av de mest sentrale funksjonene er lagring av dokumenter på din egen side, sammenligning av dokumentet på ulike språk, oppsummering av dokumentet). Mange av redskapene – lenker som binder dokumenter sammen med et klikk og en sofistikert søkemotor som på sekunder henter frem alle relevante dokumenter – er instrumenter mennesker i digitaliserte samfunn tar for gitt. Andre verktøy, som visualiseringen av prosedyren i figur 2 og autentifiseringsverktøyet «CheckLex» som jeg nå har beskrevet, er mer særegne for denne spesifikke typen digitale arkiv. Sammen bidrar de til virkemåten til et effektivt politisk-byråkratisk maskineri.

Som arkiv er EUR-lex mer enn en passiv beholder for lovtekst og dokumentasjon, det er også en del av lovkomplekset som utøver loven. Arkivet gjør det tydelig at Personvernforordningen bygger på og samhandler med et stort antall andre dokumenter, både andre lovverk, men også en rekke andre dokumentsjangre. Arkivet er noe mer enn summen av dokumentene, både fordi arkivet gjør noe mer når dokumentene samles, fordi arkivet er en institusjon i samspill med EUs øvrige institusjoner og på grunn av verktøyene arkivet tilbyr. Forbindelsen til andre dokumenter i arkivet og de ulike verktøyene som arkivet tilbyr gir dermed forordningen økt tyngde og gjennomføringskraft.

I det som følger analyserer jeg dokumentet der Europakommisjonen tegner opp sin visjon for et nytt personvern i Europa. For enkelhetsskyld har jeg valgt å kalle dette for «visjonsdokumentet».

3.1.2 Visjonsdokumentet

I dokumentet med tittelen *«A comprehensive approach on personal data protection in the European Union»*, COM(2010) 609 final, oppsummerer Europakommisjonen sin posisjon angående en ny europeisk personvernlovgivning. Med konklusjonene fra den nevnte utredningen som utgangspunkt, beskriver kommisjonen hvorfor det er behov for å erstatte personverndirektivet fra 1995 med et nytt lovverk, og tegner opp sin visjon for hvordan en ny slik lovgivning skal se ut.


EUROPEAN COMMISSION

Brussels, 4.11.2010
COM(2010) 609 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

A comprehensive approach on personal data protection in the European Union

EN EN

Figur 5: "A comprehensive approach on personal data protection in the European Union",omslag, Europakommisjonen, 2010

Dokumentet har et standardisert oppsett som gir en opplevelse av å lese en rapport. Omslaget består kun av teksten «EN», stemplet tre ganger, og alle sidene i dokumentet har dette stemplet i stor skrift i hjørnene. Dette fungerer som en påminnelse av at dette bare er en utgave av dokumentet, det vil si, den engelske versjonen i PDF-format, og at vi har å gjøre med et flerspråklig og overnasjonalt dokument. Dokumentet er satt opp på en enkel og stilren måte som gir inntrykk av et profesjonelt byråkrati. Bare ved å se en slik forside blir en slått av en mistanke om at det finnes tusenvis av dokumentforsider som er til forveksling lik denne. Jeg får følelsen av at jeg skal forstå at jeg befinner meg i et enormt byråkrati som utfører sitt arbeide med stor nøyaktighet.

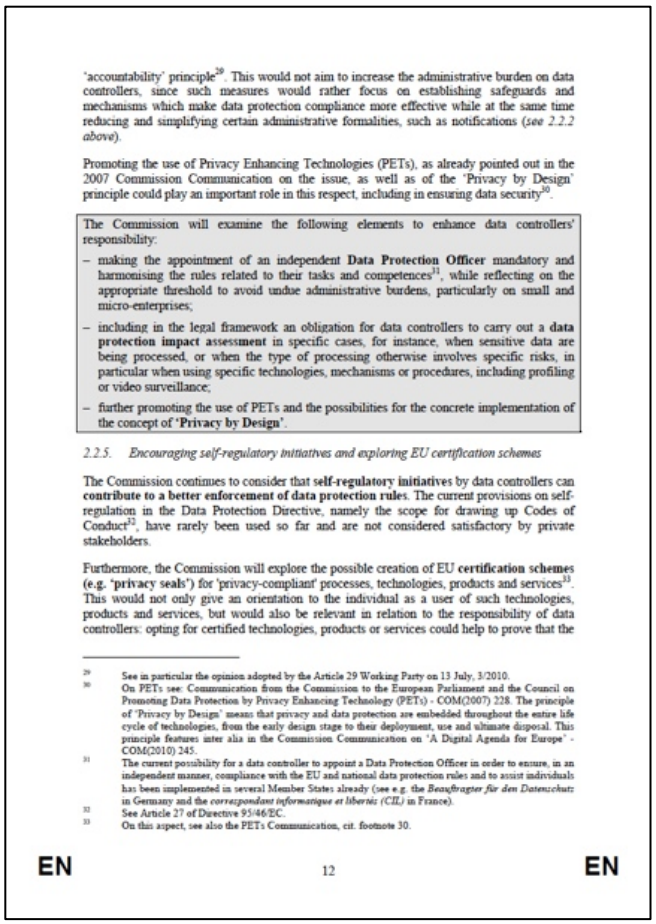
I likhet med andre kommunikasjonsdokumenter fra kommisjonen i EUR-Lex, er dokumentets tittel en formell beskrivelse av dokumentets rolle: *«COMMUNICATION FROM THE COMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS»*. Deretter følger akkurat dette visjonsdokumentets tittel: *«A comprehensive approach on personal data protection in the European Union»*. Det første som kommuniseres er kommunikasjonens retoriske situasjon (Gripsrud, 2002, s. 161). Dokumentets funksjon som et kommunikasjonsdokument, fra en sentral EU-institusjon til to andre sentrale institusjoner i

EU, fremheves foran dokumentets egen tittel. Måten dokumentet er utformet på gjør det tydelig at dokumentet er en del av et dokumentvelde. Det er kanskje nettopp fordi det står sammen med et utall andre dokumenter i EU-byråkratiet at akkurat dette dokumentet får sin legitimitet og tyngde. Dokumentet har 51 fotnoter over sine 19 sider. Lik en forskningsartikkel, trekkes det forbindelser til et stort kunnskapsfelt. Tilnærmet alle disse refererer til ulike EU-dokumenter: rapporter, kommikasjonsdokumenter, lovparagrafer, høringsvar, utredninger og dommer fra EUs domstol. Inntrykket forsterkes av figurene med prosedyrene fra EUR-lex. Dokumentet står på ingen måte alene, men står sammen med en kjede av dokumenter, både forut for og etter visjonsdokumentet, som sammen gir legitimitet og kraft til visjonen som tegnes opp.

Dokumentet er gjennomsyret av en tekst-tung stilrenhet, og inneholder ingen overflødige elementer eller visuelle virkemidler. Det er ingen grafer, ingen bilder og ingen farger i teksten. Dokumentets følger et strengt oppsett og har en nøktern tone. Sammen gir dette et tydelig byråkratisk preg. Nettopp av den grunn trer de pedagogiske grepene som er gjort desto tydeligere frem: Enkelte setninger og ord er fremhevet i fet skrift, det er satt inn oppsummerende kulepunkter i lister – men det tydeligste grepet er grå bokser som oppsummerer hver tekstdel. Med unntak av innledning og avslutning har alle undertitler sin egen oppsummerende boks, hvor de mest sentrale setningene innenfor disse boksene er fremhevet med fet skrift. Dette er pedagogiske virkemidler som kan minne om moderne lærebøker; teksten er lagt opp slik at den kan leses på ulike grundighetsnivåer, samtidig som det gir en tydelig pekepinn på hva avsenderen mener er viktigst at mottakeren får med seg. I denne sammenhengen gjør de pedagogiske grepene dokumentet godt egnet til å effektivt formidle hovedbudskapet, akkurat slik som kreves av et moderne politisk byråkrati.

Dokumentet starter med en situasjonsbeskrivelse for personopplysninger i Europa under tittelen *«New Challenges for the Protection of Personal Data»*. Først etableres viktigheten av direktivet fra 1995:

> The Directive enshrines two of the oldest and equally important ambitions of the European integration process: the protection of fundamental rights and freedoms of individuals and in particular the fundamental right to data protection, on the one hand, and the achievement of the internal market – the free flow of personal data in this case – on the other.
> (Europakommisjonen, 2010, s. 2)



'accountability' principle[29]. This would not aim to increase the administrative burden on data controllers, since such measures would rather focus on establishing safeguards and mechanisms which make data protection compliance more effective while at the same time reducing and simplifying certain administrative formalities, such as notifications (*see 2.2.2 above*).

Promoting the use of Privacy Enhancing Technologies (PETs), as already pointed out in the 2007 Commission Communication on the issue, as well as of the 'Privacy by Design' principle could play an important role in this respect, including in ensuring data security[30].

The Commission will examine the following elements to enhance data controllers' responsibility:

- making the appointment of an independent **Data Protection Officer** mandatory and harmonising the rules related to their tasks and competences[31], while reflecting on the appropriate threshold to avoid undue administrative burdens, particularly on small and micro-enterprises;
- including in the legal framework an obligation for data controllers to carry out a **data protection impact assessment** in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance;
- further promoting the use of PETs and the possibilities for the concrete implementation of the concept of **'Privacy by Design'**.

2.2.5. Encouraging self-regulatory initiatives and exploring EU certification schemes

The Commission continues to consider that **self-regulatory initiatives** by data controllers can **contribute to a better enforcement of data protection rules**. The current provisions on self-regulation in the Data Protection Directive, namely the scope for drawing up Codes of Conduct[32], have rarely been used so far and are not considered satisfactory by private stakeholders.

Furthermore, the Commission will explore the possible creation of EU **certification schemes (e.g. 'privacy seals')** for 'privacy-compliant' processes, technologies, products and services[33]. This would not only give an orientation to the individual as a user of such technologies, products and services, but would also be relevant in relation to the responsibility of data controllers: opting for certified technologies, products or services could help to prove that the

29 See in particular the opinion adopted by the Article 29 Working Party on 13 July, 3/2010.
30 On PETs see: Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technology (PETs) - COM(2007) 228. The principle of 'Privacy by Design' means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal. This principle features inter alia in the Commission Communication on 'A Digital Agenda for Europe' - COM(2010) 245.
31 The current possibility for a data controller to appoint a Data Protection Officer in order to ensure, in an independent manner, compliance with the EU and national data protection rules and to assist individuals has been implemented in several Member States already (see e.g. the *Beauftragter für den Datenschutz* in Germany and the *correspondant informatique et libertés (CIL)* in France).
32 See Article 27 of Directive 95/46/EC.
33 On this aspect, see also the PETs Communication, cit. footnote 30.

EN 12 EN

Figur 6: "A comprehensive approach on personal data protection in the European Union", s. 12, Europakommisjonen, 2010

Men, påpekes det, verden har forandret seg: «rapid technological developments and globalisation have profoundly changed the world around us, and brought new challenges for the protection of personal data.» (Europakommisjonen, 2010, s. 2) Direktivet fra 1995 var altså på riktig vei, men ny regulering må på plass for å opprettholde EUs ambisjoner i møtet med dagens situasjon. I tillegg til å argumentere for visjonen om et nytt personvernsparadigme, viser dokumentet hvordan visjonen passer inn i EU. *Den europeiske unions pakt om grunnleggende rettigheter* har også blitt en del av EUs juridiske rammeverk. Paktens artikkel 8 etablerer retten til beskyttelse av personopplysning som en grunnleggende rettighet. Kommisjonen argumenterer for at teknologisk utvikling sammen med en ny juridisk situasjon legger grunnlaget for en ny lovgivning med hensyn til «the protection of individuals with regard to the processing of their personal data and on the free movement of such data» (Europakommisjonen, 2010, s. 4, jf. Personvernforordningens tittel).

Den digitale revolusjonen jeg nevnte innledningsvis er tydelig til stede i dokumentet. Det trekkes frem noen eksempler på hvordan det med dagens teknologi både gjør det enklere for individer å dele informasjon om seg selv og å samle personinformasjon. «Skyen» nevnes som et eksempel på det første, og som et karakteristisk eksempel på en type uregulert informasjonsstrøm som utgjør et problem for personvern: Individer mister potensielt kontroll

over sine sensitive opplysninger når deres data lagres på andres maskiner. Samtidig har det blitt enklere å samle inn store menger av data om individer, både i større skala og på måter som er vanskelig å oppdage. Under dette punktet trekkes automatisk datainnsamling frem: Ulike tekniske løsninger for å samle inn informasjon om individer, både offentlig og privat, som på ulike måter sporer individer i deres vanlige liv. Det slås fast at det er en bred konsensus om at det er økt risiko knyttet til personvern («privacy and the protection of personal data»), og det konkluderes med at det er behov for et nytt lovverk som kan løse en rekke tilknyttede utfordringer (Europakommisjonen, 2010, s. 3–5).[5]

Både den digitale utviklingens muligheter, så vel som dens trusler, adresseres i situasjonsbeskrivelsen. Et nytt skal lovverk skal løse disse utfordringene, samtidig som det skal realisere to av det vi har sett er EUs viktigste og eldste ambisjoner: Beskyttelse av europeeres rettigheter og friheter, og styrke Europas indre marked.

3.1.3 En visjon om håndtering av risiko og verdi

Jeg leser dokumentet slik at det tar på seg oppgaven å kommunisere en visjon, ikke bare om en ny lov, men om en ny datapolitikk i Europa. Basert på utredningen, tegnes det opp en virkelighetsbeskrivelse og et sett av argumenter for hvorfor et nytt personvernslovverk må på plass og hvordan det bør se ut. Dokumentet beskriver også verktøyene som skal tas i bruk for å virkeliggjøre denne visjonen.

Det sentrale objektet for virkelighetsbeskrivelsen er digital teknologi. De to teknologi-beskrivelsene i dokumentet, «skyen» og automatisk datainnsamling, fungerer som prototypiske eksempler på hvordan ny digital teknologi utfordrer vernet av personopplysninger, og dermed også truer individers rettigheter. Beskrivelsenes effekt er å redusere «teknologisk utvikling og globalisering» til prototypiske eksempler som karakteriserer og kommuniserer essensen av dagens situasjon i møte mellom personopplysninger og teknologi. I dokumentet skapes en bestemt problematisering av dette møtet, og hvordan et nytt lovverk kan løse problemet.

I dokumentet er den uregulerte digitale teknologien en risiko for fysiske personer og deres personopplysninger. Et nytt lovverk vil kunne verne fysiske personer og deres

[5] Utfordringene som et nytt lovverk skal løse oppsummeres av de følgende punktene: «Strengthening individuals' rights», «Enhancing the internal market dimension», «Revising the data protection rules in the area of police and judicial cooperation in criminal matters», "The global dimension of data protection", "A stronger institutional arrangement for better enforcement of data protection rules".

personopplysninger, samtidig som det sikrer fri flyt av personopplysninger og bidra til et styrket (digitalt) indre marked; med et godt lovverk og regulering kan den digitale teknologien og informasjonsstrømmen temmes.

Visjonsdokumentet tegner altså opp selve rammen for problemet og hvordan problemet skal løses og etablerer sammenhengen mellom de sentrale aktørene i problematiseringen. Vi ser altså at dokumentet fremhever digital teknologi som den nye lovens bevegelsesgrunn. Digital teknologi kan slik forsås som et risiko-objekt i dokumentet. Grunnen til at de utgjør risiko er fordi de bidrar til økt deling og innsamling av personopplysninger. Det er *behandling* av personopplysninger som utgjør skade i form av å krenke individers rettigheter. Samtidig fremheves viktigheten av fri flyt av personopplysninger for EUs indre marked. Behandlingen av personopplysninger settes altså også i sammenheng med verdi i en økonomisk forstand. Jeg tolker dette slik at risikoen derfor blir enda større, for ved behandling av personopplysninger risikeres skade på grunnleggende rettigheter, og på den andre siden risikeres et svakere marked ved mindre behandling av personopplysninger.

I dokumentet tegnes det opp en visjon for hvordan risikoen knyttet til behandling av personopplysninger kan håndteres. Med Hilgartners begrepsapparat, kan en si at risiko-objektet forsøkes å flyttes inn og gjøres til en del av nettverket. Slik jeg tolker dette, er det nettopp fordi personopplysningene og de teknologiske utviklingene som muliggjør en økt flyt av personopplysninger samtidig ses som verdifulle. Dokumentet tegner opp et juridisk kontrollnettverk som skal håndtere risiko og sikre markedsverdi.

Dette er foreløpig en grov skisse av hvordan personopplysninger settes i relasjon med verdi og risiko, og hvordan risiko og verdi skal håndteres. Dette bildet vil jeg fylle inn videre i oppgaven. Jeg vil nå bevege meg videre til selve lovgivningen, og vise hvordan visjonen bygges inn i lovgivningen.

3.2 Personverforordningen


Official Journal L 119
of the European Union
English edition Legislation Volume 59 4 May 2016
Contents
I Legislative acts
REGULATIONS
• Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(1) ... 1
DIRECTIVES
• Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA ... 89
• Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime ... 132
(1) Text with EEA relevance
EN
Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.
The titles of all other acts are printed in bold type and preceded by an asterisk.

Figur 7: Official Journal of the European Union, L119, 2016.

Dokumentet med lovteksten er langt og skrevet i et juridisk og lite tilgjengelig språk. Teksten oppleves raskt repetitiv, og det er vanskelig å skille ut hva som er vesentlig. For å få tak på lovteksten, vendte jeg meg til kommentarlitteraturen. I denne delen av oppgaven har jeg tatt i bruk Skullerud et als. norske kommentarutgave til lovgivningen. Denne boken, som er på hele 752 sider, består av selve lovgivningen, med hver artikkel etterfulgt av forfatternes kommentarer med relevante rettskilder. Den er «skrevet med tanke på jurister og andre som berøres av forordningen i sitt arbeid» (Universitetsforlaget, u.å.). I tillegg til å ha informert min lesning av lovverket, har jeg trukket frem sitater fra kommentarutgaven for å vise frem hvordan loven tolkes og konkretiseres av juridisk litteratur. Slik sett utgjør også den norske kommentarutgaven en del av både dokumentkjeden og juridiske praksisen som jeg undersøker.

Skullerud et als. kommentarutgave beskriver lovteksten innledende slik: «Forfatterne legger ikke skjul på at det har vært utfordrende å kommentere dette regelverket. [...] Vi har en forordningstekst som er omfattende, lang og skrevet på et komplisert språk» (2019, s. 40). Av 89 sider, består de første 31 sidene av «fortale», bestående av 173 punkter. Fortale er altså teksten som kommer før selve lovartiklene og skal legge et grunnlag for disse. Kommentarutgaveforfatterne skriver videre: «I tillegg har vi en fortale, som langt på vei sier det samme som selve forordningsteksten. Denne gir begrenset veiledning i hvordan forordningens ordlyd er ment å forstå» (Skullerud et al., 2019, s. 40). Også jurister og eksperter på feltet anser altså lovteksten som lite tilgjengelig. Personvernforordningen er bare et tilfelle, men det synes som om dette forteller noe om loven som sjanger; til tross for at den skal være demokratisk, blir den på grunn av sin utilgjengelighet tilsynelatende forbeholdt jurister. Som vi skal se senere, lar ikke forordningen uten videre oversette til andre praksiser, for å få til det må det utføres et tolkningsarbeid og grensedragningsarbeid.

I de kommende avsnittene fokuserer jeg på to artikler i lovgivningen: «Definisjoner» (artikkel 4) og «Prinsipper for behandling av personopplysninger» (artikkel 5). Dette utgjør en liten, men viktig del av lovverket. Som jeg har vist i delen om visjonsdokumentet, utgjør «behandling av personopplysninger» et sentralt objekt i Europakommisjonens visjon, både som et objekt for risiko og for verdi. Derfor er disse definisjonene av spesiell interesse for denne oppgaven. Jeg har valgt ut artikkel 5 «Prinsipper for behandling av personopplysninger» fordi den tydelig knytter «behandling av personopplysninger» til IT-praksis, og slik sett utgjør en av de mest konkrete delene av forordningen.

3.2.1 Artikkel 4 Definisjoner

Artikkel 4 i Personvernforordningen utgjør lovens definisjoner, en liste med 26 definerte begreper. Gjennom definisjonene legges grunnlaget for hvordan resten av loven skal tolkes og forstås, og de spiller derfor en sentral rolle i lovgivningen. Skullerud et al. bruker 34 sider på å beskrive definisjonene som utgjør én side i lovteksten. «Personopplysninger» og «behandling» utgjør de første definisjonene:

Artikkel 4. ***Definisjoner***

I denne forordning menes med

1) «personopplysninger» enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet,
2) «behandling» enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring,

Figur 8: Personvernforordningen, Artikkel 4, 1-2

Definisjonene er svært abstrakte og viser hvor bredt loven favner. Ut fra definisjonen av «personopplysning» kan det være vanskelig å avgjøre akkurat hva som utgjør en slik opplysning. Skullerud et al. (2019) bruker i den norske kommentarutgaven fem sider på å brette ut «enhver opplysning», «om» og «identifiserbar eller identifisert fysisk person». Denne grundige behandlingen av konseptet viser både at disse definisjonene spiller en sentral rolle, men også at de i sin abstrakte og generelle form er krevende å oversette til en betydning i konkret juridisk praksis. Det som først og fremst avgjør om en opplysning er en personopplysning er «identifiserbarhetskriteriet»: «At en fysisk person er identifisert, vil si at han eller hun kan skilles ut fra en gruppe av personer» (Skullerud et al., 2019, s. 74). Definisjonen av «personopplysninger» ligner på Persondirektivet fra 1995, men den er utvidet

med flere og mer spesifikke eksempler. Identifiserbarhetskriteriet har fått et bredere nedslagsfelt. Kommentarutgaven viser på dette punktet til en diskusjon om hvor vidt identifiserbarhetskriteriet må tolkes. Teknologien kan gjøre *«at alle elektroniske spor vil kunne føres tilbake til opphavsmannen eller opphavskvinnen ettersom ny teknologi gjør det vanskeligere å kutte båndene mellom informasjon og person»* (Skullerud et al., 2019, s. 74). Hva som utgjør en «opplysning om» en fysisk person, kan også være vanskelig å avgjøre. Ofte vil opplysninger om en ting, slik som et hus, fortelle noe om eieren av huset, og en opplysning om én person kan også gi opplysninger om en annen (Skullerud et al., 2019, s. 73). Denne diskusjonen illustrerer hvor stort nedslagsfelt loven har, og det er ikke uten grunn at loven har opparbeidet seg et rykte som «the law of everything» (Purtova, 2018).

Lovgivningen, sammen med diskusjonen og tolkningsarbeidet før og etter, er her med på å skape en form for juridiske objekter, slik som «personopplysning», «fysisk person» og «den registrerte», som utøves innen et bestemt praksisfelt. Dette settet av objekter og relasjonene mellom dem danner en slags ontologi, skapt av og opprettholdt gjennom juridiske dokumenter og praksis. Lovdokumentet spiller en viktig rolle i skapelsen av slike juridiske objekter og relasjoner, og sammen med et felt av praksiser og dokumenter utøves et juridisk blikk. Disse to definisjonene både bygger på allerede eksisterende litteratur og praksis, og gir opphav til en stor mengde nye dokumenter. Sammen danner definisjonene et rammeverk for tolkning, ikke bare for å bestemme hva som faller innenfor lovens nedslagsfelt, men også for et bestemt blikk og er med på å danne et saksfelt.

Definisjonen av personopplysninger viser at selve grunnlaget for reguleringen av informasjon i tråd med Personvernforordningen er knytningen mellom «fysisk person», «opplysning» og «behandling». I møtet mellom disse oppstår to nye verdifulle juridiske objekter, «fysisk person» blir til «den registrerte» og «opplysning» blir til «personopplysning». Når opplysning etableres som personopplysning blir den verdifull på en ny måte, for da kan opplysningen vernes av loven sammen med, eller som en del av den fysiske person, for eksempel av Europas menneskerettighetskonvensjon.

Samtidig får også den «fysiske person» status som «den registrerte», eller som det heter i den engelske versjonen: til «data subject» (General Data Protection Regulation, artikkel 4,1). I denne transformasjonen møtes lov, person og arkiv. En person kan først bli til den registrerte når opplysninger om vedkommende «behandles». Det er på et vis dette punktet, når personopplysninger blir til i arkivpraksis, som er lovens sentrum. Det er dette møtet som skal reguleres. Men før det kan reguleres, eller for at det skal kunne reguleres, må

det først gjøres til juridiske objekter for loven, arkivpraksisen må gjøres regulerbar. Definisjonene spiller slik sett en sentral rolle i prosessen med å gjøre arkivpraksis regulerbar.

3.2.2 Artikkel 5 Prinsipper og ansvar

Der artikkel 4 er vid og abstrakt, slik vi nå har sett, er den neste artikkelen slående i sin motsats. Artikkelen 5 «Prinsipper for behandling av personopplysninger» er den første av seks relativt korte artikler som utgjør kapittel II i forordningen, under tittelen «Prinsipper». Kapitlet beskrives i kommentarlitteraturen som svært sentral i forordningen (Skullerud et al., 2019). Artikkel 5 får plass på en liten side, og oppsummeres i stikkordsform etter hvert punkt. Vi får da følgende prinsipper: 1a) «lovlighet, rettferdighet og åpenhet» 1b) «formålsbegrensning», 1c) «dataminimering», 1d) «riktighet», 1e) «lagringsbegrensning», 1f) ««integritet og konfidensialitet», oppsummert i 2) «ansvar». At lovgivningen oppsummeres i stikkordsform slik som dette skjer ikke andre steder i lovteksten. Akkurat her kan lovteksten minne om visjonsdokumentet. Dette tyder på et sterkt ønske om å kommunisere ut akkurat disse prinsippene. En årsak til dette er naturligvis at dette er *prinsipper*, men å bruke stikkord som kommunikasjonsvirkemiddel gjentas heller ikke senere i prinsipp-kapittelet.

En grunn til at akkurat disse prinsippene fremheves kan være fordi de er rettet mot det som i loven betegnes som «behandlingsansvarlige». Her ser vi tydelig at artikkel 5 bygger på foregående artikkel, da «Behandlingsansvarlig» også har sin egen definisjon i artikkel 4: «en fysisk eller juridisk person» som «alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes» (Personvernforordningen, art. 4.7). Artikkel 4 skiller mellom behandlingsansvarlig og databehandler: «en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige» (Personopplysningsloven, art. 4.8). Artikkel 5 kan slik sett leses som direkte tale til de som loven anser som ansvarlige for det som er lovens objekt, nemlig behandling av personopplysninger. Det er her, hos de behandlingsansvarlige, at mye av jobben med å bygge inn personvernet må gjøres.

Etterfulgt av prinsippene står en liten setning for seg selv, oppsummert som stikkordet «ansvar»: «Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr.1 overholdes» (Personvernforordningen, art. 5.2). Det er her, i denne ensomme setningen at vi finner «prinsippet om ansvarlighet» - eller «accountability principle» på engelsk. Prinsippet

blir tillagt en sentral rolle i hvordan loven skal bygges inn. Dette vil jeg komme tilbake til i neste kapittel.

3.2.3 Loven som verktøy for å bygge inn

I likhet med visjonsdokumentet, gjør kommentarlitteraturen og dokumenter i lovgivningsprosedyren det klart at lovteksten bygger videre på en stor mengde allerede eksisterende dokumenter og lovpraksis som aldri blir nevnt eksplisitt i teksten. Denne mengden av tilhørende kjeder av dokumenter som gir kontekst og legitimitet, gir et paradoksalt inntrykk av at teksten både er mettet med komprimert mening, samtidig som mye av betydningen er å finne andre steder, i dokumenter og praksis.

For en som ikke har juridisk kompetanse kan det være nærliggende å møte en lovtekst med en forventning om at dette er et sted for å finne klare svar på hva som er lov og hva som ikke er lov. Som jeg beskrev tidligere, blir det tydelig av å lese loven og dens relaterte tekster, at den heller fungerer som et tolkningsverktøy i rekken av flere, der denne loven da *sammen* med flere verktøy utgjør rammen for å ta avgjørelser.

Med definisjonene og prinsippene som utgangspunkt kan lovteksten minne om en regelbok for et spill eller en sport. Definisjonene deler inn «spillefeltet» og deler ut roller til ulike aktører. Prinsippene tegner opp spillereglene for en av de sentrale spillerne, de behandlingsansvarlige. Slik som en regelbok forteller også loven hva som er verdifullt, og hvordan noen aktører kan straffes (av andre aktører) dersom de ikke følger reglene.[6] På denne måten kan loven minne om det som Akrich kaller for «script». Akrich bruker begrepet for å beskrive hvordan teknologier har med seg brukerdefinisjoner og antagelser om virkeligheten. Det er lett å se paralleller med hvordan loven tegner opp definisjoner av aktører og hvordan visjonsdokumentet tar utgangspunkt i en bestemt virkelighetsbeskrivelse. Sammen med visjonsdokumentets beskrivelse av samtidens teknologiske situasjon, følger visjonen om en fremtid, slik den kan se ut i Europa dersom de rette reguleringene kommer på plass. Sett fra dette perspektivet kan loven ses som et verktøy for å bygge inn en fremtidsvisjon og for å tegne opp et «spillefelt» med definisjoner av aktører og objekter. Definisjonene og prinsippene, i sin abstrakte form, danner et slags nett av begreper og aktører, og beskriver hvordan disse er relatert.

[6] Loven forteller riktignok ikke noe om hvordan spillerne skal vinne, så her stopper analogien mellom spill og lov.

3.3 Loven som et verdsettingsverktøy

Personvernforordningens fullstendige tittel er *«EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning)»*. Tittelen peker ut to saker ulike saker: 1) vern av fysiske personer i forbindelse med behandling av personopplysninger, 2) fri utveksling av personopplysninger og oppheving av personverndirektivet fra 1995. Utover opphevingen av personverndirektivet, har loven har altså en dobbel rolle, den skal ivareta enhver persons rett til vern av egne personopplysninger, samtidig som disse opplysningene skal kunne deles. Dette kan høres ut som to uforenlige mål. I de kommende avsnittene vil jeg undersøke hvordan disse målsettingene smeltes sammen, og hvilke versettingspraksiser som kommer til uttrykk i forordningen og visjonsdokumentet.

3.3.1 EUs verdier som «installert base»

Loven starter med disse to fortalene:

1) Vern av fysiske personer i forbindelse med behandling av personopplysninger er en grunnleggende rettighet. I artikkel 8 nr. 1 i Den europeiske unions pakt om grunnleggende rettigheter (heretter kalt «pakten») og i artikkel 16 nr. 1 i traktaten om Den europeiske unions virkemåte (TEUV) er det fastsatt at enhver person har rett til vern av personopplysninger om vedkommende selv.
2) Prinsippene og reglene for vern av fysiske personer i forbindelse med behandling av personopplysninger som gjelder dem selv, bør, uavhengig av nevnte personers statsborgerskap eller bosted, respektere deres grunnleggende rettigheter og friheter, særlig retten til vern av personopplysninger. Hensikten med denne forordning er å bidra til å skape et område med frihet, sikkerhet og rettferdighet samt en økonomisk union og å bidra til økonomisk og sosial framgang, til å oppnå en styrking og tilnærming av økonomiene i det indre marked og til fysiske personers velferd.

Figur 9: Personvernforordningens fortale 1 og 2.

Den første fortalen slår fast at personopplysningsvern er en grunnleggende rettighet, basert på to av den europeiske unions sentrale dokumenter. Her settes personvernet i forbindelse med andre lovdokumenter: artikkel 8 nr. 1 i Den europeiske unions pakt om grunnleggende rettigheter og artikler 16 nr. 1 i traktaten om Den Europeiske unions virkemåte. Disse to paragrafene sier nesten nøyaktig det samme: «Everyone has the right to the protection of personal data concerning him or her» (Charter of Fundamental Rights of the European Union, art. 8.1). Den andre fortalen utbroderer dette, men fortsetter med å fortelle, i komprimert form, hva som er formålet med de to målsetningene.

For å forstå disse formålene er det nyttig å trekke inn Traktaten om Den europeiske union. To traktater utgjør i dag det nærmeste man kommer en grunnlov i EU i dag: Traktaten

om Den europeiske unions virkemåte (altså traktaten som blir nevnt i første fortale over) og Traktaten om Den europeiske union. De to traktatene tegner opp EUs verdier, prinsipper, målsettinger og EUs generelle virkemåte. Alle lovgivninger og beslutninger i EU må tas på grunnlag av traktatene, og i tillegg bestemmer de innenfor hvilke områder EU kan lage politikk, det som kalles EUs kompetanse (Olsen et al., 2017, s. 32, 66). De første artiklene i Traktaten om Den europeiske union starter i grove trekk med å etablere EUs formål og ambisjon. Unionen er bygget på "the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights" (Consolidated version of the Treaty on the Functioning of the European Union, 2012, art. 2). "*The Union's aim is to promote peace, its values and the well-being of its peoples*." EU skal videre *skape et område med frihet, sikkerhet og rettferdighet*, og et indre marked skal sikre bærekraftig *økonomisk og sosial fremgang* (Consolidated version of the Treaty on the Functioning of the European Union, 2012, art. 3). Det indre marked utbroderes senere i Traktaten: *"The internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties"* (Consolidated version of the Treaty on the Functioning of the European Union, 2012, art. 26). Det sistnevnte er de såkalte fire friheter som en grunnpilar i det indre marked. Uten at dette nevnes, er altså Personvernforordningen tilnærmet en oppsummering av artikkel 2 og 3 i Traktaten om Den europeiske union. Dette er også karakteristisk for forordningen, den bygger hele tiden på andre EU-dokumenter, noen ganger eksplisitt, og andre ganger mer implisitt, slik som dette.

Traktatene nevnt ovenfor kan ses som en sentral del av EUs juridiske infrastruktur. Med dette blikket utgjør de en form for «installert base» (Star & Bowker, 2002). Personvernforordningen er allerede en del av en infrastruktur som den vokser ut av, og et sett av praksiser som den er en del av. Dette gjør også at den arver styrke og retning fra den juridiske infrastrukturen den er en del av. I visjonsdokumentet skrev også Europakommisjonen at forordningen, i likhet med direktivet fra 1995, skulle realisere to av EUs viktigste ambisjoner: Å beskytte borgernes rettigheter og styrke EUs indre marked, i denne sammenheng, ved å sikre fri flyt av personopplysninger. Dette kommer tydelig til uttrykk også i de to fortalene over. Sett sammen med artikkel 2 og 3 i Traktaten om den Europeiske Union, tolker jeg forordningen som et verktøy for å bygge EUs verdier, som kommer til uttrykk i traktaten, inn praksis knyttet til behandling av personopplysninger. Europakommisjonens visjon om et nytt personvern i Europa, kan slik sett ses som en forlengelse av «prosjektet EU», slik dette kommer frem i traktaten ovenfor. Forordningen er

ikke et hvilket som helst personvern, det er et personvern i EUs bilde; et forvaltningsobjekt som blir artikulert på en slik måte at det passer inn i EUs prosjekt.

Noe av svaret på hvordan de to målsettingene forenes - «vern av fysiske personer i forbindelse med behandling av personopplysninger» og «fri utveksling av personopplysninger» - ligger altså allerede i EU, og er allerede en satt sammen i EUs fundament.

Hva menes så med «fri utveksling av personopplysninger» og hvordan skal dette styrke det indre markedet?

3.3.2 «Enhancing the internal market dimension»[7]

I personvernsforordningens fortale beskrives, i likhet med i visjonsdokumentet, personvernets situasjon:

> Den raske teknologiske utviklingen samt globaliseringen har skapt nye utfordringer med hensyn til vern av personopplysninger. [...] Teknologien har endret både økonomien og det sosiale liv og **bør ytterligere fremme den frie flyt** av personopplysninger i Unionen og overføring av disse til tredjestater og internasjonale organisasjoner**, samtidig som det sikres et høyt nivå for vern av personopplysningene**. (Personvernforordningen, fortale 6)

I motsetning til visjonsdokumentet, eksplisitt «Teknologien» - i bestemt, men uspesifisert form – som et verktøy og virkemiddel for å styrke det indre marked gjennom fri flyt av personopplysninger, med personvernet som forbehold. Teknologien må da her forstås som sterkt knyttet til den digitaliseringen som har skjedd, som muliggjør enkel, rask utveksling av mye data. Jeg tolker dette slik at Personvernforordningen skal legge til rette for teknologi som bidrar til en økt flyt av personopplysninger, som igjen styrker det indre marked. Men forordningen skal altså samtidig sikre at dette skjer på en måte som sikrer vernet av personopplysninger.

Personvernforordningen fortsetter:

> Denne utviklingen krever en sterk og mer sammenhengende ramme for vern av personopplysninger i Unionen støttet av en streng håndheving av reglene, ettersom det er viktig **å skape den nødvendige tillit** som vil gjøre at den digitale økonomien kan utvikle seg i det indre marked. (Personvernforordningen, fortale 7)

Hvem sin og hva slags tillit er det her snakk om? Jeg tolker dette slik at tillit her referer til flere relasjoner og tillit kan betraktes som noe som skal bygges inn i markedet. I borgerens tilfelle kan dette tolkes slik at Personvernforordningen skal skape tillit mellom borgeren og

[7] (Europakommisjonen 2010, s. 11)

den som behandler vedkommendes personopplysninger og teknologien dette gjøres med. Tillit skaper her en bro mellom målet om å verne personopplysninger og målet om å styrke det indre marked. Gjennom å verne personopplysninger, skapes tillit, som igjen øker flyten av personopplysninger.

På dette punktet er det nyttig å trekke inn EUs overordnede strategi for det digitale marked:

> [By creating a connected digital single market] we can create a fair level playing field where all companies offering their goods or services in the European Union are subject to the same data protection and consumer rules, regardless of where their server is based. (Jean-Claude Juncker, daværende president for Europakommisjonen, sitert i Europakommisjonen, 2015)

Det skal kort sagt skapes et digitalt marked på tvers av landegrenser, og markedet skal blomstre, ikke til tross for, men på grunn av personvern. En av de viktigste tiltakene for å skape et slikt «fair playing field», som Juncker referer til, og fri utveksling av personopplysninger er gjennom «harmonisering» i EUs lovverk (Skullerud et al., 2019, s. 36). En av utfordringene som påpekes i visjonsdokumentet ved situasjonen under personvernslovverket fra 1995 er forskjeller mellom ulike lands lover og praksis (Europakommisjonen, 2010, s. 10). Personvernforordningen forsøker å endre denne situasjonen, til dels nettopp ved at den er en forordning, og ikke et direktiv.Et direktiv gir det enkelte land vesentlig større bevegelsesfrihet. En forordning må derimot medlemsland selv vedta ved lov, og det enkelte land kan kun legge til egne bestemmelser innenfor handlingsrommet som allerede finnes i forordningen. Dette er altså to forskjellige dokumentformer med ulike gjennomslagskraft.

> Formålet er å sikre at virksomheter som behandler personopplysninger, skal kunne forholde seg til tilnærmet like regler uansett hvilket land de opererer i, og at borgerne skal vite at de nyter samme personvern, og har de samme rettighetene uansett hvilket av landene tjenestetilbyderen deres er etablert i (Skullerud et al., 2019, s. 36).

Gjennom sterkere regulering og et mer harmonisert europeisk lovverk skal det skapes trygghet og tillit, og på den måten skapes vekst i markedet. Styrket regulering og harmonisering gir de registrerte økt tillit til det digitale marked, samtidig som et harmonisert og konsistent lovverk skal gi markedsaktører trygghet (Europakommisjonen, 2015, s. 13). Harmonisert lovverk og praksis vil på den måten skape det trygge fundamentet som kreves for et grenseløst europeisk digitalt marked (Europakommisjonen, 2015, s. 14–15). Først med et reelt harmonisert lovverk vil et marked med like vilkår og et digitalt marked i vekst kunne

virkeliggjøres. Med andre ord er det altså en form for ordnet og forsvarlig fri flyt av personopplysninger som Personvernforordningen skal bidra til å sikre og styrke.

3.3.3 To målsetninger, én god dataøkonomi

Ved første øyekast synes de to målsetningene i lovens tittel å være helt adskilte. I teksten over blir det imidlertid tydelig at de to ambisjonene gjøres til to sider av samme sak. De to målene settes sammen som to sider av samme mynt, og nevnes i samme åndedrag. De settes sammen på en slik måte at de fremstår som selvfølgelige «samarbeidspartnere» som støtter og styrker hverandre.

Slik som det kommer frem i sitatet fra Juncker, skal personvernet bidra til å skape et sterkt digitalt indre marked i Europa. Formålet slik jeg ser det er å skape et *godt* digitalt marked, i dobbel forstand. Personvernforordningen skal sørge for et godt marked i den forstand at de registrertes grunnleggende rettigheter blir bevart ved å minimere risikoen ved behandling av personopplysninger. Samtidig skal forordningen sikre flyt av personopplysninger og på den måten skape et godt digitalt marked i den forstand at markedet styrkes. Harmonisering av lovverk og økt tillit er to av måtene dette gjøres på. Sett fra dette perspektivet er lovverkets formål verdiskaping i sin bredeste forstand. Loven skal ikke bare verne borgere og deres opplysninger, men også senke risikoen for misbruk av opplysninger, og dermed brudd på grunnleggende rettigheter. Den skal også skape verdi i form av å styrke et marked og skape et bedre grunnlag for flyt av personopplysninger. Loven skal altså sikre personopplysningers verdi på to måter: Personopplysninger er verdifulle fordi de er om fysiske personer, og de er verdifulle som en del av det indre marked. Gjennom regulering skal personopplysninger gjøres til et gode, for de registrerte, for virksomheter som behandler personopplysninger og for økonomien.

3.4 Oppsummering og konkluderende bemerkninger

I dette kapitlet har jeg fulgt Europakommisjonens visjon fra dens artikulasjon i visjonsdokumentet til Personvernforordningen. Jeg har vist hvordan visjonen forsøker å bygge inn og styrke to av EUs målsettinger – og dette gjøres ved å bygge et personvern på en måte som sammenfaller med EUs målsettinger. Dette gjøres ved å artikulere personopplysninger som et verdiobjekt og et risikoobjekt som sammenfaller med EUs målsettinger og verdier. Ved å sette sammen aktører og materialer på en bestemt måte, bygges et kontrollnettverk som skal verne og skape verdi, og samtidig minimere risiko. På denne

måten gjøres også visjonen om et nytt europeisk personvern til en del av visjonen om det jeg har kalt «en god dataøkonomi».

Dette har jeg gjort ved å praktisere praksisorientert dokumentanalyse og med et blikk for infrastruktur. Jeg har fulgt dokumentene, ikke bare som en kilde til informasjon, men i et praksisfelt, som dokumentkjede og som en del av en infrastruktur. Ved å også rette blikket mot de materielle praksisene i og rundt dokumentene, har jeg kunnet vise frem hvordan visjonen bygger på og bygges inn i EUs juridiske infrastruktur.

Kristin Asdal påpeker at dokumenter ikke bare beskriver virkelighet, men at de også kan være med på å endre virkelighet (Asdal, 2015b). Med EUs institusjoner og lovarkiv i ryggen, er Personvernforordningen i så måte et dokument med stort potensiale for å skape endring. Som jeg har vist er forordningen på ingen måte et løsrevet dokument, men en integrert del av EUs prosjekt og EUs juridiske infrastruktur. Dette forteller noe om hva som bygges inn i loven og IT-praksis, men også *hvordan* det bygges inn. Det er altså *ved* å gjøre visjonen og forordningen til en integrert del av EU-prosjektet og EUs juridiske infrastruktur at dokumentet får kraft. Det kan ikke dermed tas for gitt at det som står i forordningen vil bli direkte oversatt til praksis. Fra et ANT-perspektiv skjer det alltid noe i oversettelsen fra et praksisfelt til et annet, eller fra en infrastruktur til en annen. Hvor mye av, og på hvilken måte forordningen blir oversatt til praksis er et empirisk spørsmål, og dette vil jeg behandle videre i resten av oppgaven.

4 «Fra teori til praksis»: Innebygget personvern og prinsippet om ansvarlighet

I forrige kapittel viste jeg hvordan lovdokumentene beskriver et sett av utfordringer drevet frem av en teknologisk utvikling. Lovdokumentene presenterer en visjon for hvordan loven skal løse disse problemene gjennom regulering. Derigjennom skal loven også utøve verdier som både skal verne Europas borgere og styrke et digitalt marked. Men hvilke konkrete verktøy tas i bruk for at disse visjonene og verdiene skal overføres fra lov til IT- og arkivpraksis?

I dette kapitlet følger jeg to konkrete verktøy som beskrives i Personvernforordningen som skal gjøre personvernet til del av organisasjoner og teknologi: innebygget personvern og prinsippet om ansvarlighet. Disse verktøyene blir beskrevet i lovteksten, men alene gir lovteksten i liten grad innsikt i verktøyenes faktiske utforming. For å få innsikt i verktøyene henter jeg inn andre dokumenter. Sagt på en annen måte, følger jeg de respektive verktøyenes dokumentkjeder videre. Jeg bruker mest plass på Datatilsynets veileder for innebygget personvern ettersom den i tydeligst grad operasjonaliserer det «å bygge personvernet inn», og fordi den har sterkest relevans for kapitlet som følger, om hvordan personvern bygges inn i en digital tjeneste.

4.1 Innebygget personvern

Innebygget personvern er ikke et nytt konsept i Personvernforordningen. Innebygget personvern nevnes også i Personvernsforordningens forgjenger, Personverndirektivet fra 1995, men forordningen legger betydelig mer vekt på innebygget personvern (Bygrave, 2017, s. 1). Da Personverndirektivet trådte i kraft i 1995, var personvern først og fremst forstått i ett juridisk perspektiv. Utover 1990-tallet vokste IT-sektoren eksponentielt og ble betraktet som en stadig større kraft i verdensøkonomien. Samtidig skjedde det en dreining mot teknologiske løsninger for personvern. Innebygget personvern kan ses som en forlengelse av to andre slike rammeverk: personvernfremmende teknologier (privacy enhancing technology - PETs) og vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA). Parallelt med utviklingen av disse rammeverkene oppstod det en diskusjon om hvorvidt «loven var nok» for å regulere IT-sektoren og innføre tilstrekkelig personvern (Dijk et al., 2018, s. 4–5). Begrepet lov-etterslep («Law lag») har blitt brukt for å beskrive hvordan loven alltid kommer

på etterskudd, diltende etter teknologiske utviklinger, og dette har blir brukt som et argument for at ulike teknologier utenfor loven selv må tas i bruk og supplere loven for å kunne håndtere personvern i en stadig raskere digitale utvikling (jf. Reidenberg, 1997).

Innebygget personvern kan ses som et av verktøyene som utover 90-tallet ble fremmet i et forsøk på å supplere «vanlig» lovgivning. Disse løsningene kan beskrives som en dreining fra et utelukkende juridisk personvernsparadigme til det Dijk et al. (2018) kaller for «privacy engineering»: en designorientert tilnærming til personvern ved å bygge personvernet inn i IKT. (Dijk et al., 2018, s. 1–2). Van Dijk et al. argumenterer for at denne designorienteringen må ses i forlengelse av to trender i EUs lovgivning: Risiko-orientering «that brings the regulation of personal data processing toward prospective and anticipative management practices» og at personvern i økende grad gjøres av private aktører «through industrial standard setting, certification schemes, codes of conduct and best practices». Sagt på en annen måte er det en bevegelse i hvor og hvem som utfører personvernet, og en redelegering av arbeid og ansvar.

Innebygget personvern defineres i Personvernforordningens artikkel 25: «Innebygget personvern og personvern som standardinnstilling». Den første paragrafen omhandler innebygget personvern, og den behandlingsansvarlige pålegges å «gjennomføre egnede tekniske og organisatoriske tiltak [...] utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger». Den andre paragrafen tar for seg personvern som standardinnstilling: «Den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at det som standard bare er personopplysninger som er nødvendige for hvert spesifikke formål med behandlingen, som behandles». Den tredje paragrafen handler om sertifiseringsmekanismer for innebygget personvern. Disse mekanismene var enda ikke tatt i bruk da jeg samlet inn empiri til oppgaven.

Artikkel 25. Innebygd personvern og personvern som standardinnstilling

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører, skal den behandlingsansvarlige, både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen, gjennomføre egnede tekniske og organisatoriske tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering, og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter.
2. Den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at det som standard bare er personopplysninger som er nødvendige for hvert spesifikke formål med behandlingen, som behandles. Nevnte forpliktelse får anvendelse på den mengden personopplysninger som samles inn, omfanget av behandlingen av opplysningene, hvor lenge de lagres og deres tilgjengelighet. Nevnte tiltak skal særlig sikre at personopplysninger som standard ikke gjøres tilgjengelige for et ubegrenset antall fysiske personer uten den berørte personens medvirkning.
3. En godkjent sertifiseringsmekanisme i henhold til artikkel 42 kan brukes som en faktor for å påvise at kravene fastsatt i nr. 1 og 2 i denne artikkel overholdes.

Figur 10: Personvernforordningen, artikkel 25.

Personvernforordningen selv forteller likevel lite om hvordan innebygget personvern skal gjøres i praksis. I Skullerud et als kommentarutgave til Personverndirektivet (2019, s. 289) viser de til Ann Cavoukians syv steg for innebygget personvern. Prinsippene for innebygget personvern ble først introdusert av personvernmyndighetene i Ontario, Canada på

1990-tallet. Ann Cavoukian utviklet prinsippene før og i løpet av hennes tid som personvernskommisjonær (Information and Privacy Commissioner). Cavoukian argumenterer for at personvernet må bygges inn, og ikke kun kan utføres ved hjelp av juridiske verktøy: «Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation» (Cavoukian, 2011). Sitatet bygger videre på idéen om at loven alene ikke er tilstrekkelig. Andre komplementerende verktøy må tas i bruk for å sikre personvern, og det er nødvendig å bygge personvernet inn i eksisterende praksiser, teknologier og infrastrukturer. Cavoukian spesifiserer også *hvor* personvernet skal bygges inn: "Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure." (Cavoukian 2009, Privacy by design "plakat"). Cavoukians beskrivelse av innebygd personvern inkluderer altså både teknologien eller algoritmene, organisasjon og infrastruktur.

Cavoukians syv prinsipper for innebygget personvern:

1) Vær i forkant, forebygg fremfor å reparere
2) Gjør personvern til standardinnstilling
3) Bygg personvern inn i designet
4) Skap full funksjonalitet
5) Ivareta informasjonssikkerheten fra start til slutt
6) Vis åpenhet
7) Respekter brukerens personvern

(Datatilsynets oversettelse - Datatilsynet, u.å.-a)

Prinsippene er publisert som en egen plakat på to A4-sider, der innebygd personvern og de syv prinsippene beskrives i korte trekk (Cavoukian, 2011). Cavoukians syv prinsipper synes å ha blitt en kanonisk beskrivelse av innebygget personvern, og danner ryggraden for beskrivelsen av innebygd personvern, både hos Datatilsynet og i Skullerud et als kommentarutgave (2019, s. 289).

4.1.1 Datatilsynets veileder

I forlengelse av innføringen av Personvernforordningen, utviklet Datatilsynet i 2018 en veileder for innebygget personvern. Veilederen har tittelen «Programvareutvikling med innebygd personvern», og er rettet mot «utviklere, arkitekter, prosjektledere, testere og personvern- og sikkerhetsrådgivere som utvikler og bidrar til utvikling av, programvare som inneholder personopplysninger» (Datatilsynet, u.å.-c).

Figur 11: Skjermdump fra Datatilsynets nettside (Datatilsynet, u.å.).

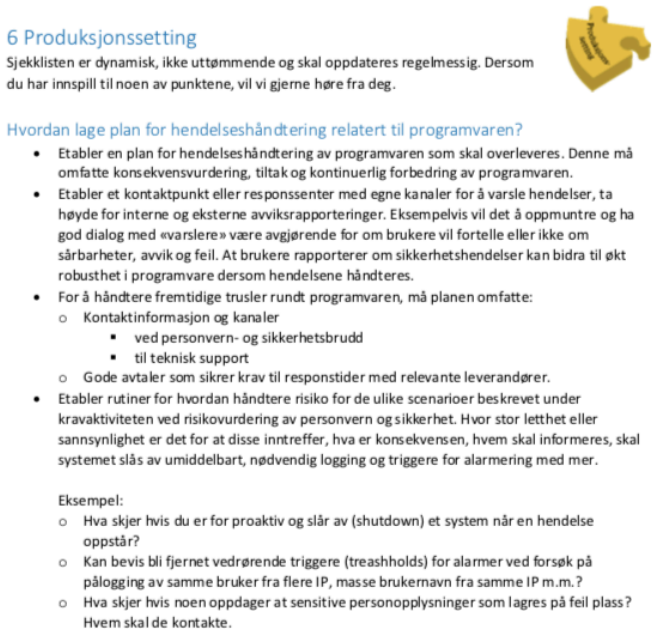
Veilederen tar for seg «Syv aktiviteter i en kontinuerlig prosess»: design, koding, test, produksjonssetting, forvaltning, opplæring og krav. «Veilederen beskriver hver av aktivitetene med våre anbefalinger til hvordan vi mener hver aktivitet bør gjennomføres, og hvilke tiltak som vi anser som viktige for å lykkes med kravet om å bygge personvern inn i en programvare». Veilederen gir en kort og generell beskrivelse av hvordan personvern kan bygges inn i hver av disse aktivitetene. I tillegg til selve veilederen, finnes det vedlegg for hver av aktivitetene, med mer detaljerte beskrivelser og sjekklister. Datatilsynet har også laget en plakat som oppsummerer veilederens hovedpunkter under hver aktivitet (figur 13), denne vil jeg komme tilbake til.

I utskrevet versjon er selve veilederen på 16 sider (uten plakat og sjekklister). Den gir først en kort beskrivelse av hva innebygget personvern er, etterfulgt av en tekst om hvordan personvern bør utføres under hver aktivitet. Under hver aktivitet gis en beskrivelse av hvordan organisasjonen kan innføre personverntiltak innen den gitte aktivitet. I tillegg til disse beskrivelsene som utgjør hoveddelen av veilederen, er det også vedlagt sjekklister til hver av aktivitetene. Sjekklistene omfatter punkter som må utføres for å gjennomføre det datatilsynet anser for å være tilstrekkelige personverntiltak i utviklingsprosessen, og utgjør et par sider per aktivitet.

4.1.2 Å bygge personvern inn i utviklingsprosessen

Veilederen er skrevet i et relativt teknisk språk. Det tas i bruk en del fagtermer, og det vises til mange verktøy, tester og rammeverk som anbefales. Dette gjør at veilederen oppleves som teknisk og lite tilgjengelig for de som ikke er kjent med fagtermene og verktøyene. For de som jobber med utvikling er dette derimot kjente begrepet og verktøy. Veilederen ble også skrevet «i samarbeid med sikkerhetseksperter og programutviklere i privat og offentlig sektor» (Datatilsynet, u.å.-c). I motsetning til Personvernforordningen, og mer spesifikt artikkel 25, som er skrevet i et mer juridisk språk, er veilederen skrevet i et språk som er ment for teknologer og utviklere. Veilederen fungerer slik sett som en oversettelse fra en juridisk kontekst til en IT-kontekst.

Det tas mange grep i veilederen for å konkretisere innebygd personvern. Dette kommer tydelig frem i sjekklistene til hver aktivitet. Sjekklistene omfatter punkter som må utføres for å gjennomføre det Datatilsynet anser for å være tilstrekkelige personverntiltak. Det brukes mye plass i sjekklistene til å eksemplifisere hvordan innebygget personvern kan sikres innen hver aktivitet. Veilederen skal kunne fungere for mange forskjellige utviklingsprosesser, men tar i bruk konkrete eksempler som lar seg generalisere, for å vise hvordan innebygget personvern *kan* utøves. Under noen av aktivitetene i hoveddelen av veilederen er det også nummererte punkter med personverntiltak som organisasjonen bør ta.



6 Produksjonssetting

Sjekklisten er dynamisk, ikke uttømmende og skal oppdateres regelmessig. Dersom du har innspill til noen av punktene, vil vi gjerne høre fra deg.

Hvordan lage plan for hendelseshåndtering relatert til programvaren?

- Etabler en plan for hendelseshåndtering av programvaren som skal overleveres. Denne må omfatte konsekvensvurdering, tiltak og kontinuerlig forbedring av programvaren.
- Etabler et kontaktpunkt eller responssenter med egne kanaler for å varsle hendelser, ta høyde for interne og eksterne avviksrapporteringer. Eksempelvis vil det å oppmuntre og ha god dialog med «varslere» være avgjørende for om brukere vil fortelle eller ikke om sårbarheter, avvik og feil. At brukere rapporterer om sikkerhetshendelser kan bidra til økt robusthet i programvare dersom hendelsene håndteres.
- For å håndtere fremtidige trusler rundt programvaren, må planen omfatte:
  - Kontaktinformasjon og kanaler
    - ved personvern- og sikkerhetsbrudd
    - til teknisk support
  - Gode avtaler som sikrer krav til responstider med relevante leverandører.
- Etabler rutiner for hvordan håndtere risiko for de ulike scenarioer beskrevet under kravaktiviteten ved risikovurdering av personvern og sikkerhet. Hvor stor letthet eller sannsynlighet er det for at disse inntreffer, hva er konsekvensen, hvem skal informeres, skal systemet slås av umiddelbart, nødvendig logging og triggere for alarmering med mer.

Eksempel:

- Hva skjer hvis du er for proaktiv og slår av (shutdown) et system når en hendelse oppstår?
- Kan bevis bli fjernet vedrørende triggere (treashholds) for alarmer ved forsøk på pålogging av samme bruker fra flere IP, masse brukernavn fra samme IP m.m.?
- Hva skjer hvis noen oppdager at sensitive personopplysninger som lagres på feil plass? Hvem skal de kontakte.

Figur 12: Sjekkliste for produksjonssetting fra Datatilsynets veileder.

På denne måten minner veilederen om en bruksanvisning for innebygget personvern, et verktøy som tar programutviklingen gjennom innebygget personvern, skritt for skritt, innenfor hver aktivitet. Dersom hvert punkt kan krysses av på listen, burde organisasjonen kunne føle seg relativt trygg. Dette står i tydelig kontrast til både Personvernforordningen og Cavoukians plakat. Ingen av disse forteller hvordan innebygget personvern skal gjøres i praksis, de tilbyr mål og prinsipper, men sier lite om hvordan disse skal oppnås. Veiledere forsøker å bidra med noe nytt: en mer konkret og direkte oversettelse av prinsippene i loven, rettet mot programutviklere.

Figur 13: "Plakat over de syv fasene i programvareutvikling med innebygd personvern", hentet 22.6.20 fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/programvareutvikling-med-innebygd-personvern/

Sjekklistene utgjør et slikt verktøy for oversettelse av lovens prinsipper inn i programutvikleres kontekst. Et annet er veilederens plakat. Plakaten består av de samme elementene som figuren i begynnelsen av veilederen: de syv aktivitetene i en sirkel, presentert som puslespillbiter. Hver aktivitet har her blitt komprimert til noen få punkter. Disse punktene er trukket frem som det viktigste som må gjennomføres for å utføre aktiviteten på en tilfredsstillende måte for å oppfylle kravene til innebygget personvern. Denne komprimeringen og fremhevingen er til dels en virkning av plakatformatet eller -sjangeren. Plakater preges av et komprimert budskap i en lettfattelig tekst, og har vanligvis som mål å nå ut til mange. En plakat som denne kan henges opp og fungere som en påminnelse. Lengre tekster leses ofte bare en gang, en plakat som denne kan fungere som en oppfrisker, med nøkkelord og slagord som har som funksjon å skape en gjenerindring av latent kunnskap. Den komprimerte teksten gir «knagger» og en komprimert sjekkliste for hvordan personvernet skal gjøres under de ulike aktivitetene i utviklingsprosessen. Plakaten, med sine visuelle og kommunikative virkemidler, er selv en måte å gjøre stegene til del av den enkelte arbeidsplass. Der vil den forhåpentligvis blir hengende på en vegg og minne om å ta i bruk kunnskapen om personvern som ellers lett blir glemt. Plakaten blir på denne måten i seg selv et verktøy for å bygge inn personvern på en helt konkret måte, ved å bli en del av kontorlandskapet der programvare blir skapt. Dette blir slik sett også en måte å gjøre personvernet til en del av fysisk infrastruktur og materiell IT-praksis.

Aktivitetene og utviklingsmetodikken spiller en sentral rolle i veilederen. Den beskriver hvordan innebygget personvern ser ut fra hver av aktivitetene i en utviklingsprosess. På den måten forsøker veilederen å konkretisere personvern for utviklere og vise hvordan personvern kan gjøres til praksis fra perspektivet til de forskjellige aktivitetene som inngår i prosessen. Under hver aktivitet er det også spesifisert hvem som er målgruppen for denne

delen av veilederen. På den måten blir hver aktivitet spisset inn for ulike deler av organisasjonen. Aktivitetene i veilederen tar utgangspunkt i ulike standardrammeverk for utviklingsmetodikk (Microsoft Security Development Lifecycle og Secure Software Development LifeCycle), men er tilpasset formålet. Samtidig skal aktivitetene være fleksible nok til å kunne tilpasses den metodikken som virksomheten bruker.

I figuren som fremstiller prosessen representeres hver av aktivitetene som en puslespillbit i en sirkel for å vise at aktivitetene henger sammen, en aktivitet fører til den neste, og prosessen er kontinuerlig. Ved å fokusere på hele utviklingsprosessen i veilederen, er det ikke bare de som jobber direkte med den tekniske løsningen som skal utvikles - slik som kodere og designere - som må ta hensyn til personvern, men hele organisasjonen som er knyttet til utviklingen. Det er ikke bare selve teknologien og de tekniske løsningene som personvernet må bygges inn i. Fagdirektøren i Datatilsynet understreker også at personvernet må trekkes inn i prosessen før en starter selve utviklingen av produktet (Intervju, fagdirektør i Datatilsynet). For å bygge personvernet inn i en teknisk løsning, holder det ikke at en utvikler stopper opp og tenker på personvern i et par minutter, personvernet må ligge til grunn for hele utviklingsprosessen, og må bygges inn i organisasjonen.

Faglederen i Datatilsynet understreker også at det er nødvendig at den enkelte utvikler har mer kunnskap om personvern en det som har vært tilfellet tidligere: «Det å lære deg hva de registrertes rettigheter og friheter er - hvis du ikke skjønner hva de registrertes rett/friheter er, eller hva prinsippene er så kan du ikke heller utvikle en app som innehar det» (Intervju, fagdirektør, Datatilsynet). En av aktivitetene i veilederen er «opplæring». Utviklere må ha grunnleggende forståelse for hva personvern *er* og hva det innebærer i utviklingen av programvare. Det holder ikke at utviklerne vet *at* programvaren skal ha innebygget personvern, de må ha en mer substansiell forståelse av personvernets definisjoner og prinsipper.

Aktivitetene er valgt for å sikre at veilederen skal kunne passe til ulike utviklingsprosesser. Likevel legger veilederen noen føringer for hvordan utvikling bør utføres. I intervjuet med fagdirektøren i Datatilsynet, påpekte hun at det å jobbe ut fra en utviklingsmetodikk er en forutsetning for å være en «seriøs» aktør. «Det har med profesjonalitet å gjøre [...] Det kan ikke være sånn: Oi, nå husket jeg på akkurat det. Du må vise at du har en struktur». Ved å ta utgangspunkt i utviklingsmetodikken, fordrer veilederen til «seriøs» programmering. Innebygd personvern er ikke bare et separat krav som uten videre kan bygges inn i en utviklingsprosess. Jeg tolker dette slik at veilederen gjennom

vektleggingen av utviklingsmetodologier også legger føringer for hva som er god utvikling, og dermed bidrar til å fremheve bestemte IT-praksiser.

4.1.3 En veileder for og av teknologer

Datatilsynet har valgt å fokusere på en mindre, mer teknisk, del av lovverket, og veilederens målgruppe er ikke nødvendigvis de som bærer hovedvekten av ansvaret i følge lovgivningen. Personvernforordningen legger hovedvekten av ansvaret på «behandlingsansvarlig», den som «bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes», altså ikke nødvendigvis den som utvikler programvaren. På denne måten skilte veilederen seg ut da den ble publisert. Den ble tatt i bruk av ulike internasjonale organisasjoner internasjonalt, og andre datatilsyn i Europa brukte veilederen som utgangspunkt (intervju fagleder, Datatilsynet). Det kan altså virke som det fantes et behov for det Datatilsynets veileder hadde å tilby. Også det Europeiske personvernrådet (European Data Protection Board) har i ettertid publisert en veileder knyttet til artikkel 25, men denne er mer generell og fokuserer ikke på utviklingsprosessen slik som Datatilsynets veileder.

I intervjuet med faglederen i Datatilsynet, begrunner hun dette valget:
«[V]i har grepet fatt i noe som er teknisk og som jeg tror er uhyre viktig for at vi skal få personvern i fremtiden, fordi vi digitaliserer så mye og fordi vi legger igjen spor etter oss over alt. [Hvis] vi ikke klarer å nå digitaliseringen og softwaren med innebygget personvern så får vi ikke personvern i fremtiden». Faglederen vektlegger den sentrale rollen som «teknologer», som hun selv identifiserer seg som, og utviklere spiller i det hun beskriver som å «materialisere personvernet ned i teknologien». Det å nå frem til utviklerne fremstod i intervjuet som en viktig motivasjon for å skrive veilederen.

Jeg tolker disse sitatene slik at teknologien og teknologene blir til de sentrale aktørene for personvernet. Uten at teknologien og teknologene innrulleres i «personvern-programmet», lar ikke personvernet seg gjennomføre. Sammenlignet med teksten i visjonsdokumentet og Personvernforordningen, skjer det her et skifte mot teknologien og teknologene som de sentrale aktørene. Det betyr ikke at de ikke lar seg kombinere, men at tyngdepunktet forflyttes.

Faglederen påpeker også at Personvernforordningen kan være abstrakt og vanskelig tilgjengelig: «[Personvernforordningen] favner så mye, og samtidig så lite. Så derfor så trenger man tolkninger ... Hva er [innebygget personvern], hvordan kan vi tolke det og hvordan kan vi sette det ut i virkelighet sånn at folk forstår det?» (intervju fagleder).

Veilederen spiller altså ikke bare en viktig rolle i å bygge personvernet inn i teknologien direkte, men også i å tolke og formidle personvernet i en teknologisk kontekst, ettersom behandlingen av personopplysninger i så høy grad skjer i digitale løsninger. Teamet som skrev veilederen er derfor også hovedsakelig bestående av folk som jobber med programvareutvikling. På denne måten blir også veilederen til et viktig tolkningsverktøy som skal konkretisere personvernet i et språk som teknologene forstår. Slik jeg tolker sitatet ovenfor, blir veilederen på denne måten et verktøy for å «sette [personvernet] ut i virkeligheten», og dette gjøres ved at veilederen er skrevet av og for teknologer. Veilederen og Datatilsynets arbeid blir dermed en sentral brikke i å sørge for at personvernet faktisk blir praktisert, og i oversettelsen fra juridisk praksis til IT-praksis. Denne veilederen og Datatilsynet er så klart ikke de eneste som står for denne oversettelsen, men en del av det arbeidet som her blir beskrevet som nødvendig for å bygge personvernet inn i teknologien.

4.1.4 Veilederen som verktøy

Veilederen kan ses som et verktøy for å bygge inn personvern. Det gjør den i kraft av å nettopp være en veileder og ved å ha den posisjonen som den har.

Datatilsynet er et uavhengig forvaltningsorgan og er både tilsyn og ombud, og definerer sin oppgave til «å føre kontroll med personvernregelverket og medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem». Datatilsynet er Norges «tilsynsmyndighet» etter Personvernforordningen, artikkel 51. Med Datatilsynet som avsender, får veilederen autoritet på området. Veilederen er ikke juridisk bindende, men den vil tillegges vekt dersom relevante saker blir tatt opp i retten: «Den er ikke juridisk bindende, men du må komme med gode grunner hvis du skal gå mot den. Da må du nesten vise at du skal ha gjort bedre vurdering enn oss» (Intervju, jurist i Datatilsynet).

Samtidig som Personvernforordningen legger tydelige føringer for Datatilsynets veileder, ligger det også en fleksibilitet i en veileder som denne. Teamet som har utviklet den, har måttet skrive den slik at den er i tråd med Personvernforordningen, men i «oversettelsen» fra juridisk praksis til en IT-praksis har de også hatt en frihet i å kunne utforme veilederen slik de ønsker. Dette kommer til uttrykk i hva veilederen velger å fokusere på og hvordan den er utformet. Eksempelvis velger veilederen å ta utgangspunkt i en bestemt utviklingsmetodikk. På den måten legger også veilederen noen føringer for hva som er de viktigste aspektene i utvikling, og hva som er god utvikling, og den forteller noe om hva slags utvikling som lar seg forene med Personvernsforordningens krav.

Datatilsynets veileder kan ses som en del av, og en utvidelse av, en dokumentkjede der Personvernforordningen utgjør en slags kjerne. I dokumentkjeden utgjør veilederen et verktøy for å bygge inn personvernet. Den forsøker å utgjøre et mellomledd mellom loven og utviklere av programvare. Slik sett er veilederen et verktøy for å bygge inn personvern i IT-praksis (eller eventuelt for å bygge inn *innebygget* personvern). Dette gjøres også i veiledningsdokumentet ved å tilby et verktøy for organisasjoner som utvikler programvare. En stor andel av det som står i Datatilsynets veileder finnes ikke konkret i Personvernforordningen. Veilederen bidrar slik sett med en egen utvidet versjon av personvernet som vi får presentert i Personvernforordningen, konkretisert for programvareutviklere.

4.2 Accountability

4.2.1 Accountabilty-begrepet

Prinsippet om ansvarlighet dukker som nevnt opp i Personvernforordningens prinsipper for behandling av persondata. I Personvernforordningen er «accountability» overstatt til ansvarlighet. Her forsvinner imidlertid viktige nyanser i oversettelsen. «Accountability» overlapper med, men kan ikke reduseres til ansvarlighet . Ordet har sitt opphav i betydningen «state of being answerable» («Accountability», u.å.). Dette har blitt trukket frem som en utfordring med begrepet i sammenheng med overnasjonal lovgivning i EU fordi ordet vanskelig lar seg oversette til andre språk. Andre overlappende begreper som brukes på engelsk er “responsibility”, “assurance”, “reliability”, “trustworthiness” (Artikkel 29-gruppen, 2010, s. 7–8), “liablility” (Raab, 2012, s. 16) og “transparency” (Cool, 2019).

Giovanni Buttarelli, lederen for Europas Datatilsyn, beskriver «accountability» som noe mer enn lovlydighet: «Being accountable for data processing is not a substitute for compliance with the applicable legal obligations. It should be understood as an ethical responsibility for activities that take place for a given purpose, whether profit making, law enforcement, social care, or research—or even a combination of them» (Buttarelli, 2016). Også den nærmeste norske oversettelsen, «ansvarlighet», peker mot en moralsk verdi. Samtidig krever accountability det å *kunne* svare for og å kunne dokumentere sine handlinger. Å være «accountable» krever både den rette praktiske kunnskapen og de rette tekniske innretninger som gjør det mulig å gi et tilfredsstillende svar dersom spørsmålet blir stilt. I sammenheng med personvern, er accoutability dermed også et teknologisk og praktisk

anliggende. For at en organisasjon skal være «accountable», må det kunne dokumenteres at relevante handlinger er ansvarlige.

Accountability-begrepet i personvernsforordningen kan ses som en større langvarig trend på mange ulike samfunnsområder. Michael Power (1997) har kalt denne trenden for en «audit explosion», karakterisert av en form for styring som preges av evaluering og etterprøving. Power viser til at denne formen for styring vokste eksponentielt fra 1980-tallet, og knytter den til en modernisering av offentlig sektor som ofte blir assosiert med «New Public Management». Staten påtar seg en tilsynsrolle, samtidig som ansvar og kontroll i økende grad blir forskjøvet inn i organisasjoner og bedrifter. Forutsetningen for denne formen for styring er at organisasjonene som skal forvaltes blir «accountable».

4.2.2 Prinsippet om ansvarlighet og personvern

Accountability-begrepet er ikke nytt innen personvern. Accountability som et personvernsprinsipp har opphav i OECDs veiledning fra 1981, «Guidelines on the Protection of Privacy and Transborder Flows of Personal Data» (Raab, 2012). Bennett (2012) påpeker at accountability alltid har vært implisitt i personvernslovgivning, men i motsetning til personvernsforordningen fra 1995, gjøres accountability eksplisitt med Personvernforordningen.

«Accountability» har, som nevnt, blitt oversatt til «ansvarlighet», og prinsippet i Personvernforordningen (art 5.2) (engelsk: «Accountability principle») er blitt oversatt til «prinsippet om ansvarlighet». Jeg vil heretter omtale disse i sin norske språkdrakt.

Artikkel 29-gruppen var EUs arbeidsgruppe for personvernspørsmål, og var sammensatt av medlemsstatenes datatilsynsmyndigheter. Navnet hadde sitt opphav fra artikkel 29 i Personverndirektivet fra 1995 (Skullerud et al., 2019, s. 42). Med Personvernforordningen ble artikkel 29-gruppen oppløst og erstattet av Personvernrådet (European Data Protection Board) med utvidet ansvar og makt (Personvernforordningen artikkel 68). I 2010 skrev Artikkel 29-gruppen en uttalelse («opinion») om prinsippet om ansvarlighet. I visjonsdokumentet er det uttalelsen fra Artikkel 29-gruppen som det refereres til når det begrunner hvorfor prinsippet om ansvarlighet må lovfestes. Artikkel 29-gruppen var altså en sentral aktør i denne sammenhengen. Både i visjonsdokumentet og i artikkel 29-gruppens uttalelse beskrives prinsippet om ansvarlighet som en viktig del av svaret på hvordan personvern skal bygges inn. Artikkel 29-gruppen viser i sin uttalelse til at EUs personvernlovgivning så langt ikke har blitt tilstrekkelig etterlevd i datapraksiser: «Unless

data protection becomes part of the shared values and practices of an organization, and responsibilities for it are expressly assigned, effective compliance will be at considerable risk, and data protection mishaps are likely to continue» (Artikkel 29-gruppen, 2010, s. 2). Å gjøre et ansvarlighetsprisipp til lov vil bidra til å omgjøre personvern fra «teori til praksis», slår artikkel 29-gruppen fast: «Data protection must move from 'theory to practice'. Legal requirements must be translated into real data protection measures» (Artikkel 29-gruppen, 2010, s. 3). Når Europakommisjonen tar opp tråden videre i visjonsdokumentet, blir prinsippet om ansvarlighet trukket frem som det nødvendige verktøyet for å heve de behandlingsansvarliges ansvar (Europakommisjonen, 2010). Prinsippet om ansvarlighet fremstilles altså som en nøkkel for å bygge inn personvern i behandlingen av personopplysninger.

I Skullerud et als kommentarutgave legges uttalelser fra Artikkel 29-gruppen og Personvernrådet til grunn som «viktige og tunge rettskilder» (2019, s. 41). Artikkel 29-gruppens dokument er med andre ord et sentralt dokument i dokumentkjeden knyttet til prinsippet om ansvarlighet. Dokumentet utgjør en form for ekspertuttalelse som på den ene siden hadde innvirkning på lovgivningsprosessen, og på den andre siden blir lest som en autoritativ kilde når lovverket skal tolkes. I tillegg til å vise hvilken rolle dokumentet spiller i dokumentkjeden knyttet til prinsippet om ansvarlighet, viser dette at datatilsynene i EU (og EØS) har stor påvirkningskraft i lovarbeidet både før og etter at Personvernforordningen trådte i kraft.

Til tross for at prinsippet bare utgjør én setning i den endelige Personvernforordningen, som fastslår at «den behandlingsansvarlige er ansvarlig for og skal kunne påvise at [prinsippene] overholdes», tillegges prinsippet en sentral posisjon. Som jeg viste til i forrige kapittel, kommer «accountability-prinsippet» til slutt i artikkel 5, Prinsipper for behandling av personopplysninger, og «pålegger den behandlingsansvarlige å påse og påvise at prinsippene blir overholdt» (Skullerud et al., 2019, s. 105). Artikkel 29-gruppen påpeker i sin uttalelse at «[I]ts emphasis is on showing how responsibility is exercised and making this verifiable» (Artikkel 29-gruppen, 2010). I praksis betyr prinsippet altså at den behandlingsansvarlige skal kunne vise og dokumentere at de behandler personinformasjon i tråd med Personvernforordningen. Dette kan umiddelbart virke som en selvfølge: Burde ikke dette være en konsekvens av lovgivningen også uten et slikt prinsipp? Likevel ses dette altså som en ny utvikling innen personvernslovgivning (Bennett, 2012). Dette indikerer at prinsippet likevel utgjør en viktig forskjell. Med prinsippet om ansvarlighet får den behandlingsansvarlige en større del av ansvaret og en økt dokumentasjonsbyrde for å sikre og

vise at behandlingen av personopplysningen er i tråd med lovgivningen. På denne måten bygger prinsippet ansvar og «accountability» inn i den enkelte behandlingsansvarlige organisasjon. Som Power påpeker, representerer dette en spesifikk form for styring der ansvar og kontroll blir flyttet fra stat og inn i organisasjoner. Slik sett er også «accountability» et verktøy for å distribuere ansvar, og på den måten rekonfigurere relasjonen mellom aktører.

4.3 Oppsummering og konkluderende bemerkninger

Jeg har pekt på innebygget personvern og prinsippet om ansvarlighet som to verktøy for å gjøre personvernet til en del av organisasjon og teknologi. Ansvarlighetsprinsippet forsøker å bygge ansvaret for personvern inn i organisasjoner. Slik sett er det et verktøy for å distribuere ansvar. Innebygget personvern forsøker å bygge inn personvernet i tekniske løsninger og inn i organisasjonene som utformer og står ansvarlige for løsningene.

I dette kapitlet har jeg vist hvordan dokumenter i forlengelse av Personvernforordningen bidrar til å utøve EUs personvern, og her har jeg fulgt verktøyene videre inn i noen slike dokumenter, og vist frem akkurat hvordan verktøyene forsøker å bidra til å «bygge inn» personvernet. På denne måten utgjør også dokumentene selv verktøy for å «bygge inn». Dokumentene i dette kapitlet gjør dette på ulike måter, og har ulike posisjoner i sine respektive dokumentkjeder. Artikkel 29-gruppens uttalelse ble tatt i bruk av Europakommisjonen i utarbeidelsen av lovverket og deretter i kommentarutgaven i tolkningen av lovverket som en rettskilde. Dokumentet ble altså brukt både som en ekspertuttalelse og som et tolkningsverktøy. Datatilsynets veileder er et dokument rettet mot programutviklere, og forsøker å være en slags oversettelse og en bro fra det juridiske feltet til IT-feltet. Veilederen, og innebygget personvern som helhet, skal være et verktøy for å overføre personvern fra lovdokumentene, over i IT-feltet, der det skal «materialiseres ned i» algoritmene. På hver sin måte bidrar dokumentene i dette kapitlet til å bygge personvernet inn i informasjonsinfrastruktur: i organisasjoner og digital teknologi. Som sådan kan verktøyene og dokumentene i dette kapitlet betraktes som infrastrukturering: de utvider og modifiserer infrastruktur.

I en viss forstand kan dokumentene ses som en slags utvidelse av lovverket - som en slags lovens lange arm. Dokumentene bygger videre på hverandre, og selv om selve lovdokumentet utvilsomt spiller en sentral rolle, er det *sammen* med mange andre dokumenter at lovdokumentet får den effekten det har. Slik sett har også verktøyene, innebygget

personvern og prinsippet om ansvarlighet, og de respektive dokumentkjedene også som oppgave å bygge personvern *ut* av loven.

Dette tar oss tilbake til diskusjonen om hvorvidt «loven er nok» og lovens «law lag». Innebygget personvern og accountability kan ses som verktøy som forsøker å gjøre lov på nye måter, og andre steder. De er verktøy som forsøker å bygge lovens ansvar og prinsipper *ut fra* loven og *inn i* informasjonsinfrastruktur. Det at verktøyene og dokumentene i dette kapitlet kan ses som en utvidelse av lovverket betyr imidlertid ikke at dokumentene i dette kapitlet er nøytrale medium som formidler lovgivningen. Dokumentene og verktøyene er også med på å forme hvordan personvern «bygges».

Van Dijk et al. argumenterer for at innebygget personvern kan ses i forlengelse av to trender: risikoorientering og privatisering av ansvar. Begge disse aspektene finne vi også igjen i Powers argumentasjon om «accountability» som en del av det han kaller «audit society». Disse tendensene er også til stede i de to verktøyene jeg har analysert i dette kapitlet. Ansvarlighetsprinsippet kan ses som en form for distribuering av ansvar og innebærer en spesifikk form for styring der. Innebygget personvern betyr også i praksis at ansvaret i høyere grad tillegges den enkelte organisasjon. Risikoorienteringen er også tydelig i Datatilsynets veileder. Hensynet til personvernet blir i veilederen allestedsnærværende: i hele utviklingsprosessen, hele organisasjonen, og ikke minst i relasjonen til aktører utenfor organisasjonen.

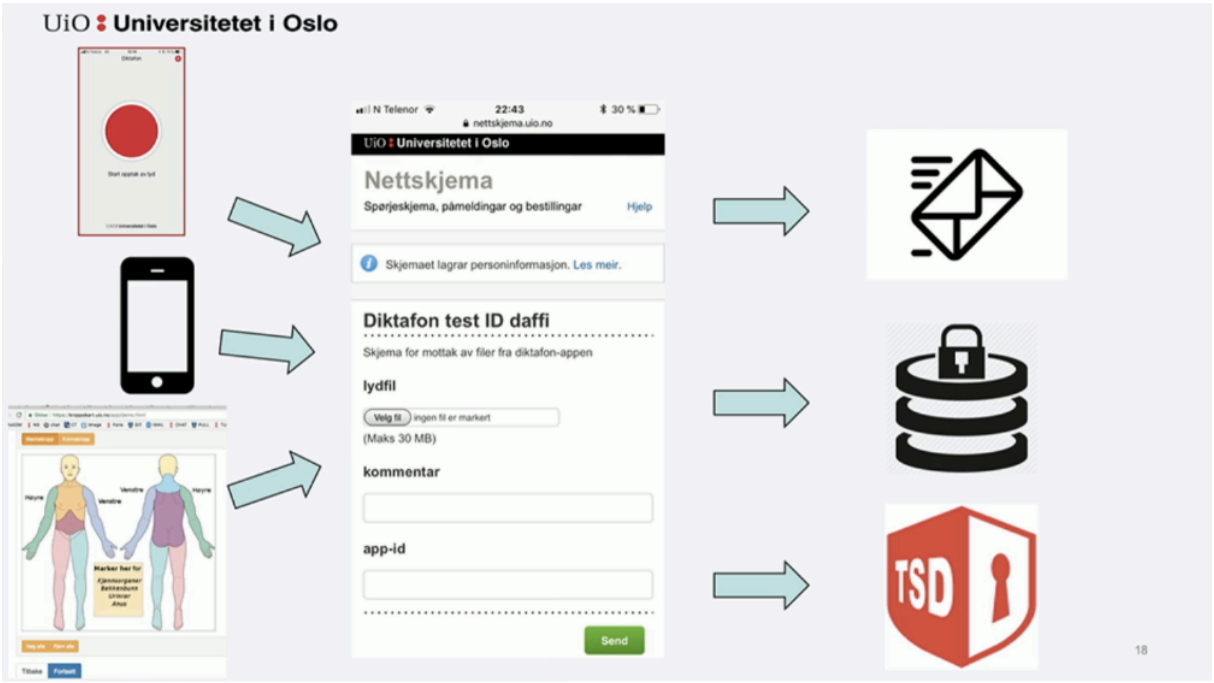
5: Å bygge inn personvern i IT-praksis: Nettskjema

I dette kapitlet vil jeg undersøke hvordan kravene fra Personvernforordningen gjøres til en del av IT-praksis. Dette gjør jeg ved å analysere en digital tjeneste og organisasjonen som utvikler denne tjenesten: USIT (Universitetets senter for informasjonsteknologi) og Nettskjema. Jeg starter med å beskrive Nettskjema, den tjenesten Nettskjema tilbyr og hvordan den bygger på en digital infrastruktur. Dette gjør jeg for å vise frem hvordan en tjeneste for behandling av personopplysninger ser ut i denne sammenhengen, og for å beskrive en slik teknologi og infrastruktur som personvernet skal bygges inn i. Deretter analyserer jeg hvordan personvern oversettes til IT-praksis: Hvordan blir personvernet til en del av utviklernes praksis, og hvordan bygges personvernet inn i Nettskjema. Her bygger jeg på empiri fra intervju med en utviklingsleder i USIT, en video-presentasjon om innebygget personvern og analyse av Nettskjema.

5.1 Nettskjema: databasens portvokter

Nettskjema er en digital tjeneste for datainnsamling, utviklet og opprettholdt av Universitetets senter for informasjonsteknologi (USIT) ved Universitetet i Oslo. USIT er en IT-organisasjon under Universitetet i Oslo med ansvar for å levere IT-infrastruktur, tjenester og løsninger for universitetet. USIT er også et kompetansesenter for IT for hele Høgskole og universitetssektoren i Norge. (USIT, u.å.-b). For forskere og ansatte ved universiteter og høgskoler i Norge som skal samle inn personopplysninger til ulike prosjekter er Nettskjema et verktøy for å samle inn slik data på en trygg måte (USIT, u.å.-c). Løsningen er blitt anerkjent som en trygg løsning i denne sammenhengen av Norsk senter for forskningsdata (Høgskolen i Innlandet, u.å.). Flere universiteter og høgskoler anbefaler å bruke Nettskjema for innsamling av personopplysninger, og i noen tilfeller er det eneste tillate spørreskjemaverktøy for sensitiv informasjon.[8] Nettskjema blir dermed en form for obligatorisk passasjepunkt for forskere i Norge som skal samle inn personopplysninger gjennom spørreskjema.

[8] https://www.inn.no/bibliotek/skrive-og-referere/nettskjema-verktoey-for-datainnsamling, http://bibliotek.usn.no/forskerstotte/forskningsdata/innsamling-lagring-og-arkivering-av-forskningsdata/, https://www.hiof.no/tjenester/it/programvare/nettskjema/



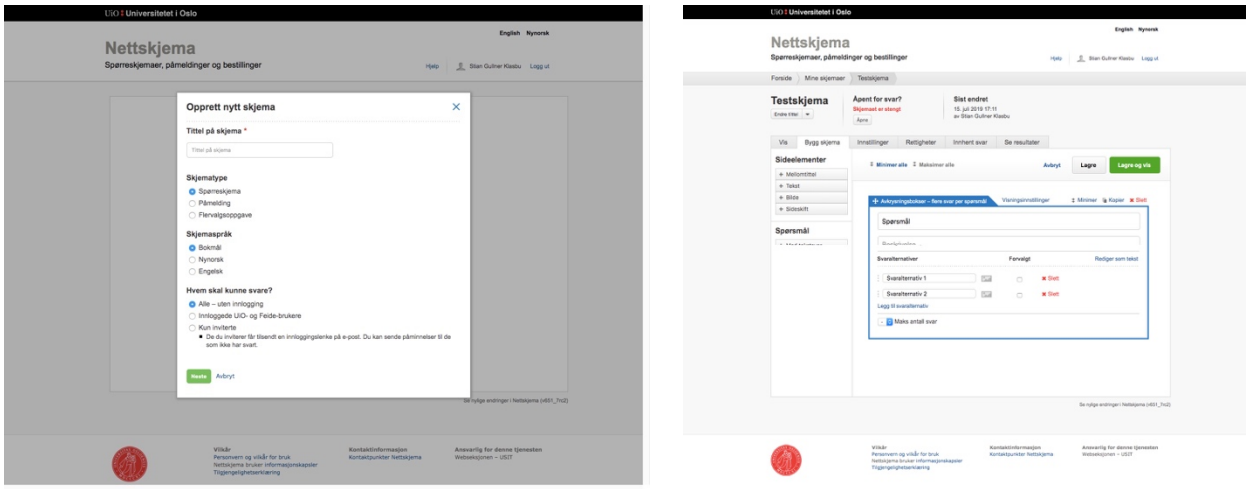
Figur 14: Skjermdump fra USITs presentasjon om innebygget personvern.

Nettskjema er en løsning for et sett av brukere som setter sammen skjema (kalt skjemaeiere), som, når skjemaet er klart, presenterer skjema for brukere (kalt respondenter), altså de som skal fylle inn skjemaet. Slik sett har Nettskjema flere typer brukere, avhengig av hvor disse inngår i prosessen. Nettskjema er også en løsning for å laste dataene fra respondenter inn i databaser på en sikker måte. I tillegg omfatter Nettskjema-tjenesten lagring av informasjonen i databaser, hvor det kun er skjemaeier som har mulighet til å hente ut informasjonen fra databasen. Nettskjemas brukstilfeller deles inn i forskning (der brukere er forskningsobjekter og forskere er «skjemaeier») og administrative formål (der brukerne er ansatte og studenter ved universitetet).

Fra skjemaeiers perspektiv er nettskjema en løsning for innhenting av informasjon. Sett fra dette perspektivet er første steg i prosessen å stille spørsmål. Nettskjema er i dette steget en løsning for å utforme selve skjemaene som senere skal brukes til å samle inn informasjon om respondenter. Brukeren av Nettskjema på dette punktet er skjemaets eier.

Når et skjema skal lages, blir skjemaeieren presentert med et eget skjema for å lage skjema. Nettskjema er altså, i informasjon-innsamlingsprosessen, først et skjema for å lage skjema, et slags «metaskjema», med spørsmål om hvilke spørsmål som skal stilles og hvordan de skal stilles. Nettskjema er dermed en del av en infrastruktur som er der allerede, før spørsmålene som skal besvares er stilt.

Når skjemaet er gjort klart, kan skjemaet deles med respondenter. Når en respondent trykker på en lenke til et skjema, blir brukeren enten bedt om å logge inn og identifisere seg gjennom «ID-porten» eller «Feide», eller brukeren er anonym, alt etter hva skjemaeieren har valgt for sitt skjema. Etter at respondenten har fylt inn et skjema lastes dette inn i databasen via en sikker kryptert overføring av data.



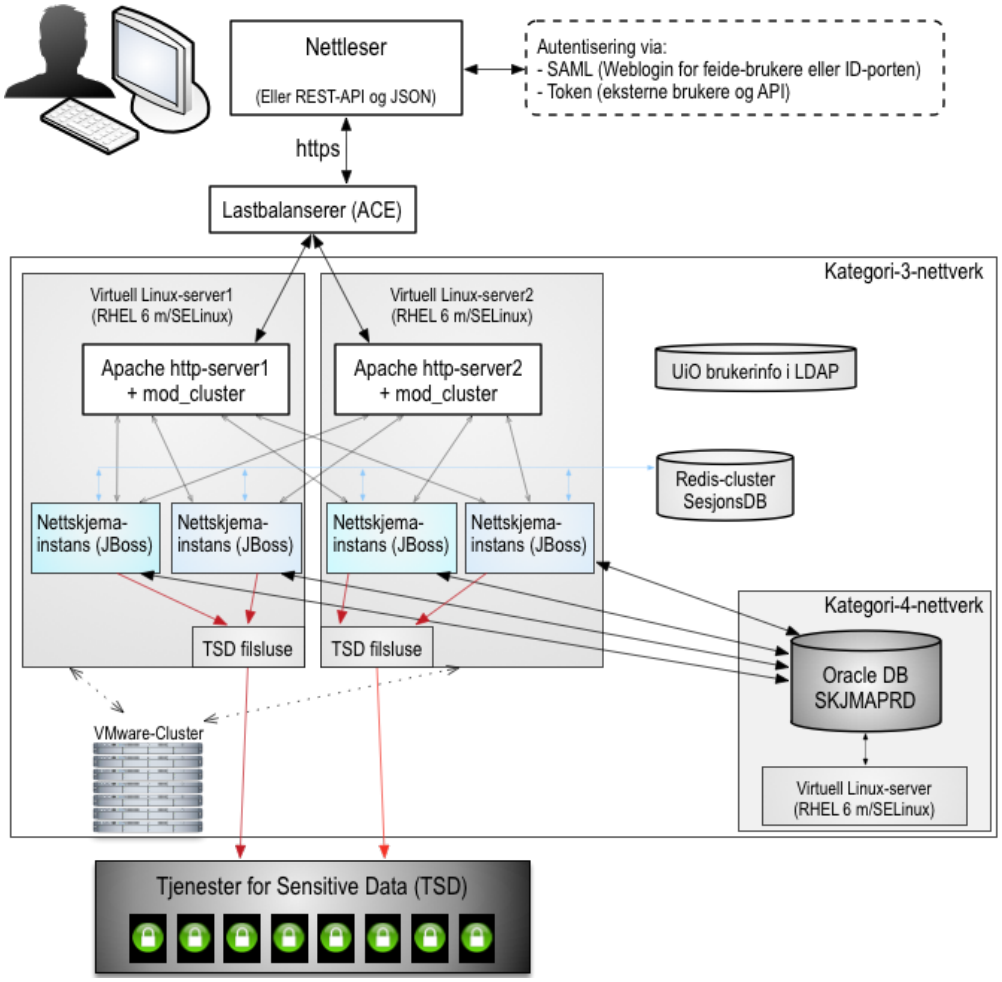
Figur 15: Skjermdump fra Nettskjema. (Hentet 10.1.2020)

Nettskjema er altså en sammensatt teknisk løsning, men tjenestens kjerne er sentrert rundt «skjema» for informasjonsinnhenting. «Skjemaet» kan komme i mange ulike former, og er ikke nødvendigvis et skjema som brukeren fyller inn. Det kan eksempelvis også være et bilde eller en lydfil som lastes opp via en mobil-app, men også i et slikt tilfelle vil filen lastes inn i «skjemaet» før informasjonen lastes opp og lagres i selve databasen. Nettskjema blir på den måten midtpunktet eller portalen som all informasjon fores gjennom før den når frem til databasen.

5.1.1 Nettskjemas digitale infrastruktur

Den tekniske infrastrukturen bak Nettskjema beskrives på USITs nettsider under overskriften «Teknisk systembeskrivelse for Nettskjema», illustrert av flytskjema i figur 16. Flytskjemaet viser hvordan en internett-plattform som Nettskjema består av kompleks struktur av tekniske løsninger, standarder, protokoller og ulike kodespråk. Nettskjema er med andre ord bygget på en allerede eksisterende digital infrastruktur.

På den ene siden av skalaen er det infrastrukturen som er helt nødvendig for at en tjeneste som Nettskjema skal kunne nå ut til dens brukere. Internett, med alle dets protokoller og nasjonale og overnasjonale infrastruktur, samt alle innretninger som gjør det mulig for



Figur 16: «Teknisk systembeskrivelse for Nettskjema». (Hentet 10.1.20 fra https://www.uio.no/tjenester/it/adm-app/nettskjema/mer-om/systembeskrivelse/)

brukere å «se» Nettskjema, slik som nettleseren, er det åpenbare eksemplet. På den andre siden av skalaen er de helt bestemte tekniske løsningene som USIT har valgt å ta i bruk. Den førstnevnte delen av infrastrukturen som Nettskjema bygger på, representeres minimalistisk i flytskjemaet som et ikon av en bruker og en datamaskin. Det er skalaens motpol, USITs ansatte arbeider med til daglig og som er flytskjemaets objekt. Samtidig er infrastrukturen i flytskjema en representasjon av et konkret nettverk i nettverkene som internett består av, en del av et internettverk (Høgskolen i Innlandet, u.å.).

Nettskjema støtter seg eller bygger på en rekke ulike forskjellige former for digital infrastruktur. I flytskjema og på nettsiden nevnes:

- Programvare:
    - Apatche (web-server), JBoss (applikasjonserver)
    - Oracle DB (Databaseprogramvare)
- Operativsystem: Linux, RHEL 6 (Red Hat Enterprise Linux)
- Protokoll: Https (Hypertext Transfer Protocol Secure)

- Kodespråk: Java, JavaScript, Freemarker
- Filformat: JSON
- Ekstern informasjonsutveksling: Feide og ID-porten (via SAML ((Security Assertion Markup Language)))
- API (Application Program Interface): REST-API (Representational State Transfer)
- Lokal Hardware: datamaskiner og servere

I tillegg kommer en mengde «kodebiblioteker»: «ferdige» samlinger av funksjoner som kan benyttes av annen programvare, eksempelvis de som brukes av Nettskjema. Slike biblioteker er vanligvis satt sammen av andre utviklere, og kan være både åpen kildekode (uten betaling eller andre restriksjoner for bruk) eller er kjøpsvare. Det er vanlig at en digital plattform, slik som nettskjema, i høy grad støtter seg på slike kodebiblioteker.

De digitale løsningene er hele tiden i bevegelse og må kontinuerlig oppdateres, vedlikeholdes, testes og skannes for feil. I intervju med utviklingslederen, forteller han at det ikke er uvanlig at de legger ut ti versjoner av programvare som er en del av Nettskjema på en dag.

> Vi har jo greid å lage en løsning der vi legger ut nye versjoner hele tiden, det er jo litt moderne utvikling, men det handler også om sikkerhet. Nå skanner vi også biblioteker. Hvis vi av en eller annen grunn ikke har lagt ut en ny versjon på en del dager, også har det kommet et hull så må vi oppdage det også – selv om vi ikke har lagt ut en ny versjon. [...] Det var en ny type skanning som vi skjønte at vi ikke hadde tatt høyde for.

Infrastrukturen som Nettskjema bygger på er altså hele tiden i endring, og det kreves et kontinuerlig arbeid for å sikre at Nettskjema er trygt. Mye av infrastrukturen er ekstern og ute av USITs direkte kontroll, og hastigheten på endringene er økende. Alle de ulike komponentene i listen over må jevnlig testes og oppdateres. Jeg ser dette som en form for synkroniseringsarbeid med den eksterne infrastrukturen. Dette viser den tette sammenvevingen i digital infrastruktur, og det viser det massive arbeidet som kontinuerlig gjøres for at infrastrukturen er synkronisert. I økende grad er disse prosessene automatiske og gjøres av ulike algoritmer. Synkroniseringsarbeidet blir slik sett i stor grad delegert til algoritmer.

Som vi skal se skaper de tette forbindelsene mellom både interne og eksterne aktører noen utfordringer i møte med et strengere personvernsparadigme.

5.1.2 Å bli «GDPR-ready»

I en presentasjon med tittelen «Vi er GDPR-ready» på en konferanse for utviklere, forteller utviklingslederen om hvordan USIT har arbeidet for å gjøre Nettskjema til en sikker løsning med innebygget personvern. Han starter foredraget med å fortelle om en personvernskandale som rammet USIT og Universitetet i Oslo i 2006, da et stort antall personnumre ble lekket på nett. Deretter, i 2018, ble Nettskjema og USIT presentert som finalist i Datatilsynets konkurranse for innebygget personvern og Norsk senter for informasjonssikrings pris for god informasjonssikkerhet og tillit (fidus-prisen). Foredraget dreier seg altså om hvordan USIT har gjennomgått denne endringen, med fokus på Personvernforordningen og Nettskjema.

Utviklingslederen forteller videre at de aldri kunne kommet til å lekke personnumrene i dag. «En risikovurdering ville umiddelbart indikert at [det å legge ut denne filen] er strengt forbudt] [...] Hvis jeg likevel [hadde lagt ut en slik fil] ville det umiddelbart gått alarmer for oss». Prosedyrer for risikohåndtering er altså bygget inn, og en del av arbeidet med å håndtere denne risikoen er delegert til algoritmer som vil varsle dersom sensitiv informasjon havner på galt sted. Utviklingslederen gir uttrykk for at det har skjedd store endringer, de har gått fra å være verst i klassen til noen av de beste. Så hva innebærer denne endringen? «Hva er det som gjør at vi kan lage [løsninger] for innsamling av sensitiv informasjon [i dag]? Jo, vi har innebygget personvern.» Nettskjema er med andre ord «GDPR-ready».

Jeg forstår «GDPR-ready» som et slags synonym for «å ha innebygget personvern». Begrepet peker mot å det å bygge inn i en struktur eller det er å gjøre organisasjonen og teknologien kompatibel med en standard. Jeg får assosiasjoner til begrepet «HD-ready», som en kunne finne på klistremerker festet på TV- og dataskjermer for noen år tilbake. I begge tilfeller pekes det mot en ny standard som er i ferd med å bli innført, og som en form for sertifisering eller bekreftelse på at løsningen er kompatibel med denne nye standarden. I tilfelle med begrepet «HD-ready» ble det brukt som et slags salgspunkt ovenfor brukeren om at produktet er i overenstemmelse med fremtidens infrastruktur. Å proklamere seg som «GDPR-ready» er dermed en måte å kommunisere til brukeren, med ett enkelt begrep, at produktet kan tas i bruk, uten at brukeren – i dette tilfellet, skjemaeieren - skal trenge å bekymre seg for å komme i konflikt med personvern-standarden og den juridiske infrastrukturen.

5.1.3 Fra juss til IT

Senere i foredraget forteller utviklingslederen om da USIT ble nominert til Datatilsynets pris for innebygget personvern og han skulle forsvare valgene de hadde tatt med Nettskjema i henhold til Personvernforordningen foran juryen. Han sier spøkfullt: «Nå har jeg snakket så mye om GDPR at nå burde jeg lese den». Med latter fra salen begynner han å lese opp fra artikkel 25 for å illustrere hvor vanskelig språk forordningen er skrevet i, og hvor vanskelig det er å forstå hva artikkel 25 egentlig betyr:

> Jeg har ikke sjans til å lese det som står der! [...] Så da gikk jeg til juristen vår og spurte om hva jeg skulle gjøre. Så sier han «Dette er jo en lureoppgave. Det er artikkel 5 som legger grunnlaget for artikkel 25. Hvis du skal vinne denne konkurransen må du bare si at det egentlig er snakk om artikkel 5'».

Utviklingslederen fortsetter med å beskrive artikkel 5 "Det som er fint her er stikkordoppsummeringen for hvert punkt". Han fortsetter foredraget med stikkordene som utgangspunkt for å beskrive hva USIT har gjort for å bli «GDPR-ready».

Her dukker dokumentene som jeg har analysert tidligere i oppgaven opp igjen. Artikkel 25 om innebygget personvern blir brukt som en illustrasjon på hvor utilgjengelig loven er for utviklere. Artikkel 5, «Prinsipper for behandling av personopplysninger», blir trukket frem som en helt sentral del av lovgivningen. Stikkordene er unntaket fra regelen om en utilgjengelig lovtekst, og fungerer som en nøkkel for å forstå hva forordningen egentlig betyr for utviklere. Her kommer også møtet mellom IT-praksis og juridisk praksis tydelig frem. Det er først når utviklingslederen skal presentere Nettskjema som innebygget personvern at han oppsøker lovteksten, og det trengs en jurist til for å forklare hva som egentlig er relevant i dette tilfellet.

Utviklingslederen konkluderer om innebygget personvern: «For hva er innebygd personvern? Det er jo veldig mye. Det er å gjøre ting bra, på en måte». Etter at USIT ble finalist i Datatilsynets konkurranse for innebygd personvern ble de også involvert i arbeidet med utviklingen av Datatilsynets veileder «Programvareutvikling med innebygd personvern», som vi har stiftet bekjentskap med tidligere i oppgaven. Om dette arbeidet forteller han i foredraget: «Det jeg fant ut etterhvert var at det egentlig handler om å programmere ordentlig [...] Det er egentlig moralen her, hvis du programmerer ordentlig så er dere jo innenfor!» Her ser vi at utviklingslederen fremhever det som er sentralt for sitt eget fag, programmering. På denne måten blir personvern gjort til noe internt i IT-feltet, ikke som et eksternt krav, men som ett etos for utviklere. Personvernet er her med skape nye grensedragninger for hva som er «innafor».

I intervju utyper utviklingslederen hvordan personvern og sikkerhet[9] har påvirket IT-feltet:

> Det styrker seriøs programmering. Jeg tenker det er det som er den svære greia som ligger under. Hva er det som definerer seriøs programmering? Tidligere så var det mye mer ting du fikk en feeling av hva var seriøst.

Tidligere var det altså mye mer uklart hva som utgjorde «seriøs programmering». Resultatet av «bølgene» av sikkerhet, personvern og universell utforming legger grunnlaget for en mer eksplisitt og operasjonalisert forståelse av hva «god programmering» innebærer. Personvern blir her sett som en forsterkning av de (gode) programmeringspraksisene som allerede finnes, men det fastsetter og tydeliggjør det som allerede har vært ansett som god praksis. Personvern forstått i denne sammenhengen kan dermed beskrives som en verdsettingsspraksis for hva som er «ordentlig» programmering og «god» kode.

Samtidig er dette ett av mange krav som stilles til utviklere. Utviklingslederen forklarer at det har blitt vanlig å skrive i jobbutlysninger at man ser etter «full stack-utviklere», altså en som har «alt»: «Du kan alt - du skal kunne databaser, javascript, mobilapper». Utviklere på et team har forskjellig kompetanse, og som beskrevet over blir også teamet komplementert av jurister og IT-sikkerhet, men utviklingslederen understreket samtidig at dette ikke er nok. Personvern og sikkerhet blir en del av dette «alt» som en utvikler må kunne. Og som sitatene over viste oss; personvernet internaliseres gjennom en forståelse av hva som er «innafor» og gjennom et sett av *gode* praksiser.

5.1.4 Innbygget personvern med dataminimering

I presentasjonen legger utviklingslederen spesielt fokus på hvordan de har imøtekommet kravet om dataminimering for å bli «GDPR-ready». Dataminimering er et krav i Personvernforordningens artikkel om innebygget personvern (Personvernforordningen art. 25). I artikkel 5 defineres det slik: «Personopplysning skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»)» (Personvernforordningen art. 5,c). Hva betyr da dataminimering for akkurat Nettskjema?

[9] Her nevner også utviklingslederen universell utforming. Digitaliseringsdirektoratet skriver om universell utforming «Universell utforming handlar om å utforme omgjevnadane slik at vi tek omsyn til variasjonen i funksjonsevne hos innbyggarane, inkludert personar med nedsett funksjonsevne» (Digitaliseringsdirektoratet, u.å.). Jeg har ikke inkludert dette ettersom det er utenfor oppgavens felt.

Fra intervju, presentasjon og USITs nettsider om Nettskjema har jeg identifisert flere ulike måter dataminimering gjøres i tilknytning til Nettskjema:

a) Alle skjemaer som brukes blir automatisk scannet av algoritmer som forsøker å avgjøre om skjemaet inneholder personopplysninger. Det sendes deretter ut varsel til «eieren» av skjemaet dersom det ikke blir slettet etter 6 måneder. Skjemaet slettes automatisk hvis ikke eieren foretar seg noe.
b) Det oppfordres til å ikke bruke «fritekst-felt». Årsaken er at en ikke kan kontrollere hva som skrives inn i et tekstfelt. Dermed risikerer man at uønsket informasjon lagres.
c) De lagrer ikke informasjon om hvem som fyller inn skjemaene, selv om du er logget inn i deres tjeneste (uio og feide), med mindre det krysses av eksplisitt at eieren av skjemaet må ha den informasjonen. Det gjorde de ikke før personvern kom på agendaen. *«Sånt gjorde vi ikke før i det hele tatt, at vi fjernet all dataen. Det jo mye større fare for feil, det er jo en konsekvens av dette. Det er jo veldig nytt.»*
d) I motsetning til tidligere så laster det ikke ned informasjon om personen det gjelder fra andre databaser.
e) Alle vedlegg i Nettskjema slettes automatisk.

Punktene viser at Nettskjema ikke bare er en muliggjørende informasjonsteknologi for innhenting av opplysningene. Nettskjema interagerer med innhentingen av informasjon, både når skjemaeier lager skjemaet, når respondenten svarer, og etter at opplysningene er hentet inn. Utfordringen i et slikt informasjonssystem er ikke bare å sørge for at informasjon «lekker ut», det er også helt sentralt at ikke «gal» informasjon kommer inn i systemet i det hele tatt, eller at feil informasjon havner på feil sted. På den måten tar også Nettskjema, som alle informasjonssystemer eller arkiver, del i et sorteringsarbeid. Tiltakene for dataminimering er én slik praksis der Nettskjema legger føringer for hvilken informasjon som kommer inn i systemet og hvordan denne behandles.

Figur 17: Skjermdump fra Nettskjema. (Hentet 10.1.2020)

Dette arbeidet skjer på ulike steder og på ulike tidspunkt og av et stort antall ulike aktører. Det oppfordres til å ikke bruke tekstfelt (b)

før eieren lager skjemaet. Når brukeren fyller inn skjemaet blir ikke (ytterligere) informasjon om brukeren lagret (med mindre det er krysset av eksplisitt skjemaets eier)(c). Når informasjonen om brukeren sendes inn til databasen sjekkes den ikke lenger opp mot andre databaser (d). Også etter at informasjonen fra skjemaet fylles inn i databasen, utføres arbeid for å forsikre at informasjon ikke blir værende for lenge i databasen. Skjemaene skannes for personopplysninger og varsler sendes ut til eieren dersom skjemaet ikke slettes (a).

Bare et av disse tiltakene handler om informasjonsformidling rettet mot brukere: Oppfordringen til å unngå å bruke tekstfelt er iverksatt gjennom tekst som er lagt ut på informasjonssidene om Nettskjema. De resterende tiltakene involverer automatiserte prosesser, dvs. algoritmer, på ulike måter. To av tiltakene (c og d) er «negative» tiltak som innebærer fravær av algoritmer som ble brukt tidligere. Nettskjema lagrer ikke lenger automatisk informasjon om hvem som fyller inn skjemaene, med mindre skjemaeieren eksplisitt endrer innstillingene for skjemaet (c). Dette er et eksempel på «personvern som standard»: Standardinstillingen er å ikke samle inn (mer) personinformasjon. For skjemaeieren betyr personvern som standardinnstilling i praksis at «Nei» allerede er krysset av i stedet for «Ja», på spørsmål om personinformasjon skal lagres. Dette viser hvordan personvern ofte er et resultat av et stort antall små valg som er dytter brukeren i retning av å gi fra seg mindre personinformasjon. I dette tilfellet et kryss som er satt noen piksler lenger opp eller ned.

5.1.5 Å bygge inn i algoritme

To andre tiltak innebærer at nye algoritmer blir satt i kraft (a og e). Et av tiltakene er automatisk skanning av skjema med personopplysninger.

Figur 14 viser hvordan Nettskjemas algoritmer «rydder» skjemaer som inneholder bestemte ord. Når en skjemaeier lager et skjema blir hun spurt om skjemaet har spørsmål som kan være personidentifiserende, men skjemaene skannes etter personinformasjon i tilfelle skjema skulle inneholde personidentifiserende informasjon til tross for at skjemaeieren har huket av for at skjemaet ikke har slikt innhold. Noe av sorteringsarbeidet blir derfor delegert til algoritmer som skanner informasjonen i databasen etter personinformasjon. Personidentifiserende informasjon blir operasjonalisert ved hjelp av et sett av søkeord, og på den måten kan algoritmen få jobben med å identifisere skjema som potensielt inneholder personinformasjon. «Rydding» av skjema innebærer ikke sletting av skjema og all informasjonen i det, men sletting av den bestemte informasjonen som mistenkes å kunne være

personidentifiserende. Denne informasjonen er ikke «uønsket» i utgangspunktet, men *blir* uønsket når den har blitt værende for lenge i databasen. USIT informerer på sine nettsider om hvordan skjemaene vil blir «ryddet».

Automatisk rydding av personopplysninger i Nettskjema

Med jevne mellomrom kjøres det rydding av personopplysninger i Nettskjema. Det blir varslet til skjemaeiere på e-post i forkant om hvilke skjema dette gjelder.

Hvilke skjema plukkes ut

Gamle skjemaer med personopplysninger blir plukket ut etter følgende kriterier:

Skjema som ikke har mottatt svar på 6 måneder og som inneholder personopplysninger.

Vi antar at et skjema har personopplysninger dersom minst ett av følgende kriterier er oppfylt:

- Den som svarer må logge inn med brukernavn og passord.
  - Dette gjelder kun dersom du har svart "Ja" på "Vil du vite hvem som har svart på skjemaet?"
- Skjemaet inneholder minst ett av feltene: "PersonID", "Fullt navn", "Brukernavn", "E-postadresse" eller "Vedlegg".
- Skjemaet har spørsmål der vi antar at det bes om personopplysninger.
  - Dette gjelder spørsmål som inneholder minst ett av følgende ord:

```
"personnu", "personnr", "fødselsn", "fnr",  "norwegian national id", "social secur
"personal nu", "personal id", "studentn", "student nu", "studienu", "student id",
"passnr", "passnu", "passport n", "fødseld", "fødselsd", "birth da", "birthda", "f
"etternavn", "fullt navn", "fornamn", "etternamn", "fullt namn", "first name", "gi
"forename", "surname", "last name", "family name", "full name", "legal name", "bru
"user name", "username", "privatadr", "privat adr", "private add", "home add"
```

Følgende blir ryddet bort

Når Nettskjema kjører automatisk rydding av personopplysninger, blir følgende gjort:

- Kobling mellom besvarelse og den som har svart blir fjernet
- Listen over inviterte blir tømt
- Innholdet i Spesialfelter blir fjernet
- Innholdet i svar på spørsmål der vi antar at det bes om personopplysninger blir fjernet

Figur 18: Skjermdump, "Rydding av personopplysninger i Nettskjema" (Hentet 10.1.2020 fra https://www.uio.no/tjenester/it/adm-app/nettskjema/hjelp/se-resultater-analyse/rydde-slette.html)

Disse eksemplene er illustrerende hvordan personvern bygges inn i et digitalt informasjonssystem og hva personvern «betyr» når personvernet skal settes ut i digital

praksis, her først og fremst i form av dataminimering. Mye av arbeidet består av utallige ørsmå justeringer, slik som skjermdumpen ovenfor illustrerer. Implementering og endringen av nye algoritmer gjør en stor del av dette arbeidet.

Algoritmens handlinger må kodes, skritt for skritt, i en rigid oppskrift uten rom for tvetydighet og tolkning,[10] og krever streng operasjonalisering. Det er fordi algoritmen bare kan bare ta knøttsmå skritt av gangen, men til gjengjeld tar den alltid samme avgjørelser og den kan gjøre disse små handlingene veldig raskt. Når oppgaven først er satt, kan algoritmen gjøre oppgaven sin med stor effektivitet og uten feil, i tråd med oppgavene den har fått. Disse egenskapene gjør algoritmer skaleringsvennlige; en oppgave kan repeteres nærmest i det uendelige med minimal motstand. Slik settes også algoritmene i arbeid med Nettskjema.

Det som gjør algoritmen skaleringsvennlig er også det som gjør at den kun kan gjøre oppgaver som er satt med rigide rammer, strengt operasjonalisert skritt for skritt. Når algoritmen innrulleres i programmet må det gjøres på denne måte, med en oppgave som er strengt definert og operasjonalisert skritt for skritt. Listen med søkeord i figur 18 er et godt eksempel på den type oppgave som lar seg vellykket delegere og skalere med algoritme. At søkeordene bare er delvis fullstendige ord illustrerer at algoritmen ikke trenger å forstå oppgaven den blir gitt. Hva som gjør at søkeordene indikerer at skjemaet potensielt inneholder personopplysninger er irrelevant. Så lenge oppgaven er gitt på den rigide og møysommelige måten som algoritmen krever, vil den gjøre nettopp den oppgaven som den er tillagt med stor effektivitet. Det er slik sett ett én-til-én forhold mellom oppgavebeskrivelsen og oppgaveutførelsen. Teamet med utviklere har her valgt ut deler av ord som de ser som indikasjon på at skjemaet spør etter personopplysninger. Algoritmen er kontrollerbar og formbar i den forstand at den lett kan modifiseres etter utviklerens ønske, og gjøre akkurat det utvikleren ber om, det gjør den til en kraftfull alliert.

Samtidig er det også en sårbarhet i oversettelsen mellom utvikler og algoritmens handlinger. Fordi algoritmen er så rigid som den er, uten tolkningsrom, kreves også samme rigiditet både fra utvikleren og i informasjonen som algoritmen behandler. Dersom ord mangler fra listen eller det er skrivefeil, vil ikke algoritmen kunne plukke opp skjemaet med potensiell personinformasjon. Hvis et ord i listen er for bredt definert vil algoritmen kunne

[10] Algoritmen som beskrives her er en «klassiske form» for algoritme. Det finnes også algoritmer som er i stand til å gjøre mer nyanserte tolkninger, slik som noen former for maskinlæring, for eksempel. Også disse algoritmene er bygget på enkle diskrete skritt, men blir skalert til å kunne ta mer nyanserte avgjørelser, å skille bilder av hunder fra katter, for å ta et enkelt og klassisk eksempel. Algoritmene som beskrives her er av en enklere form.

komme til å rydde et skjema uten personinformasjon. I algoritmens føyelighet og «ufeilbarlighet» kommer altså andre sårbarheter til uttrykk. Når personvern gjøres algoritmisk, og blir til algoritmisk personvern, blir også programmet modifisert; algoritmene gjør personvern på sin egen måte og legger føringer for hvordan personvern gjøres, og informasjon bearbeides.

Søkeordene er klassiske beskrivelser av personopplysninger: personnummer, adresse, fullt navn, osv. Men Personvernforordningen gir en langt mer fleksibel beskrivelse av personinformasjon, slik vi så i første analysekapittel. Dette er vanskelig å fange opp med den formen for rigiditet som er bygget inn i algoritmer. Slike typer komplekse relasjoner som Personvernforordningen beskriver som personopplysninger lar seg ikke lett defineres og operasjonaliseres i tråd med algoritmens behov, og er personinformasjon i kraft av et sett komplekse relasjoner. Slike komplekse relasjoner krever tolkning og forståelse på en måte som er fremmed for algoritmens rigide logikk.

Tiltakene for dataminimering illustrerer en form for sorteringsarbeid for å sørge for at informasjon ikke havner på galt sted. I denne sammenheng er det informasjon i form av personopplysninger. Med et nytt personvernsparadigme gjøres det nye grensedragninger også for hvilken informasjon som kan være hvor, og hvilken informasjon som er verdifull, og på hvilken måte den er verdifull. Ved USIT kommer noen konsekvenser av nye grensedragninger til syne gjennom tiltakene for dataminimering.

Tiltakene har som formål å sikre at uvedkommende informasjon ikke kommer inn i databasene, og dette arbeidet gjøres av mange ulike aktører på ulike steder og på ulike tidspunkt. Dette sorteringsarbeidet kan også beskrives som en del av en verdisettingspraksis. Mange former for sortering handler om å luke vekk det som ikke er verdifullt; å skille klinten fra hveten. Når det kommer til personopplysninger og personvern er det motsatt. Personopplysninger, og da spesielt sensitive personopplysninger, er i en viss forstand for verdifulle til å lagres. Også her er det klinten som skal skilles fra hveten, men det er hveten som må lukes ut, altså det som er «for verdifullt».

5.1.6 Å bygge inn i organisasjon og praksis

På spørsmål om hva som er det viktigste verktøyet for å utvikle i tråd med personvernet, svarer utviklingslederen at det er «folkene» som er viktigst.

En holdningsendring har funnet sted, både i USIT og i IKT-bransjen generelt, påpeker flere av mine informanter. For å illustrere dette i intervjuet forteller utviklingslederen

lattermildt en anekdote fra en kollega i en annen IKT-bedrift, om når de for første gang fikk beskjed om at de måtte tenke på innebygget personvern: «[V]i pleier alltid å begynne prosjektene med ett minutt stillhet der vi tenker på det [personvern], også fortsetter vi.» I kontrast til dagens situasjon ved USIT og Nettskjema, har i dag personvern-problematikken fått en mer fremtredende, praktisk rolle i utviklernes arbeid:

> Jeg tror kanskje den største overgangen er den bevisstgjøringen, i alle fall innenfor utvikling hos oss, at alle er bevisste på det, og at en tenker seg om veldig nøye før en logger ting eller lagrer ting. Det har jo nesten skjedd de siste årene. Vi lagrer veldig mye mindre data - hvis du logger inn i vår tjeneste så lagrer vi ikke en gang brukernavnet ditt en gang.

Med andre ord, i dag tenker en ikke bare over det og fortsetter som før, men en har endret praksis til å samle inn og logge mye mindre data enn tidligere, før Personvernforordningen. Slik innebygget personvern i form av dataminimering trekkes frem som en av de viktigste endringene, men minst like viktig er den doble endringen, i både «bevissthet» og praksis i hele organisasjonen, blant samtlige teknikere, og ikke bare en og annen «entusiast».

Spesielt tre endringer i praksis trekkes frem knyttet til organisasjonspraksis av utviklingslederen. For det første understreker han at personvernhensyn tas opp fortløpende når en applikasjon som Nettskjema utvikles eller videreutvikles. Det er ikke tilstrekkelig at personvernhensyn tas opp i begynnelsen eller i slutten av prosessen. For det andre har USIT, sammen med Universitet i Oslo, de siste årene ansatt flere IT-jurister. Juristene konsulteres underveis i utviklingsløpet eller når utviklerteamet er usikre på noe knyttet til personvern. Den tredje praksisen som han trekker frem er at all kode må godkjennes av to utviklere før den legges ut til testing.

Utviklingslederen beskriver personvernet som «en bølge som har skylt over IKT-feltet» og påvirket måten man jobber med utvikling:

> Vi hadde jo en bølge med sikkerhet, for en 5-6 år siden så fikk IT-sikkerhet veldig høyt fokus, og vi måtte hele tiden i møte om IT-sikkerhet, og vi begynte å få sikkerhetsfolk her og sånt. Nå er de litt sånne rådgivere på siden og jobber med avvik egentlig. [...] Hos oss var det jo sånn at vi fikk ansatt den første juristen for kanskje 7 år siden. I dag er det 4. Så det har vært en ekstrem økning i antallet jurister. Men nå har vi sluttet litt å snakke med dem igjen. For nå tar vi bare opp ting når det er spesifikt, fordi vi forventer at folk selv [utviklerne] vet hva som er innenfor og hva som ikke er innenfor [...] Du kan ikke ha med jurister og sikkerhets-folk fra begynnelsen. Det blir en utopi.

Her ser vi at utviklingslederen peker på at kunnskapen om hva som er innenfor og ikke må overføres fra juristene til utviklerne («folk») etter en viss tid. Dette er dermed også en beskrivelse av hvordan krav til sikkerhet og personvern blir «bygget inn» i USIT i praksis. Når det av ulike grunner blir satt fokus på et tema, slik som personvern eller sikkerhet,

oppstår det et stort behov etter ekspertise, delvis på grunn av mangel av mangel på kunnskap, men også fordi endringen ikke enda har størknet eller satt seg og situasjonen er udefinert. Men når situasjonen etterhvert er mer avklart, og utviklerne – i dette tilfellet – har lært av den relevante ekspertisen, er ikke lenger behovet like sterkt, og kunnskapen anses altså for å være bygget inn i organisasjonens praksis.

5.1.7 Å bygge inn i nettverket

Arbeidet med en slik IKT-infrastruktur, med Nettskjema som eksempel, synes å være gjennomsyret av risiko og sårbarhet, og kravene fra personvernlovgivningen øker dette ytterligere. Utviklingslederen peker på ulike kilder til risiko:

> [J]eg vil jo si at løsningen vår tar jo høyde for at alle som er brukere av tjenesten vår er kjeltringer. Det ligger til grunn hos oss. At forskerne er kjeltringer og de prøver å bruke vår løsning for å jukse i forskningen. [...] Det skal vi greie å stoppe de i, eller egentlig så prøver vi å stoppe de i at de er dumme og lekker persondata.
>
> Vi stoler ikke noe mer på noe annet utstyr, fordi vi antar at alt er kompromittert hele tiden. Så vi har et helt annet regime hos oss.
>
> [D]et er utviklerne som er det svakeste leddet. Det har vi gjort veldig mye tiltak rundt. [...] Ingen får lov til å legge noe til test hos oss uten at det har vært fire øyne på det.

Jeg tolker dette slik at systemet og infrastrukturen er «truet» fra alle kanter. Alt og alle er en potensiell trussel. Den digitale løsningen, brukerne av løsningen og utviklerne bak løsningen kan på ulike måter true systemets intenderte operasjon og føre til at informasjon havner på avveie. Poenget med Nettskjema, infrastrukturens objekt, er informasjonen som innsamles. Det er først og fremst informasjonen som er det verdifulle objektet som må beskyttes og behandles med omtenksomhet. En viktig oppgave er å unngå at persondata «lekker». Infrastrukturen er som et rør som hele tiden må tettes, der informasjon er det verdifulle objektet som ikke må lekke ut. Utviklingen av slike informasjonssystemer fremstår som vel så mye som et lappearbeid som et konstruksjonsarbeid. Dette lappearbeidet kan minne om en form for omsorg for infrastrukturen og for informasjonen som samles inn og lagres.

Som vi også har sett er et informasjonssystem på internett, slik som Nettskjema, tett forbundet med et stort antall «eksterne» aktører. Ettersom USIT er behandlingsansvarlig for personopplysningene, betyr det også at de indirekte betyr dette at de også er «ansvarlige» eller «accountable» for alle de tekniske løsningene som brukes i tilknytning til Nettskjema. Dette medfører at alle tekniske løsninger som tas i bruk utenfra må behandles som en risiko fordi de

kan føre til lekkasjer, enten på grunn av feil eller uforutsette konsekvenser, eller fordi andre aktører ønsker å få tak i personopplysninger.

Personvernlovgivningen er med på å bidra til at risikonivået for personopplysninger, og tillit mellom aktører i denne sammenhenger kommer til en høyere pris. Behandlingsansvarlig (her USIT) holdes etter lovgivningen ansvarlig for personopplysninger som samles inn og det som gjøres med opplysningene. Informasjonsutveksling med eksterne aktører kommer derfor med en risiko. Som vist tidligere i kapitlet, befinner en nett-tjeneste som Nettskjema seg i en tett sammenvevd infrastruktur, bestående av både interne og eksterne aktører. Høyere terskel for tillit mellom aktører er derfor en stor utfordring. Utviklingslederen bekrefter at kravene til personvern skaper en høyere terskel for tillit, men påpeker også at tillit distribueres ulikt:

> Vi har veldig høy tillit i Norge og i sektoren, også har vi veldig lav tillit til alle andre. Vi har tillit til ID-porten, det er det eneste vi stoler på av eksterne aktører, resten synes vi er skummelt.

Ut fra sitatet kan det også virker som at det er enklere å ha tillit til aktører som er «nærmere», altså til aktører «i Norge og i sektoren». Jeg tolker dette slik at fordi kravene til personvern øker risiko, blir terskelen for tillit høyere, og dette bidrar til å forsterke de allerede eksisterende grensedragningene for hvem som har tillit.

5.2 Oppsummering og konkluderende bemerkninger

I dette kapitlet har jeg vist hvordan det nye personvernet interagerer med IT-praksis, og hvordan personvern gjøres i praksis i en konkret digital plattform for datainnsamling.

Jeg har beskrevet tidligere hvordan risiko og verdi er sentrale elementer i det nye europeiske personvernet. Her har jeg vist hvordan dette bygges inn i IT-praksis og infrastruktur. Som jeg har vist tidligere, blir behandlingen av personopplysninger knyttet til en større risiko i nye personvernet. Jeg har vist hvordan personopplysninger som verdi- og risiko-objekt i denne sammenhengen gir opphav til nye sorteringspraksiser for å sikre at opplysningene ikke «lekker» eller havner på galt sted. For en digital tjeneste som Nettskjema, som et system for innsamling, oppbevaring og behandling av opplysninger, er opplysninger allerede en verdifull ressurs, og dette forsterkes ytterligere med kravene fra Personvernforordningen.

I analysen har jeg beskrevet hvordan utviklere gjør personvernet «til sitt eget» ved at innebygget personvern blir sett som en del av det å gjøre «god programmering». I likhet med

Datatilsynets veileder blir det her gjort et verdsettingsarbeid gjennom grensedragninger av hva som er «god praksis». Dette grensearbeidet er til dels en forsterking av allerede eksisterende praksis, samtidig som nye elementer trekkes inn. Med begreper som «GDPR-ready» og «god programmering» oversettes personvernskrav fra juridisk praksis til IT-praksis, gjennom ulike former for verdsetting, og transformeres fra et uhåndterlig objekt til noe som i stor grad kan håndteres med verktøy teknologene allerede har for hånden.

Opprettholdelsen av infrastrukturen som muliggjør Nettskjema er allerede gjennomsyret av risiko, og jeg har vist hvordan nye personvernkrav øker risikonivået når personopplysninger skal behandles. En slik digital infrastruktur krever en mengde forbindelseslinjer, både internt og eksternt for organisasjonen. En infrastruktur som denne trekker hele tiden på løsninger og tjenester som utarbeides utenfor organisasjonen. Ettersom organisasjonen står ansvarlig for alt som skjer med personopplysningene, blir også slike eksterne forbindelseslinjer mer risikable, og leder til at terskelen for tillit til andre organisasjoner blir høyere.

Arbeidet med å håndtere verdiene og risikoen knyttet til personopplysninger blir delegert til både utviklere, algoritmer og brukere. I dette kapitlet har vi sett hvordan mye arbeid delegeres til algoritmer når personvernet skal bygges inn i infrastrukturen. Som vi har sett tidligere er tolkningsarbeid helt sentralt i juridisk praksis. Det er ikke slik at lovteksten er «ferdig tolket». Den må settes sammen med og ses i lys av annen lovgivning og lovpraksis. Når krav fra personvernet skal gjøres med algoritmer, må det også oversettes til en annen «logikk». Med slike algoritmer som blir beskrevet i dette kapitlet, må denne formen for tolkningsarbeid gjøres *før* arbeidet kan overlates til algoritmene. Oversettelsesarbeidet må altså på dette punktet gjøres på algoritmenes premisser.

6 Konklusjon

Som jeg nevnte innledningsvis kan EUs Personvernforordning ses i kontekst av et bredere digitaliseringsprosjekt. Overordnet kan denne oppgaven ses som en undersøkelse av hvordan digitalisering gjøres i møtet mellom juridisk og teknologisk infrastruktur i et moderne overnasjonalt demokratisk system. Det nye personvernet kan ses som et steg i EUs digitaliseringsprosjekt. Digitaliseringen må skje i tråd med EUs grunnverdier, og slik sett er også det nye personvernet en måte å stryke og utvide EUs målsettinger i den bredere digitaliseringen av samfunnet med personopplysninger som det primære forvaltningsobjektet. Sentralt i denne visjonen står det som jeg har kalt for god digitalisering: et digitalt marked og en datapolitikk som både verdsetter personopplysninger i tråd med europeiske borgeres grunnleggende rettigheter og samtidig verdsetter personopplysningers kunnskaps- og markedsverdi.

Samtidig kommer denne visjonen som en reaksjon på et nytt teknologisk landskap. Ny teknologi og måten vi bruker teknologien på, har gjort personopplysninger mer verdifull fordi teknologien muliggjør nye forbindelser og ny kunnskap om «fysiske personer». Dette gjør både at personopplysningene har større kunnskaps og markedsverdi, fordi mer verdifull kunnskap kan hentes ut fra opplysningene. Samtidig er det både mer informasjon tilgjengelig for å identifisere en person, og det er lette å identifisere ved hjelp av mindre informasjon. Opplysningene blir på denne måten tettere knyttet til den fysiske person, og slik sett er det ikke bare personopplysningene som endres, men også subjektet, eller det enda mer treffende «data subject» i den engelske utgaven av Personvernforordningen. Dette kommer også til uttrykk i forordningen, som bruker et bredere definisjon av personopplysning og hva som er identifiserbar person. Dette er en del av digitaliseringen som lovdokumentene både beskriver og forsøker å regulere.

I denne oppgaven har jeg sett nærmere på hvordan denne visjonen gjøres til lov og gjøres til del av IT-praksis. I innledningen startet jeg med et generelt spørsmål om hvordan teknologipolitikk utøves gjennom lov. Forskningsspørsmålet jeg stilte var «Hvordan bygges en visjon om et nytt personvern inn i lov og IT-praksis». Jeg har undersøkt dette spørsmålet ved å følge en konkret oversettelseskjede. Denne har jeg fulgt ved å studere et knippe empiriske steder: I EUR-Lex så jeg på Europakommisjonens visjonsdokument og Personvernforordningen; hos datatilsynet undersøkte jeg veilederen for innebygget personvern hos datatilsynet og hos USIT analyserte jeg hvordan det nye personvernet ble

gjort til del av organisasjonen og den digitale plattformen «Nettskjema». På denne måten har jeg kunne stille dette forskningsspørsmålet på disse ulike stedene, som kommer til uttrykk i hvert sitt analysekapittel, og på den måten har jeg kunnet undersøke hvordan personvernet blir til i praksis på ulike steder i kraft av og i møte med infrastruktur og slik kunne følge en «implementeringskjede».

I Europakommisjonens visjonsdokument presenteres virkelighetsbeskrivelse der et sett av utfordringer knyttet til nye digitale teknologier blir lagt frem, og Europakommisjonen foreslår et nytt juridisk rammeverk for å møte disse utfordringene. Det tegnes opp en skisse over de ulike aktørene på feltet og relasjonene mellom dem. Disse plasseres inn i fortid, nåtid og fremtid på en slik måte at «EUs verdier» og lovverket blir til et obligatorisk passasjepunkt for å løse problemene som beskrives. Dette arbeidet fortsetter på et mer detaljert plan i Personvernforordningen, der aktørene og spillereglene operasjonaliseres med juridisk språk, juridiske virkemidler, og gjøres til denne måten til juridiske objekter som loven skal virke ovenfor.

Personvernforordningen og visjonsdokumentet befinner seg i EUs arkiv for lovdokumenter, EUR-Lex. Arkivet og dokumentene er en del av en bredere juridisk infrastruktur. Dokumentene trekker hele tiden på en lang rekke andre dokumenter, hvorav mange av de befinner seg i arkivet. Arkivet bidrar til å gjøre dokumentene tilgjengelig og trekke forbindelser mellom dem. Et dokument som Personvernforordningen står ikke alene, men samhandler med de utallige dokumentene i arkivet når visjonen om et nytt personvern utøves.

Personopplysninger er det sentrale objektet for forordningen, og skal forvaltes i tråd med to av EUs formål: å sikre grunnleggende rettigheter for borgere og å styrke det indre markedet gjennom fri flyt. Disse to målsettingene kan virke motstridende, men i visjonsdokumentet smeltes de sammen. Visjonen som tegnes opp kan slik sett ses som en sammensmeltning av disse målsettingene, med personopplysninger som sitt objekt. En viktig del av denne visjonen er også et harmonisert europeisk lovverk på tvers av land. Et slikt harmonisert lovverk skape trygghet og tillit og på denne måten sikre et «godt digitalt marked».

Teknologipolitikk utøves gjennom lov ved gjennom en problematisering og ved å delegere og distribuere ansvar og risiko, og på den måten loven til et verktøy for å utøve visjonen. En av de konkrete måtene delegering gjøres i Personvernforordningen, er gjennom to verktøy jeg har sett nærmere på: prinsippet om ansvarlighet («accountability») og innebygd personvern. Dette er verktøy som beveger ansvar og risiko fra det juridiske feltet og inn i IT-

praksis, det vil si inn i organisasjoner og digital teknologi. Dette er dermed også verktøy som forsøker å innrullere disse aktørene inn i EUs «digitaliseringsprogram», altså digitalisering i tråd med EUs målsettinger.

Prinsippet om ansvarlighet gjør dette ved å bygge «accountability» inn i organisasjoner. I artikkel 29-gruppens dokument om «accountability» argumenteres det for at dette er en måte å gjøre lov til praksis. Samtidig kan prinsippet tolkes i lys av det Power kaller for «audit society», i en bevegelse der kontroll og ansvar i økende grad blir overført fra stat til den enkelte organisasjon. Gjennom gjennomsiktighet og forflytning av ansvar kan også prinsippet ses som en måte å styrke det indre marked gjennom nye grensedragninger mellom stat og organisasjon. Dette kan dermed både ses som en del av visjonen, i tråd med de to målsettingene som jeg har diskutert, og en måte å flytte ansvar fra lov til organisasjon.

Artikkelen i Personvernforordningen om innebygget personvern fokuserer på å bygge inn personvernet i både teknologi og organisasjoner som utvikler slike løsninger. I Datatilsynets veileder for innebygget personvern fremheves utviklere og algoritmer som sentrale aktører i utøvelsen av personvern. Veilederen forsøker å bli en form for brobygger mellom juridisk praksis og IT-praksis. Den forsøker å konkretisere og operasjonalisere «innebygget personven» for IT-praksis, og på den måten innrullere nye aktører i kontrollnettverket som skal håndtere risiko knyttet til personopplysninger. Dette gjøres ved å ta i bruk et språk og en rekke verktøy fra IT-feltet, og på denne måten re-kontekstualiseres og oversettes visjonen.

Forordningen er skrevet i et komprimert, abstrakt og utilgjengelig juridisk språk. Både empirien fra kommentarutgaven, Datatilsynets veileder og i USIT blir det tydelig at det gjøres en stor mengde tolkningsarbeid for å oversette juridisk tekst til IT-praksis. I Datatilsynet og USIT gjøres et grensedragningsarbeid og verdsettingspraksiser for å gjøre personvern til en del av IT-praksis. Dette kommer til uttrykk gjennom hvordan personvernet gjøres til en del av det som karakteriseres som «god programmering». Veilederen gjør dette ved å legge til grunn en utviklingsmetodikk som min informant ser på som en del av «seriøs programmering». Utviklingslederen hos USIT beskriver på sin side personvernet innenfor et rammeverk av hva som er «innafor» i god utviklings-praksis. Her bidrar personvernet til dels til å forsterke allerede eksisterende praksis, og til dels til å tegne opp nye grensedragninger for god praksis. Dette får frem et interessant aspekt ved hvordan personvernet bygges inn. Gjennom forsterkning av eksisterende praksiser og nye grensedragninger, internaliseres på denne måten personvern og gjøres til en del av utviklernes egen praksis.

For å bygge personvernet inn i den digitale plattformen, blir mye av arbeidet delegert til algoritmer. I analysen av Nettskjema har jeg vist hvordan personvernet må oversettes og operasjonaliseres til algoritmens «logikk», for at algoritmene skal la seg innrullere i programmet. Slik sett legger også algoritmene føringer for hvordan personvernet utøves når personvernet skal «bygges inn i teknologien».

I arbeidet med denne oppgaven har jeg utviklet begrepet «God digitalisering». Ved å bruke dette begrepet har jeg forsøket å få frem hvordan verdsettingspraksis både er sentralt i den teknologipolitiske visjonen som Europakommisjonen tegner opp og prosessen med å «bygge inn personvernet». Visjonsdokumentet og Personvernforordningen gjør et retorisk arbeid der personopplysninger blir artikulert som både risiko og verdi. Behandling av personopplysninger utgjør en risiko fordi det kan komme til å krenke individers rettigheter, samtidig legges det vekt på behandling av personopplysninger som en viktig ressurs for det indre marked. Slik er risiko og verdi to sider av samme sak i dette tilfellet, og her smeltes de to målsettingene jeg har diskutert sammen. Behandling av personopplysningene utgjør en risiko *fordi* personopplysninger er verdifullt. Dokumentene jeg har analysert spiller på denne måten en viktig rolle i utformingen og modifikasjonen av personopplysning som verdi og risiko-objekt. Som Hilgarner påpeker, har artikuleringen av risiko-objektene implikasjoner for hvem som har ansvar, plikt og rett til å håndtere risikoen som objektet utgjør. Dette er en viktig måte Personvernforordningen blir et verktøy for å utøve den teknologipoltiske visjonen som tegnes opp i «visjonsdokumentet».

Hilgarner beskriver ulike strategier for å håndtere risiko-objekter. Objektene kan plasseres inn i nettverket, eller de kan forøkes å flyttes ut av nettverket. Jeg har i denne oppgaven vist hvordan risiko-objektet plasseres inn i nettverket – eller de blir «bygget inn» i nettverket, som jeg har kalt det. De bygges inn i nettverket fordi de er, og skal gjøres, verdifulle – dette er slik jeg ser det kjernen av visjonen. Personopplysninger som risiko- og verdi-objekt er ikke bare en del av visjonen, men det er også *ved* å artikulere personopplysninger som risiko og verdi at visjonen skal bygges inn. Kravene fra Personvernforordningen, blir som jeg har vist oversatt til egne verdsettingspraksiser i møte med IT-praksis. I Datatilsynets veileder og i USIT kommer dette som nevnt til uttrykk ved at personvernet gjøres til en del av IT-praksis, altså uttrykt som «god programmering», «seriøs programering» og hva som er «innafor» som god utviklings-praksis. I veilederen og hos USIT blir også risiko gjort til en del av IT-praksis ved at ansvar og risiko delegeres i nettverket av mennesker og algoritmer. Personopplysninger som risiko-objekt kommer også til uttrykk i

USIT som en høyere terskel for tillit til aktører «utenfor» organisasjonen. Risiko og verdi spiller med andre ord en sentral rolle når visjonen om et nytt personvern skal bygges inn i IT-praksis. Når risiko og verdi «oversettes» fra lov til IT-praksis blir den imidlertid modifisert og tilpasset av aktørene, og det er dermed ikke *samme* verdi- og risiko-objekt i enden av oversettelseskjeden.

6.1 Metodisk-teoretisk refleksjon

I denne oppgaven har jeg kombinert flere perspektivet fra STS-feltet. Med et ANT-blikk, har jeg i denne oppgaven vist frem de mange ulike aktørene i nettverket settes sammen for å bygge inn det nye personvernet Jeg har hentet inspirasjon fra infrastruktur-perspektivet når jeg har undersøkt hvordan personvernet bygges inn i den digitale infrastrukturen. I likhet med Geirbos bruk av begrepet «infrastrukturering», har jeg hatt fokus på praksisaspektet ved infrastruktur. Dette har jeg gjort ved å bruke det sensitiverende konseptet «å bygge inn», og på den måten kunnet undersøke hvordan en visjon gjøres til en del av en infrastruktur – i dette tilfellet juridisk infrastruktur og IT-infrastruktur.

Jeg har også anvendt perspektiver fra verdsettingsstudier for å beskrive verdsettingspraksiser som er involvert i skapelsen og implementeringen av en visjon for det jeg har kalt for «god digitalisering». Dette har jeg også komplimentert med Hilgartners begrep om risiko-objekter og kontrollnettverk. Dokumentene jeg har studert spiller en sentral oppgave i dette arbeidet. For å studere disse har jeg tatt i bruk praksis-orientert dokumentanalyse. Ved å fokusere på dokumentene som sted og som praksis har jeg kunnet vise frem dokumentene som aktive deltagere i å bygge inn en visjon.

Bruken av personopplysninger er i dag, som jeg har beskrevet i stor endring. Det teknologiske landskapet er i endring, mengden av informasjon som samles inn. Dette interagerer samtidig med endringer i hvordan slike informasjonsstrømmer og digitalisering reguleres. Dette gjør personvern til en svært relevant tematikk for dagens teknologipolitikk. Denne oppgaven bidrar til kunnskap om hvordan teknologipolitikk utøves i praksis. Den bidrar også med kunnskap om hvordan en teknologipolitisk visjon får kraft gjennom nettverk eller kjeder av dokumenter og aktører i en oversettelseskjede, samtidig som den hele tiden tilpasses og modifiseres underveis og i møtet med aktører og infrastruktur.

Dokumentene i denne oppgaven er digitale, og befinner seg i en digital infrastruktur. Samtidig er de dokumenter som er med på å skape og forme fremtidig digitalisering. Ved å kombinere et infrastruktur-perspektiv, verdsettingsstudier, praksis-orientert dokumentanalyse

har jeg kunnet vise frem hvordan juridisk infrastruktur møter IT-infrastruktur, og hvordan dokumenter og praksiser i dette møtet er med på å utøve en bestemt versjon av digitalisering. Dette har satt meg i stand til å følge de mange ulike aktørene som kommer sammen for å bygge inn personvernet, ikke bare mennesker som befinner seg i ulike praksisfelt, men også dokumentene, arkiver eller databaser og algoritmer. Samtidig har dette også gjort det mulig å fokusere på møtet mellom infrastrukturene som disse aktørene inngår i, og hvordan nye praksiser blir bygget inn i disse infrastrukturene. For at en teknologipolitisk visjon skal bygges inn, må de mange ulike aktørene innrulleres i programmet. Dette krever som vi har sett en stor mengde oversettelses arbeid og grensedragningsarbeid for at de ulike aktørene skal ta del i programmet. Programmet tilpasses og modifiseres på denne måten underveis i møte aktører og infrastrukturen som visjonen skal bygges inn i. Dette mener jeg at jeg har kunnet vise frem på en unik måte ved å følge en konkret oversettelseskjede, fra visjonsdokument til implementering i organisasjon, og ved å følge både dokumenter og infrastruktur med et praksisorientert perspektiv.

6.2 Potensielle forbindelser og videre forskning

I prosessen med å følge etableringen av et nytt personvern, har det dukket opp en rekke interessante forbindelser som kunne blitt forfulgt.

Ett spor som jeg fulgte et stykke på veien i prosessen i skrivingen av oppgaven var relasjonen mellom det nasjonale og overnasjonale, hvordan dette spiller inn og kommer til uttrykk når et overnasjonalt lovverk skal etableres, samt hvordan visjonen fra EU blir oversatt til en norsk juridisk kontekst. Det er også flere gjennomgående geografiske temaer knyttet til lovgivningen. Et viktig anliggende for Personvernforordningen er å regulere flyt av informasjon på tvers av geografiske grenser. På den ene siden ligger det store utfordringer i å regulere et (relativt) desentralisert og «grenseløst» internett. Samtidig er det utallige hindringer som må overstiges for å sikre samarbeid på tvers av nasjonale grenser i Europa. Datatilsynet spiller på mange måter i denne sammenheng en rolle som en brobygger mellom nasjonale myndigheter og institusjonene på den ene siden og overnasjonale organisasjoner og andre nasjoners datatilsyn på den andre siden.

I min empiri, som ikke har fått plass i oppgaven, dukker utfordringene knyttet til dannelsen av en felles overnasjonal personverninfrastruktur blant annet opp i såkalt «grenseoverskridende saker», saker som ikke «tilhører» noen enkelt lands datatilsyn, og derfor må håndteres mellom datatilsynene, og utfordringer knyttet til et

kommunikasjonssystem mellom de ulike datatilsyn. I tillegg dukket det opp flere språk- og kultur-barrierer som gjorde det vanskelig å oversette juridiske krav fra EU til de ulike medlemslandene, og utfordringen blir desto større for en stat som ikke er en del av EU, men som likevel skal implementere lovverket, slik som Norge. Hvordan personvernlovgivningen gjøres «grenseoverskridende», samtidig som andre grenser etableres og modifiseres, ville vært en svært interessant tematikk som ville vært godt egnet for videre STS-studier.

Det er også flere steder i min empiri der jeg gjerne skulle gått dypere og bredere inn, dersom jeg hadde hatt mulighet, tid og oppgavens omfang hadde tillatt det. En spennende mulighet hadde vært å utføre intervjuer og feltarbeid i Europakommisjonen eller i Det europeiske personvernrådet. Dette kunne gitt utfyllende empiri om arbeidet og praksisene knyttet til slike dokumenter jeg har studert fra overnasjonale institusjoner. Dette viste seg imidlertid praktisk vanskelig for en oppgave med et omfang som denne. Det hadde også vært interessant å ha et bredere empirisk tilfang fra en IT-organisasjon som USIT. Jeg skulle gjerne lest noe av selve algoritmen bak Nettskjema og anvendt verktøy fra praksis-orientert dokumentanalyse, og jeg skulle også gjerne vært deltagende observatør under utvikling av en løsning eller på møter med utviklere. Disse forslagene ble ikke imøtekommet av USIT, og jeg valgte å heller fokusere på den empirien jeg hadde. Det kunne også vært interessant fra et STS-perspektiv å «følge personvernet» helt til endebruker, og undersøke hvordan en teknisk løsning med innebygget personvern faktisk blir møtt av brukeren. I denne oppgaven har jeg altså valgt å fokusere på andre aspekter, men dette er empiriske retninger som er godt egnet for videre STS-forskning.

Litteraturliste

Accountability. (u.å.). I *Online Etymology Dictionary*. Hentet 2. april 2020, fra https://www.etymonline.com/word/accountability

Amelang, K., & Bauer, S. (2019). Following the algorithm: How epidemiological risk-scores do accountability. *Social Studies of Science*, *49*(4), 476–502. https://doi.org/10.1177/0306312719862049

Artikkel 29-gruppen. (2010). *Opinion 3/2010 on the principle of accountability*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

Asdal, K. (2011). *Politikkens natur—Naturens politikk*. Universitetsforlaget.

Asdal, K. (2015a). Enacting values from the sea: On innovation devices, value-practices and the co-modifications of markets and bodies in aquaculture. I I. Dussauge, C.-F. Helgesson, & F. Lee (Red.), *Value Practices in the Life Sciences* (s. 168–185). Oxford University Press.

Asdal, K. (2015b). What is the issue? The transformative capacity of documents. *Distinktion: Scandinavian Journal of Social Theory*, *16*(1), 74–90. https://doi.org/10.1080/1600910X.2015.1022194

Asdal, K., Cointe, B., Hobæk, B., Huse, T., Morsman, S., Måløy, T., & Reinertsen, H. (2019). *The Good Economy: Re-casting the bioeconomy, its normativities and its troubles*. https://www.sv.uio.no/tik/english/research/projects/little-tools/news/2019/asdal_et_al_2019_the_good_economy_wp3_2019.pdf

Asdal, K., & Druglitrø, T. (2017). Modifying the biopolitical collective: The law as a moral technology. I K. Asdal, T. Druglitrø, & S. Hinchliffe (Red.), *Humans, animals and biopolitics: The more than human condition* (s. 66–84). Routledge.

Asdal, K., & Reinertsen, H. (2020). *Hvordan gjøre dokumentanalyse: En praksisorientert metode* (Under utgivelse 2020). Cappelen Damm.

Bennett, C. J. (2012). The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats. I *Managing Privacy through Accountability*. Palgrave Macmillan UK : Imprint: Palgrave Macmillan.

Bowker, G. C., & Star, S. L. (1999). *Sorting things out: Classification and its consequences*. MIT Press.

Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law*, *6*(2), 77–78. https://doi.org/10.1093/idpl/ipw006

Bygrave, L. (2017). Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review*, *1*, 105–120. https://doi.org/10.18261/issn.2387-3299-2017-02-03

Callon, M. (1984). Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. *The Sociological Review*, *32*(1_suppl), 196–233. https://doi.org/10.1111/j.1467-954X.1984.tb00113.x

Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles*. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Cool, A. (2019). Impossible, unknowable, accountable: Dramas and dilemmas of data law. *Social Studies of Science*, *49*(4), 503–530. https://doi.org/10.1177/0306312719846557

Corbin, J., & Strauss, A. (2008). Strategies for Qualitative Data Analysis. I *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (3. ed.). http://methods.sagepub.com.ezproxy.uio.no/book/basics-of-qualitative-research/n4.xml

Datatilsynet. (u.å.-a). *Innebygd personvern*. Hentet 15. juni 2020, fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/

Datatilsynet. (u.å.-b). *Om Datatilsynet*. Datatilsynet. Hentet 22. juni 2020, fra https://www.datatilsynet.no/om-datatilsynet/

Datatilsynet. (u.å.-c). *Programvareutvikling med innebygd personvern*. Hentet 12. juni 2020, fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/programvareutvikling-med-innebygd-personvern/

Datatilsynet. (2019). I *Store norske leksikon*. http://snl.no/Datatilsynet

Dewey, J. (1913). The Problem of Values. *The Journal of Philosophy, Psychology and Scientific Methods*, *10*(10), 268–269. https://doi.org/10.2307/2013679

Digitaliseringsdirektoratet. (u.å.). *Kva er universell utforming?* Hentet 22. juni 2020, fra https://uu.difi.no/kva-er-universell-utforming

Dijk, N. van, Tanas, A., Rommetveit, K., & Raab, C. (2018). Right engineering? The redesign of privacy and personal data protection. *International Review of Law, Computers & Technology*, *32*(2–3), 230–256. https://doi.org/10.1080/13600869.2018.1457002

Doganova, L., Giraudeau, M., Helgesson, C.-F., Kjellberg, H., Lee, F., Mallard, A., Mennicken, A., Muniesa, F., Sjögren, E., & Zuiderent-Jerak, T. (2014). Valuation Studies and the Critique of Valuation. *Valuation Studies*, *2*(2), 87–96. https://doi.org/10.3384/vs.2001-5992.142287

Edwards, P. N. (1998). Y2K: Millennial reflections on computers as infrastructure. *History and Technology: History of Computing Approaches, New Directions*, *15*(1–2), 7–29. https://doi.org/10.1080/07341519808581939

Edwards, P. N. (2010). *A vast machine: Computer models, climate data, and the politics of global warming*. MIT Press.

EUR-Lex. (u.å.-a). *About EUR-Lex*. Hentet 5. oktober 2019, fra https://eur-lex.europa.eu/content/welcome/about.html

EUR-Lex. (u.å.-b). *Access to the Official Journal*. Hentet 7. oktober 2019, fra https://eur-lex.europa.eu/oj/direct-access.html

EUR-Lex. (u.å.-c). *Official Journal*. Hentet 5. oktober 2019, fra https://eur-lex.europa.eu/content/help/oj/intro.html

Europakommisjonen. (2010). *A comprehensive approach on personal data protection in the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52012PC0011

Europakommisjonen. (2015). *A Digital Single Market Strategy for Europe*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

Foucault, M. (1991). *Discipline and Punish: The Birth of the Prison* (A. Sheridan, Overs.; New Ed edition). Penguin.

Foucault, M. (2007). 1 February 1978. I M. Senellart, F. Ewald, & A. Fontana (Red.), *Security, territory, population: Lectures at the Collège de France, 1977-78* (s. 87–114). Palgrave Macmillan.

Geirbo, H. C. (2017). *Crafting connections - practices of infrastructuring: An ethnographic study of developing a village electricity grid in Bangladesh*. University of Oslo, Faculty of Mathematics and Natural Sciences, Department of Informatics.

Gripsrud, J. (2002). *Mediekultur, mediesamfunn* (2. utg.). Universitetsforl.

Hay, I. M. (2016). *Qualitative research methods in human geography* (4. utgave). Oxford University Press.

Hilgartner, S. (1992). The Social Construction of Risk Objects: Or, How to Pry Open Networks of Risk. I L. Clarke & J. F. S. Jr (Red.), *Organizations, Uncertainties, And Risk* (1 edition). Westview Press.

Hoeyer, K., Bauer, S., & Pickersgill, M. (2019). Datafication and accountability in public health: Introduction to a special issue. *Social Studies of Science*, *49*(4), 459–475. https://doi.org/10.1177/0306312719860202

Hogle, L. F. (2019). Accounting for accountable care: Value-based population health management. *Social Studies of Science*, *49*(4), 556–582. https://doi.org/10.1177/0306312719840429

Høgskolen i Innlandet. (u.å.). *«Nettskjema» (verktøy for datainnsamling)*. Hentet 22. juni 2020, fra https://www.inn.no/bibliotek/skrive-og-referere/nettskjema-verktoey-for-datainnsamling

Jasanoff, S. (2008). Making Order: Law and Science in Action. I E. J. Hackett, O. Amsterdamska, J. Wajcman, & M. Lynch (Red.), *The Handbook of Science and Technology Studies*. MIT Press.

Kuner, C., Jerker, D., Svantesson, B., Cate, F. H., Lynskey, O., Millard, C., & Ni Loideain, N. (2017). The GDPR as a chance to break down borders. *International Data Privacy Law*, *7*(4), 231–232. https://doi.org/10.1093/idpl/ipx023

Latour, B. (1999). *Pandora's hope: Essays on the reality of science studies*. Harvard University Press.

Latour, B. (2004). *Politics of nature: How to bring the sciences into democracy* (s. X, 307). Harvard University Press.

Latour, B. (2009). *The Making of Law: An Ethnography of the Conseil d'Etat* (1 edition). Polity.

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems Practice*, *5*(4), 379–393. https://doi.org/10.1007/BF01059830

Law, J. (2004). *After method: Mess in social science research* (s. VIII, 188). Routledge.

Law, J. (2007). *Actor Network Theory and Material Semiotics*. http://www.heterogeneities.net/publications/Law2007ANTandMaterialSemiotics.pdf

Law, J. (2015). On the Methods of Long-Distance Control: Vessels, Navigation and the Portuguese Route to India: *The Sociological Review*. https://journals.sagepub.com/doi/10.1111/j.1467-954X.1984.tb00114.x

Marres, N. (2007). The Issues Deserve More Credit: Pragmatist Contributions to the Study of Public Involvement in Controversy. *Social Studies of Science*, *37*(5), 759–780. https://doi.org/10.1177/0306312706077367

Mol, A. (2003). *The Body Multiple: Ontology in Medical Practice*. Duke University Press.

Muniesa, F. (2011). A Flank Movement in the Understanding of Valuation. *The Sociological Review*, *59*(2_suppl), 24–38. https://doi.org/10.1111/j.1467-954X.2012.02056.x

Nick Seaver. (2019). Knowing Algorithms. I David Ribes & Janet Vertesi (Red.), *DigitalSTS: A Field Guide for Science & Technology Studies* (s. 412-). Princeton University Press.

Olsen, E. D. H., Rosén, G., & Trondal, J. (2017). *Hvordan virker EU?* (s. 218). Universitetsforlaget.

Power, M. (1997). *The Audit Society: Rituals of Verification* (1. utg. reprinted 2013., s. XIX, 183). University Press.

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176

Reidenberg, J. (1997). Lex Informatica: The Formulation of Information Policy Rules through Technology. *Tex. L. Rev.*, *76*, 553.

Reinertsen, H. (2016). *Optics of Evaluation. Making Norwegian foreign aid an evaluable object, 1980-1992*. https://www.duo.uio.no/handle/10852/50572

Raab, C. (2012). The Meaning of 'Accountability' in the Information Privacy Context. I *Managing Privacy through Accountability*. Palgrave Macmillan UK : Imprint: Palgrave Macmillan.

Sejersted, F. (1998). *Teknologipolitikk*. Universitetsforl. http://urn.nb.no/URN:NBN:no-nb_digibok_2010051208014

Skjølsvold, T. M. (2015). *Vitenskap, teknologi og samfunn: En introduksjon til STS*. Cappelen Damm akademisk.

Skullerud, Å. M. B., Rønnevik, C., Skorstad, J., & Pellerud, M. E. (2019). *Personopplysningsloven og personvernforordningen (GDPR): Lov om behandling av personopplysninger 15. juni 2018 nr. 38 (personopplysningsloven) og Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) : kommentarutgave*. Universitetsforlaget.

Star, S. L., & Bowker, G. C. (2002). How to Infrastructure. I *Handbook of New Media: Social Shaping and Consequences of ICTs* (s. 151–162). SAGE Publications, Ltd. https://doi.org/10.4135/9781848608245

Thompson, C. (2013). *Good Science: The Ethical Choreography of Stem Cell Research*. The MIT Press.

Universitetsforlaget. (u.å.). *Personopplysningsloven og personvernforordningen (GDPR)*. Hentet 23. mai 2020, fra https://www.universitetsforlaget.no/personopplysningsloven-og-personvernforordningen-gdpr-1

USIT. (u.å.-a). *Nettskjema*. Hentet 29. april 2020, fra https://www.uio.no/tjenester/it/adm-app/nettskjema/index.html

USIT. (u.å.-b). *Om USIT*. Hentet 29. april 2020, fra https://www.usit.uio.no/om/index.html

USIT. (u.å.-c). *Sikkert Nettskjema og særlige kategorier av personopplysninger*. Hentet 22. juni 2020, fra https://www.uio.no/tjenester/it/adm-app/nettskjema/hjelp/opprette/nettskjema-og-sensitive-data.html

van den Hoonaard, W. C. (2008). Sensitizing Concepts. I L. Given (Red.), *The SAGE Encyclopedia of Qualitative Research Methods*. SAGE Publications, Inc. https://doi.org/10.4135/9781412963909.n422

Vertesi, J., Ribes, D., DiSalvo, C., Loukissas, Y., Forlano, L., Rosner, D. K., Jackson, S. J., & Shell, H. R. (Red.). (2019). Introduction. I *DigitalSTS* (s. 1–10). Princeton University Press; JSTOR. www.jstor.org/stable/j.ctvc77mp9.4

Weiss, R. S. (1994). *Learning from strangers: The art and method of qualitative interview studies*. Free Press.

Ziewitz, M. (2016). Governing Algorithms: Myth, Mess, and Methods. *Science, Technology, & Human Values*, *41*(1), 3–16. https://doi.org/10.1177/0162243915608948