Personvernrettslige utfordringer ved kameraovervåkning på arbeidsplassen

Perspektiver fra et studium av intelligent videoanalyse

Kandidatnummer: 5

Antall ord: 11 763

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

30.05.2018

“Big Brother is watching you”
- George Orwell, 1984

Innholdsfortegnelse

1 Innledning

1.1 Tema og problemstilling

Den teknologiske utviklingen har de siste årene skjedd så raskt at det nesten daglig kommer nye løsninger på markedet. Til illustrasjon melder Datatilsynet om prototyper på kameraer som er sammensatt av flere mikrokameraer. Resultatet er at overvåkningskameraene kan oppnå en kvalitet på oppimot én gigapiksel. Dette muliggjør identifisering av hvert eneste menneske som befinner seg på et område tilsvarende en hel fotballstadion eller et stort bytorg.[1] De nye overvåkningskameraene har med andre ord 988 megapiksler mer enn dagens beste telefoner.[2]

Det ingen tvil om at det meste vi foretar oss i løpet av en dag blir registrert. Uavhengig av om du er på Instagram eller shopper på nettet, eller om du går innom en butikk og benytter deg av bankkortet, legger man igjen spor og fanges opp av overvåkningskameraer. Det er tilnærmet umulig å komme seg unna teknologiens haukeøyne i dagens samfunn.

Teknologien gir arbeidsgiver stadig større valgmulighet når det kommer til kontrolltiltak på arbeidsplassen. Et praktisk og stadig mer aktuelt kontrolltiltak, er kameraovervåkning. Overvåkningen skal bidra til at arbeidsplassen er en sikker og trygg plass for arbeidstakerne. Samtidig kan arbeidsgiver oppdage underslag og andre forbrytelser og misligheter dersom det foreligger mistanke om dette. Resultatet av overvåkning på arbeidsplassen er likevel ikke så svart/hvitt. Dagens teknologi blir billigere, og derfor mer tilgjengelig for arbeidsgiver å benytte. Dette kan medføre alvorlige konsekvenser dersom overvåkning ikke tas på alvor. Eksempelvis åpner den teknologiske utviklingen for uautorisert salg av opplysninger, mengdeinnsamling av personopplysninger og indirekte diskriminering på arbeidsplassen.

Oppgaven vil ta for seg kameraovervåkning på arbeidsplassen. Mer presist er det overordnede spørsmålet hvilke personvernrettslige utfordringer som oppstår ved bruk av kameraovervåkning på arbeidsplassen. Oppgaven vil legge særlig vekt på kameraovervåkning

[1] Datatilsynets rapport (2016) s. 18
[2] www.apple.com/no

med intelligent videoanalyse,[3] og hvordan denne teknologien påvirker arbeidstakers personvern sammenlignet med tradisjonell kameraovervåkning.

1.2 Aktualitet

I mai 2018 trådte EUs nye Personvernforordning[4] General Data Protection Regulation (GDPR) i kraft. I den anledning får Norge en ny personopplysninglov, som trolig vil tre i kraft i løpet av juli 2018.[5] Personopplysningsloven implementerer forordningen og sikrer at norsk rett er i samsvar med personvernreglene i EU. Etter år med debatt om GDPR i virksomheter over hele Europa, er den nå gjeldende rett. Et gjennomgående tema har vært hvorvidt virksomhetene vet hva de nye personvern-endringene innebærer, og om de er forberedt på dem. I den forbindelse gjennomførte Deloitte en undersøkelse i februar 2017, hvor kun 19% av virksomhetene som deltok svarte at de var godt eller svært godt forberedt på de nye reglene som skulle tre i kraft om et drøyt år.[6] En del virksomheter har derfor hatt en travel vår i 2018 for å sikre at de i tilstrekkelig grad har implementert de nye reglene. Da den nye personopplysningsloven trer i kraft først i juli, kan det videre virke som også regjeringen har hatt et travelt år med implementeringen av GDPR.

En virksomhet som har hatt det travelt denne våren er Facebook, etter «Cambridge Analytica-skandalen» fant sted i mars. Skandalen gjaldt selskapet Cambridge Analytica som hadde samlet inn brukerdata fra flere titalls millioner Facebook-brukere. Som et resultat av dette slettet mange brukerkontoen sin hos Facebook, da de følte at deres personvern ikke ble tilstrekkelig ivaretatt.[7] At GDPR har gitt økt oppmerksomhet og fokus på den betydelige verdien enkeltindividets personopplysninger har, kan nok være en av faktorene til at folk opplevde Facebook-skandalen som såpass inngripende.

Parallelt med personvernets voksende aktualitet, har det skjedd nyutviklinger på den teknologiske fronten når det kommer til bruk av intelligent videoanalyse. Blant annet åpnet netthandel-selskapet Amazon en dagligvarebutikk i Seattle i starten av 2018. Butikken er basert på en kombinasjon av kamerateknologi, maskinlæring og sensorer som tillater butikkens kunder å ta med seg varene de skulle trenge, uten å gå gjennom et kassasystem på

[3] Se punkt 2.6 for nærmere forklaring av begrepet
[4] Regulation 2016/679
[5] Justis- og beredskapsdepartementet (2018), regjeringen.no
[6] Deloittes personvernundersøkelse 2017
[7] Plikk (2018), Tek.no

vei ut av butikken. Varene trekkes automatisk fra deres Amazon-konto på vei ut.[8]
Et annet eksempel på nyutviklinger ved bruk av intelligent videoanalyse og maskinlæring, finner man i lakseoppdrettsnæringen. Startup-bedriften Aquabyte tilbyr blant annet en ny måte å undersøke laks i oppdrettsanlegg for lus ved bruk av kamerainstallasjoner nede i merdene.[9]

Kameraer med intelligent videoanalyse i overvåkningssammenheng har blitt billigere å bruke de siste årene.[10] Dette åpner for at flere virksomheter kan benytte seg av slike kameraer. Etterspørsel og bruk antas derfor å ville øke.

Bruk av kameraer med intelligent videoanalyse på arbeidsplassen er således et aktuelt og spennende tema sett i lys av arbeidstakers personvern. På den ene siden gjør intelligent videoanalyse kameraovervåkningen enklere for arbeidsgiver. På den andre siden skal denne teknologien benyttes innenfor personvernets stadig strengere rammer.

1.3 Rettskildebildet

Oppgavens problemstilling berører både nasjonal og internasjonal rett. EUs nye Personvernforordning erstatter personverndirektivet,[11] og ligger dermed som et bakteppe for den rettslige reguleringen av kameraovervåkning på arbeidsplassen. Forordningen angir de generelle retningslinjene for reglementet som gjelder om personvern på nasjonalt nivå. GDPR viderefører hovedprinsippene i tidligere gjeldende direktiv, men tilpasser regelverket til den teknologiske utviklingen og styrker personers vern av personopplysninger ytterligere. Personvernforordningen anses som den viktigste endringen på 20 år sett i lys av menneskets personvern innen det teknologiske feltet.[12] Forordningen skal videre sikre at personvernreglene i Europa blir mer enhetlige.[13] I Norge gjennomføres regelverket ved inkorporasjon gjennom den kommende personopplysningsloven § 1.[14]

[8] Dagens Næringsliv, publisert 22.01.2018
[9] www.aquabyte.no
[10] Datatilsynets rapport (2016) s. 14
[11] Direktiv 95/46/EF
[12] www.eugdpr.org
[13] www.regjeringen.no «Ny lov om behandling av personopplysninger på høring»
[14] Se til det utkastet til ny personopplysningslov, Prop. 56 LS (2017-2018) s. 237.
Vi er videre forpliktet til å inkorporere forordningen gjennom EØS-avtalen artikkel 7 bokstav a.

I likhet med personverndirektivet inneholder ikke Personvernforordningen noen konkret regulering av kameraovervåkning. Departementet har derfor funnet det hensiktsmessig å ha nasjonale regler om kameraovervåkning på arbeidsplassen i tillegg til de generelle reglene som fremkommer av GDPR. Grunnlaget for nasjonale regler om kameraovervåkning finner Departementet i forordningens art. 88 som åpner for at «*Medlemsstatene kan […] fastsette nærmere regler […] i forbindelse med ansettelsesforhold…».*

Departementet la ved et utkast til bestemmelser om kameraovervåkning på arbeidsplassen i høringsnotatet om ny personopplysningslov,[15] men valgte å ikke videreføre disse reglene i ny lov. Begrunnelsen for avgjørelsen er at Departementet anser det som mer hensiktsmessig at reglene bør plasseres i en forskrift tilknyttet arbeidsmiljøloven[16] (aml.).[17] Reglene i utkastet er i hovedsak en videreføring av bestemmelsene etter den gamle personopplysningsloven kapittel VII.[18] I proposisjonens vedlegg A «Forslag til lov om behandling av personopplysninger (personopplysningsloven)» har Departementet i § 34 lagt frem forslag om ny § 9-6 i arbeidsmiljøloven, som skal inneholde en hjemmel for en forskrift om kameraovervåkning i virksomheten.[19] Det forventes derfor at det kommer en forskrift som regulerer kameraovervåkning på arbeidsplassen nasjonalt, i nærmeste fremtid.

Etter norsk rett faller man således tilbake på intern, nasjonal lovgivning hva angår kameraovervåkning på arbeidsplassen. Inngangsvilkårene for overvåkning følger av arbeidsmiljøloven kapittel 9, som omhandler arbeidsgivers muligheter til å utføre kontrolltiltak i virksomheten.

I tillegg til lovgivningen vil tilhørende forarbeider til arbeidsmiljøloven og personopplysningsloven være relevant for identifiseringen av personvernrettslige utfordringer ved kameraovervåkning på arbeidsplassen, da disse bidrar til å presisere lovens innhold. Det samme gjelder uttalelser fra Artikkel 29-gruppen, som er EUs oppnevnte rådgivende organ som passer på at personvernreglene etterleves i EU og EØS.[20]

[15] Høringsnotat 6 juli 2017 Snr. 17/4200 s. 133
[16] Lov 17.06.2005 nr. 62
[17] Prop. 56 LS (2017-2018) s. 177 punkt 31.3.3.3
[18] Lov 14.04.2000 nr. 31
[19] Prop. 56 LS (2017-2018) s. 245
[20] www.datatilsynet.no «Søkemotorers plikter – Artikkel 29-gruppen»

Personopplysninger har dessuten et vidtrekkende vern gjennom EMK art 8 nr. 1 som sier at «*enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse*». Norge er forpliktet til å sikre etterlevelse av artikkelen da Den europeiske menneskerettskonvensjon er bindende for Norge, jf. menneskerettighetsloven § 2.[21] Retten til privatliv har også grunnlovs rang, jf. Grunnloven § 102.[22]

Når det kommer til rettspraksis, finnes det lite om kameraovervåkning på arbeidsplassen. De Høyesterettsavgjørelsene som gjelder dette temaet, berører tilfeller der det er skjedd et brudd på reglene om kameraovervåkning. Et tilfelle som går igjen i retten, er arbeidsgivers manglende opplysning til arbeidstakerne om at virksomheten har kameraovervåkning av de ansatte.[23] At det foreligger lite rettspraksis på området kan være et resultat av at mange personvernsaker blir behandlet av Datatilsynet og Personvernnemnda. Datatilsynet er et uavhengig forvaltningsorgan som utleder sin myndighet gjennom pol. § 42. Personvernnemnda er også et uavhengig forvaltningsorgan, og avgjør klager over Datatilsynets avgjørelser etter pol. § 43 jf. 42 fjerde ledd. Disse synes videreført i ny personopplysninglov, hhv pol. §§ 20 og 22.[24]

Ved identifiseringen av personvernrettslige utfordringer ved kameraovervåkning på arbeidsplassen har det metodisk vært utfordrende å behandle et relativt nytt felt. Rettsutviklingen på dette feltet har skjedd gradvis gjennom våren, og et resultat av dette har vært at rettskildene har vært tidvis begrenset. Siden reglementet er nytt fra 25. mai 2018, vil også rettsutviklingen i EU og Norge etter ikrafttredelsen av GDPR være utenfor rettskildebildets rekkevidde.

1.4 Avgrensning

Det overordnede spørsmålet retter seg mot arbeidstakers personvern. Oppgaven avgrenses derfor mot overvåkning andre steder enn på arbeidsplassen. Dette betyr videre at oppgaven heller ikke vil behandle situasjoner hvor andre mennesker enn de som er arbeidstakere i

[21] Lov 21.05.1999 nr. 30
[22] Lov 17.05.1814
[23]Se blant annet Rt. 1991 s. 616 «Gatekjøkkenkjennelsen» og Rt. 2001 s. 688 «Tippekassekjennelsen»
[24] Prop. 56 LS (2017-2018) s. 240

virksomheten, blir fanget opp av kamera. Kunder og besøk på arbeidsplassen reiser også personvernspørsmål, men vil altså ikke bli behandlet i det følgende.

Avhandlingens fokus er på kameraovervåkning på arbeidsplassen. Oppgaven vil derfor ikke behandle øvrige kontrolltiltak som arbeidsgiver kan iverksette på arbeidsplassen i tråd med arbeidsmiljøloven kapittel 9, selv om dette kan medføre personvernrettslige utfordringer. Den vil heller ikke behandle brudd fra arbeidsgiver sin side på adgangen til å utføre kontrolltiltak etter aml.

Oppgaven vil videre kun å ta for seg personvernreglementet etter forordningen GDPR, Personopplysningloven og Arbeidsmiljøloven.

1.5 Den videre fremstillingen

I den videre fremstillingen skal det gjøres rede for sentrale begreper av relevans for oppgavens videre fremstilling (avsnitt 2), før sentrale hensyn vil bli belyst (avsnitt 3). Deretter vil jeg i avsnitt 4 drøfte personvernrettslige utfordringer som oppstår ved kameraovervåkning på arbeidsplassen ved bruk av intelligent videoanalyse.
Til slutt rundes oppgaven av med noen avsluttende bemerkninger (avsnitt 5).

2 Begrepsforklaringer

2.1 Arbeidstaker og arbeidsgiver

Arbeidstaker og arbeidsgiver er definert i arbeidsmiljøloven § 1-8. Etter aml. § 1-8 første ledd defineres arbeidstaker som enhver som «*utfører arbeid i annens tjeneste*». Denne definisjonen er også brukt i blant annet arbeidstvistloven § 1 bokstav a, men kan variere, slik at arbeidstakerbegrepet anses som relativt.[25]

I henhold til lovens forarbeider er arbeidstakeren normalt økonomisk avhengig og befinner seg i et underordningsforhold til arbeidsgiver.[26] At arbeidstakerbegrepet synes å forutsette et avhengighetsforhold, er videre lagt til grunn i dommen Norsk Stålpress[27] som presiserer at dette er en avgrensning mot selvstendige oppdragstakere og personer med en løsere tilknytning til bedriften. Artikkel 29-gruppen kom imidlertid nylig med uttalelser som kan trekke i retning av at den norske forståelsen må tøyes noe. I Opinion 2/2017 skriver de at arbeidstaker-begrepet skal dekke alle situasjoner hvor det er et arbeidsrettslig forhold uavhengig av om forholdet har grunnlag i en arbeidskontrakt eller ikke. Dette er fordi det har kommet nye business-modeller over de siste årene, slik at eksempelvis freelance-arbeid er blitt mer vanlig.[28]

Videre presiserer forarbeidene at «*en person skal regnes som arbeidstaker i lovens forstand hvis tilknytningen til arbeidsgiver reelt sett har karakter av et ansettelsesforhold*».[29] Dette beror på en skjønnsmessig helhetsvurdering hvor det er det reelle forholdet som er avgjørende, jf. blant annet dommen Avlaster II.[30]

Arbeidsgiver defineres i aml. § 1-8 andre ledd som enhver som har «*ansatt arbeidstaker for å utføre arbeid i sin tjeneste*». Arbeidsgiverbegrepet i loven er definert ut fra ansettelsesforholdet som forutsetter en arbeidsavtale. Det er derfor inngåelsen av en arbeidsavtale som i utgangspunktet knytter noen til arbeidsgiverbegrepet og pålegger dem

[25] Skjønberg mfl. (2017) s. 49
[26] Ot.prp.nr.49 (2004-2005) s 73.
[27] Rt. 1986 s. 1322 side 1323
[28] Artikkel 29-gruppen, Opinion 2/2017 s. 4
[29] Ot.prp.nr.49 (2004-2005) s 73.
[30] HR-2016-1366-A avsnitt 62

plikter etter aml.[31] Forarbeidene legger til grunn at også juridiske personer kan være arbeidsgiver, men «*arbeidsgiverfunksjonene vil utøves av den juridiske persons organer eller andre som kan opptre på dennes vegne*».[32]

Det er videre arbeidsgiver som kan foreta kontrolltiltak i virksomheten, dersom tiltaket har «saklig grunn i virksomhetens forhold» og dette ikke innebærer en «uforholdsmessig belastning» for arbeidstaker jf. aml. § 9-1.

2.2 Behandlingsansvarlig og databehandler

Behandlingsansvarlig og databehandler er kjente roller fra personvernlovgivningen, som blir videreført i forordningen. Behandlingsansvarlig er definert i GDPR art. 4 nr. 7 som en

> «*Fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes […]».*

En behandlingsansvarlig har med andre ord hovedansvaret for å fastsette hvilke formål personopplysninger skal behandles etter, samt sikre at virksomheten behandler personopplysningene innenfor dette formålet og gjeldende regelverk til enhver tid.

I forarbeidene til personopplysningsloven presiseres det at man som behandlingsansvarlig ikke kan fraskrive seg ansvaret og bestemmelsesretten ved å sette arbeidet bort til noen andre. Et naturlig utgangspunkt er derfor at det kun er rettssubjekter med partsevne som kan sitte som behandlingsansvarlig. Med dette menes det at det foreligger en mulighet for å bli saksøkt og at saken kan føres for domstolene. Som regel vil det være en juridisk person som er virksomhetens behandlingsansvarlige.[33]

Databehandler er definert i GDPR art. 4 nr. 8, og er en:

> «*Fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige*».

[31] Skjønberg mfl. (2017) s. 58-59
[32] Ot.prp.nr.49 (2004-2005) s 74
[33] NOU 1997:19 s. 132

En databehandler vil ofte være en leverandør av IT-tjenester. [34] Forordningen art. 28 punkt 3 krever at databehandlerens behandling av virksomhetens data skal være fastsatt ved avtale med den behandlingsansvarlige. Databehandlere opptrer derfor kun på oppdrag fra en behandlingsansvarlig. Artikkel 28 punkt 2 presiserer videre at databehandleren ikke kan engasjere andre databehandlere uten at det er blitt innhentet samtykke om dette fra den behandlingsansvarlige. Reglene skal sikre at databehandleren er autorisert til å behandle den aktuelle informasjonen og at arbeidet blir underlagt en form for taushetsplikt. Avtalen skal videre sikre at de kun behandler de personopplysningene som blir etterspurt i oppdraget.[35]

2.3 Personvern

Personvern er ikke legaldefinert i verken norsk eller europeisk rett. Departementet virker imidlertid til å ønske å videreføre gjeldende rett i den grad dette lar seg gjøre ved den nye lovreguleringen for 2018.[36] Det kan derfor virke som nåværende personopplysningslov og tilknyttede forarbeider fortsatt vil være av aktualitet ved forståelsen av ordet personvern også etter ny lov trer i kraft.

Det legges derfor til grunn at personvern skal forstås på samme måte både før og etter forordningen trer i kraft. Av pol. § 1 første ledd fremkommer det at formålet med loven er å «*beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger*». Videre har Personvernkommisjonen lagt følgende definisjon til grunn: «*Personvern dreier seg om ivaretakelse av personlig integritet; ivaretakelse av enkeltindividets mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse*».[37]

I pol. § 1 andre ledd står det videre at personopplysninger skal bli behandlet i samsvar med «grunnleggende personvernhensyn» som «*behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger*». Forarbeidene utdyper at «*den enkeltes ukrenkelighet skal respekteres både i privatliv, arbeidsliv og i offentlige sammenhenger*», samt at enhver i utgangspunktet har «*råderett over kunnskap denne gir fra seg om seg selv*».[38]

[34] Datatilsynets punktliste «Nye personvernregler fra 2018. Hva betyr det for din virksomhet?» punkt 7.
[35] Regulation 2016/679 Art. 28 punkt 3 bokstav a og b.
[36] Prop. 56 LS (2017-2018) s. 173
[37] NOU 2009:1 s. 32
[38] NOU 1997:19 s. 130-131.

I tillegg til reguleringen av personvern i personopplysningsloven, har man over tid utviklet et ulovfestet personvern gjennom norsk rettspraksis. Dette ulovfestede vernet ble blant annet lagt til grunn av Høyesterett i dommen To mistenkelig personer[39] som begrunnelse for at det ikke var greit å fremføre filmatiseringen. Det vises her til Høyesterett sin uttalelse på side 1219 hvor de sier at det «*… i norsk rett finnes et alminnelig rettsvern for personligheten, og at ankemotparten innenfor rammen av dette vern har rett til å motsette seg oppførelsen av den omhandlende film*».

I boken *Personvern i arbeidsforhold* skriver Kjølaas at vi i dag bruker «personvern» med særlig fokus på den «*enkeltes interesse i å kunne kontrollere behandlingen av opplysninger om seg selv, særlig som følge av dagens IKT*», men at personvern i utvidet forstand «*omfatter mye mer enn vern mot misbruk av elektroniske innsamlede og lagrede opplysninger*».[40]

Internasjonalt benytter man seg i stor utstrekning av begrepet «privatliv» når man snakker om personvern jf. blant annet EMK art. 8. Denne begrepsbruken finner vi igjen i Grunnloven § 102. Begrunnelsen for «privatliv» og «personvern» vil i stor utstrekning være overlappende.[41]

Selv om den enkeltes personvern har stor betydning, eksisterer det ikke et absolutt vern.[42] Arbeidsgiver kan blant annet iverksette nødvendige kontrolltiltak dersom tiltaket har «saklig grunn» og det ikke innebærer en «uforholdsmessig belastning for arbeidstakeren» jf. aml. § 9-1 første ledd. Slik sett fungerer arbeidstakers personvern og arbeidsgivers styringsrett som hverandres begrensning.

2.4 Personopplysninger

Personopplysninger er i GDPR art. 4 nr. 1 definert slik:

> «*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*

[39] Rt. 1952 s. 1217
[40] Kjølaas (2010) s. 21
[41] Svendsen (2010) s. 15
[42] Regulation 2016/679 Fortalen punkt 4

flere elementer som er spesifikke for nevnte fysiske personers fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet».

Definisjonen er en videreføring av personverndirektivet[43] art. 2. Ordlyden viser at det sentrale er at det er skjedd en form for innhenting, lagring eller bruk av informasjon som kan kobles opp til et konkret menneske. Kan ikke den aktuelle informasjonen linkes til en enkeltperson, er den ikke verneverdig personvernsrettslig.[44] Ordlyden legger videre til grunn at juridiske personer ikke har vern etter forordningen.[45]

Artikkel 29-gruppen har uttalt at det ved vurderingen av «enhver opplysning» skal legges til grunn en vid tolkning.[46] Dette underbygges av forordningens fortale punkt 26 hvor det står at «*Når det skal fastslås om en fysisk person er identifiserbar, bør det tas hensyn til alle midler som det med rimelighet kan tenkes […] å identifisere vedkommende direkte eller indirekte […]*».

At man trenger en pin-kode for å kunne identifisere et enkelt menneske ut fra en opplysning regnes derfor også som en personopplysning. Videre vil en opplysning som kun er kjent mellom noen personer ikke være til hinder for at det skjer en identifikasjon mellom opplysningen og personen.[47]

En begrensing etter forordningen er imidlertid at den ikke verner om personopplysninger som blir behandlet i «*rent personlige eller familiemessige aktiviteter*».[48] Forordningen forutsetter med andre ord at opplysningene benyttes i et arbeidsrettslig forhold for at den yter vern.[49]

2.5 Kameraovervåkning

Kameraovervåkning er definert i pol § 36. Ordlyden synes videreført i den kommende personopplysningsloven § 31 annet ledd,[50] samt i utkastet til bestemmelser om kameraovervåkning på arbeidsplassen som Departementet la ved i høringsnotatet for den nye

[43] Direktiv 95/46/EF
[44] Regulation 2016/679 Fortalen punkt 26
[45] Dette er videre slått fast i Regulation 2016/679 Fortalen punkt 14
[46] Artikkel 29-gruppen Opinion 4/2007 s. 6
[47] Ot.prp.nr.92 (1998-1999) s. 101
[48] Regulation 2016/679 art. 2 bokstav c
[49] Dette presiseres videre i Regulation 2016/679 Fortalen punkt 18
[50] Prop. 56 LS (2017-2018) s. 241

personopplysningsloven.[51] Det antas derfor at ordlyden vil være den samme i det nye regelverket.

Etter pol. § 36 første ledd er kameraovervåkning definert som

> «*Vedvarende eller regelmessig gjentatt personovervåkning ved hjelp av fjernbetjent eller automatisk virkende overvåkningskamera eller annet lignende utstyr som er fastmontert*».

Av andre ledd fremkommer det at «*både overvåkning med og uten mulighet for opptak av lyd- og bildemateriale*» anses som kameraovervåkning. Også «*utstyr som lett kan forveksles med ekte kameraløsninger*» faller inn under definisjonen, jf. pol. § 36 første ledd tredje setning. Dette blir omtalt som såkalte «dummy-kameraer», som er «*falske kameraer som har til formål å gi inntrykk av at overvåkning foregår*».[52]

Bestemmelsen gjelder for «personovervåkning». Ordlyden tilsier at formålet med kameraovervåkningen må være å overvåke menneskelig aktivitet. Schartum og Bygrave (2016) skriver at det «*må være påregnelig at opplysninger fra overvåkningen vil omfatte gjenkjennelige fysiske personer, som vil kunne ha verdi for den som overvåker*». Videre skriver de at det holder at det er «*nærliggende og påregnelig at opplysninger fra overvåkningen vil komme til å omfatte fysiske personer*» for å falle innenfor ordlyden personovervåkning.[53]

Personovervåkningen må være av en «vedvarende eller regelmessig» karakter for å falle inn under bestemmelsens virkeområde. Det betyr at det ikke er nok at overvåkningen skjer ved engangstilfeller, men at det må skje jevnlig og av et visst omfang. Vilkåret «Regelmessig gjentatt» omfatter også overvåkning som styres av et dataprogram, slik at man ikke er avhengig av menneskelig innvirkning for å være innenfor pol. § 36.[54]

Ordlyden «fastmontert» i første ledd tilsier at mobilt utstyr som håndholdte kameraer og droner ikke reguleres etter reglene om kameraovervåkning etter pol. Dette er videre klargjort i

[51] Høringsnotat 6 juli 2017 Snr. 17/4200 s. 133.
[52] Prop. 47 L (2011-2012) kap. 9, merknader til § 36
[53] Schartum og Bygrave (2016) s. 215
[54] Schartum og Bygrave (2016) s. 216

lovens forarbeider.[55] Heller ikke kameraer som er montert i lastebiler, taxier og andre ting som er i bevegelse faller innenfor ordlyden.[56]

2.6 Intelligent videoanalyse

Datatilsynet har i rapporten «Sporing i det offentlige rom. Bruk av WiFi, Bluetooth, nettvarder (beacons) og intelligent videoanalyse» gjennomført en utredning av hva intelligent videoanalyse er og hvordan det fungerer. I rapporten forklarer Datatilsynet at Intelligent videoanalyse (IVA) er en teknologi som muliggjør automatisk digital analyse av informasjon som et overvåkningskamera fanger opp ved å tolke endringer fra bilde til bilde.[57]

Videre utdyper Datatilsynet at IVA kan analysere både lagrede opptak eller foreta analysen direkte i overvåkningskameraet. Gjennom bildeanalysen lagres det metadata om hvilken informasjon som finnes i bildene. Rapporten opplyser at metadataene kan være alt fra farge, retning, fart, størrelse, og om det er et kjøretøy eller et menneske.[58]

Datatilsynet deler opp bruksområdene for IVA i tre hovedkategorier: Deteksjon og sporing, beskrive objekter og identifisere objekter. Dette muliggjør at man kan få automatiske varsler basert på forhåndsbaserte kriterier, at man kan foreta konkrete søk i opptak og få tilgang til detaljert statistikk basert på metadataene som analysen registrer.[59]

Som Datatilsynet illustrerer, vil teknologien bak IVA være særlig relevant i sikkerhetsformål, men at det også vil komme nye tilfeller hvor man kan bruke denne teknologien. Blant annet trekker rapporten frem muligheten til å benytte IVA i kommersielle forhold ved å optimalisere reklameinnholdet basert på kundens kjønn og alder, eller om det er en ny eller tidligere kunde av butikken. Et annet eksempel rapporten trekker frem er at teknologien også kan være en god ressurs for arbeidsledelsen, da det bidrar til å planlegge ressursbruk etter opphopning av kø og lignende.[60]

[55] Prop. 47 L (2011-2012) kap. 9, merknader til § 36
[56] Dette legges blant annet til grunn i Høringsnotat 6 juli 2017 Snr. 17/4200 s. 117
[57] Datatilsynets rapport (2016) s. 13
[58] Datatilsynets rapport (2016) s. 13
[59] Datatilsynets rapport (2016) s. 13
[60] Datatilsynets rapport (2016) s. 14

Datatilsynet konkluderer med at det er vanskelig å forutse det fulle spekteret av konsekvenser ved bruk av IVA og at det i prinsippet kun er fantasien som setter grenser for hva som kan analyseres i bildene og hvordan denne informasjonen brukes videre.[61]

[61] Datatilsynets rapport (2016) s. 14

3 Sentrale hensyn

I arbeidsrettslige forhold er det særlig to hensyn som gjør seg gjeldende. På den ene siden har man arbeidsgivers behov om å kunne beskytte virksomheten sin. På den andre siden har man arbeidstakerne, og deres behov for å beskytte deres personopplysninger. Disse hensynene er ofte motstridende da arbeidsgivers behov for sikkerhet på arbeidsplassen utfordrer og griper inn i arbeidstakers personvern. Det er derfor viktig å finne en balanse mellom disse to hensynene. Det er nettopp denne balansen arbeidsmiljøloven, personopplysningsloven og personvernforordningen i stor grad forsøker å regulere.

Arbeidsgiver benytter styringsretten for å oppnå og iverksette relevante kontrolltiltak på arbeidsplassen. Hammerverk-dommen[62] beskriver arbeidsgivers styringsrett som en rettsnorm. Dommen viser til arbeidsrettslig rettspraksis som i lang tid har lagt til grunn at styringsretten tilligger arbeidsgiver. Både som følge av den personlige arbeidsavtalen, men og gjennom tariffmessig forankring.[63] At arbeidsgivers styringsrett er anerkjent både gjennom den personlige arbeidsavtalen og tariffavtaler synes klart allerede i 1922, jf. ARD 1922 s. 86.

Innholdet og rekkevidden av arbeidsgivers styringsrett begrenses av lovgivning, tariffavtaler, og det individuelle arbeidsforholdet. For å slå fast arbeidsgivers handlingsrom i lys av styringsretten må man derfor vurdere grunnlaget for styringsretten innenfor disse tre begrensingene. Handlingsrommet som er igjen etter man har vurdert styringsretten opp mot lovgivning, tariffavtaler og det individuelle arbeidsforholdet, er det arbeidsgiver kan forholde seg til ved utøvelse av styringsretten.[64] Styringsretten kan således betraktes som en form for restkompetanse.[65]

Arbeidsmiljøloven § 9-1 første ledd oppstiller vilkårene for kontrolltiltak i virksomheten, og er et godt eksempel på lovfestede begrensinger av styringsretten. Er ikke vilkårene oppfylt, vil ikke kontrolltiltaket være lovlig å gjennomføre. - Det foreligger ikke handlingsrom.

Når det kommer til begrensninger ut fra det individuelle arbeidsforholdet vil dette bero på en tolkning og utfylling av arbeidsavtalen som er inngått partene imellom.[66] Imidlertid vil ikke

[62] Rt. 1977 s. 902
[63] Rt. 1977 s. 902 side 914
[64] Skjønberg mfl. (2017) s. 100
[65] Evju (2010) s. 41-42
[66] Rt. 2000 s. 1602 «Nøkk» side 1609

enhver regulering av arbeidsvilkårene i avtalen fungere som en begrensing av styringsretten.[67] Avgjørende for om det foreligger en begrensning i styringsretten, er om arbeidsgiver har påtatt seg en særskilt forpliktelse eller gitt et særlig avkall på styringsretten i arbeidsavtalen.[68] I Theatercafé-dommen[69] vurderte Høyesterett hvorvidt en caféeier kunne endre praksisen på arbeidsplassen hva angår tips. Grunnet konflikter mellom servitørene og øvrige arbeidstakere på caféen, ønsket eieren av caféen å dele tipset mellom de ansatte. Retten fant ingen begrensinger i lov eller tariffavtale, og vurderte derfor tilfellet opp mot den individuelle arbeidsavtalen. Arbeidsavtalene inneholdt ingen skriftlige bestemmelser om hvem som hadde rett på tipset. At servitørene hadde blitt informert om tipsordningen på ansettelsesmøtet kunne heller ikke anses som en del av arbeidsavtalens vilkår, men kun orientering av gjeldende praksis på caféen.[70] Arbeidsgiver hadde derfor mulighet til å endre praksis på caféen i lys av styringsretten.[71]

På motsatt side av styringsretten står som nevnt arbeidstakers behov for personvern.[72] Behovet for personvern nyter i dag et godt rettslig vern. Blant annet fungerer EMK art. 8 som et generelt europeisk vern av privatlivet.[73] Tilsvarende regel finner man i Grunnloven § 102. At privatlivet får beskyttelse på grunnlovsnivå styrker vernets posisjon i samfunnet, og understreker at personvern er et viktig aspekt ved lovgivningen i Norge.[74] Personvernkommisjonen har uttalt at en grunnlovfesting av vernet av privatlivet har «*stor betydning både rettslig, politisk og symbolsk*», ved at det stadfester at de «*individuelle rettigheter er en viktig del av vår rettsstat*».[75] Behovet for vern av personopplysninger er antatt å øke i takt med den teknologiske utviklingen, da teknologien muliggjør innsamling, bruk, oppbevaring og spredning av informasjon om den enkelte.[76] Forarbeidene presiserer at vernet ikke er absolutt, men at det «*må utvises respekt for privatlivet, selv under […] overvåkning eller kontroll*» av den enkelte.[77]

[67] NOU 2004:5 side 271
[68] Rt. 2009 s. 1465 «Senvakt» avsnitt 38, HR-2016-2286-A «Rygge kommune» avsnitt 27 og Skjønberg mfl. (2017) side 102
[69] Rt. 2008 s. 856
[70] Rt. 2008 s. 856 avsnitt 36
[71] Rt. 2008 s. 856 avsnitt 52
[72] Se oppgavens punkt 2.3 for nærmere forklaring av personvern
[73] Aall (2015) s. 214
[74] Dok.nr.16 (2011-2012) s. 177
[75] Dok.nr.16 (2011-2012) s. 173
[76] Dok.nr.16 (2011-2012) s. 178
[77] Dok.nr.16 (2011-2012) s. 178

4 Personvernrettslige utfordringer ved kameraovervåkning på arbeidsplassen

4.1 Innledning

I dette kapittelet vil jeg drøfte personvernrettslige utfordringer som oppstår, eller kan oppstå, dersom arbeidsgiver benytter seg av kameraovervåkning på arbeidsplassen. Som nevnt innledningsvis i oppgaven vil det bli lagt særlig vekt på bruk av kameraovervåkning med intelligent videoanalyse ved identifiseringen av de rettslige utfordringene. Hvordan IVA stiller seg i forhold til tradisjonell kameraovervåkning blir behandlet fortløpende i teksten der dette anses fravikelig.

I den videre fremstillingen vil jeg ta for meg følgende personvernsrettslige utfordringer:
I punkt 4.2 vil jeg se på bruk av kameraovervåkning som kontrolltiltak. I Punkt 4.3 vil jeg ta for meg vilkåret «i virksomheten». Deretter vil jeg diskutere det forhold at personvernet ikke er absolutt (punkt 4.4), før jeg går inn i GDPR art. 5 og diskuterer problemstillinger knyttet til krav om formål (punkt 4.5), prinsippet om gjennomsiktighet (punkt 4.6) og kravet om dataminimering (punkt 4.7). I punkt 4.8 vil jeg problematisere menneskelige svakheter ved den teknologiske utviklingen. Punkt 4.9. tar for seg innebygd personvern før jeg avslutningsvis tar for meg problem knyttet til frister for sletting av data i punkt 4.10.

4.2 Kameraovervåkning som kontrolltiltak

4.2.1. Bakgrunn

Arbeidsgiver kan etter arbeidsmiljøloven utføre et eller flere kontrolltiltak i virksomheten dersom de aktuelle vilkårene som nevnt i punkt 2.1, er oppfylt. Hvor inngripende kontrolltiltaket er på arbeidstaker varierer i stor grad mellom de ulike formene for kontrolltiltak. Kameraovervåkning vil være et av de kontrolltiltakene som i økt grad griper inn i arbeidstakers personvern. Dette er fordi kameraer monitorerer et fast område over lenger tid og kan plukke opp ting som arbeidsgiver ellers ikke ville fått med seg. At kameraovervåkning oppleves som et inngripende kontrolltiltak ser man blant annet ved at personvernopplysningsloven oppstiller egne regler for kameraovervåkning i kapittel VII. Det betyr at kameraovervåkning på arbeidsplassen er underlagt et dobbelt sett med regler; både de

alminnelige reglene for kontrolltiltak i arbeidsmiljøloven og de spesielle reglene om kameraovervåkning i personopplysningsloven. Et annet argument for at kameraovervåkning er et inngripende tiltak er at personvernreglene likestiller dummy-kameraer[78] med ordentlige kameraer som tar opp lyd og/eller bilde.[79] Det er derfor nok at en person *tror* han blir filmet for at dette regnes som et inngrep i personvernet. Det samme gjelder for falsk skilting av overvåkning på området.

4.2.2. Økt inngrep i personvernet ved bruk av IVA?

Kameraovervåkning representerer en stor personvernsrettslig utfordring nettopp fordi det oppleves som svært inngripende for arbeidstaker. Det er ikke alt man ønsker at skal bli fanget opp av et kamera, med mulighet for nærmere ettersyn. Det er derfor viktig at arbeidsplassen ikke blir overvåket mer enn det reglene tillater.

Kriminolog Heidi Mork Lomell (2010) nyanserer synet på kameraovervåkning som et inngripende kontrolltiltak ved å poengtere at «*hovedmengden av videoovervåkningssystemene i Norge baserer seg […] på reaktiv filming og symbolsk avskrekking heller enn proaktiv overvåkning*». Forskning viser derfor at man som «*hovedregel ikke blir sett selv om man går forbi et overvåkningskamera*».[80]

Dette synspunktet støttes av at arbeidsgiver ikke lenger trenger å se igjennom alle opptakene sekund for sekund, slik de måtte før. Kameraer med IVA-teknologi tillater søk på konkrete detaljer, slik at arbeidsgiver kun vil se de sekvensene av opptaket som samsvarer med søket. Teknologien bidrar med andre ord til en mer effektiv og enkel overvåkningsløsning for arbeidsgiver.

Et positivt resultat av at arbeidsgiver kan søke i opptakene på bakgrunn av definerte kriterier, er videre at det kan skåne arbeidstakeren for unødvendig gjennomsyn av overvåkningsopptakene fra arbeidsgiver sin side. Med andre ord vil det meste av opptaket forbli usett ved bruk av hurtigsøking. Datatilsynet presiserer i den sammenheng at det ikke vil være selve IVA-teknologien som vil være personvernkrenkende, men bruken av

[78] Se punkt 2.5 for definisjon
[79] Lov 14.04.2000 nr. 31 § 36 første ledd tredje setning
[80] Lomell (2010) s. 246

teknologien.[81] Dette kan trekke i retning av at kameraer med IVA ikke er å anse som mer inngripende i den enkeltes personvern enn hva tradisjonell kameraovervåkning er.

Likevel er det ikke å komme unna det faktum at IVA-teknologien automatisk samler inn og identifiserer enorme mengder av data ut fra hvert enkelt bilde som registreres på kameraet. Resultatet av dette er at arbeidsgiver sitter med store data som de kan søke seg frem i, uten å løfte en finger for å opparbeide seg denne informasjonen. Et slikt informasjonslager vil mest sannsynlig kreve flere titalls timer med logg-arbeid per opptak.
Dette poenget fremhever Datatilsynet som et sentralt argument for hvorfor IVA er å anse som et enda større inngrep i den enkeltes personvern enn tradisjonell kameraovervåkning. Særlig gjelder dette fordi man ved IVA automatisk blir registrert dersom man befinner seg innenfor kameraets synsfelt. Det betyr at IVA-teknologien muliggjør at det trekkes slutninger om det som skjer på overvåkningsbildene uten at en fysisk person er til stede og ser på opptakene.[82]

Bruken av IVA resulterer derfor i at forskningen som Lomell viser til når hun påpeker at man i de fleste tilfeller ikke blir sett, antagelig ikke holder mål lenger. Selv om arbeidsgiver sannsynligvis ikke vil se det meste av opptaket, vil teknologien fortsatt registrere all bevegelse og trekke slutninger ut fra bildene. Dette havner så i en søkbar database, hvor arbeidsgiver kan sitte med detaljer og sammenhenger han kanskje ikke hadde oppdaget om han så på opptakene manuelt.

På denne bakgrunn påpeker Schartum (2010) en sentral virkning av den teknologiske utviklingen. Han mener at teknologi kan øke tillitten i samfunnet om at det skjer en «*rettslig effektiv regulering*».[83] Med økende fremtidig bruk av IVA, vil han nok ha rett i dette. Siden IVA opererer uten at noen må være til stede, kan man være sikker på at alle bevegelser blir registrert og logget presist til enhver tid. Et resultat av dette kan bli at man vil bevege seg mer over mot en proaktiv overvåkning.

Schartum presiserer imidlertid at:

> «*Muligheten for å bruke automatisering bygger på den enkle observasjonen at datasystemer alltid følger regler. Så lenge arbeid bare kan skje ved bruk av datamaskinsystemer, vil det alltid utføres i tråd med gjeldende regler.*

[81] Datatilsynets rapport (2016) s. 16
[82] Datatilsynets rapport (2016) s. 16
[83] Schartum (2010) s. 32

> *Forutsetningen er selvfølgelig at aktuelle rettsregler kan uttrykkes i programmeringsspråk og således styre myndighetenes arbeid*».[84]

Det Schartum konstaterer her er at IVA bare kan brukes i den grad teknologiens rekkevidde innskrenkes gjennom programmeringsspråket, slik at ethvert bruk av IVA vil være i tråd med forordningens rammer.

Forutsetningen er med andre ord at systemutviklerne bak intelligent videoanalyse må tolke GDPR for å se hvilke prosessuelle og materielle krav forordningen oppstiller for ivaretakelse av den enkeltes personvern. Deretter må utviklerne få konvertert de rettslige kravene inn i programmet ved bruk av aktuell koding under programmeringen av systemet.

4.2.3. Oppsummering

At man må befinne seg innenfor forordningens rammer tilsier at bruk av IVA ikke vil representere en større personvernsrettslig utfordring på arbeidsplassen enn det tradisjonell kameraovervåkning gjør. Likevel støtter jeg meg til Datatilsynets syn om at IVA vil bli enda raskere og mer presis i fremtiden, slik at «*potensialet for inngripende overvåkning [er] dramatisk*» og at det videre vil være «*vanskelig å forutse det fulle spekteret av konsekvenser over tid*».[85]

4.3 Vilkåret «i virksomheten».

4.3.1 Reglenes virkeområde

I GDPR art. 3, som omhandler forordningens geografiske virkeområdet, fremgår det at

> *«Denne forordning får anvendelse på behandling av personopplysninger som utføres i forbindelse med aktivitetene ved virksomheten til en behandlingsansvarlig eller en databehandler i Unionen, uavhengig av om behandlingen finner sted i Unionen eller ikke».*

[84] Schartum (2010) s. 32-33
[85] Datatilsynets rapport (2016) s. 14 og 16

Personvernforordningen gjelder altså behandling av personopplysninger i forbindelse med «virksomheten». Videre åpner art. 88 for nærmere fastsettelse av nasjonale regler om behandling av personopplysninger i forbindelse med ansettelsesforhold.

I lys av artikkel 88 fant Departementet det hensiktsmessig å fastsette nasjonale særregler for kameraovervåkning, som i dag forefinnes i personopplysningsloven kapittel VII. I høringsnotatet la Departementet frem utkast til regler om kameraovervåkning på «arbeidsplass».[86] Dette ble av mange kommentert i høringssvarene. Det ble påpekt at begrepet «arbeidsplass» anses som uklart.[87] I proposisjonen som kom i mars 2018, endret derfor Departementet reglene til å gjelde for arbeidsgivers kameraovervåkning «i virksomheten».[88] Reglene samsvarer således med ordlyden i GDPR og arbeidsmiljøloven kapittel 9.

4.3.2 Tilstrekkelig avgrensning?

Spørsmålet er dermed om denne ordbruken vil medføre en tilstrekkelig avgrensning av kameraovervåkning på arbeidsplassen. Dersom avgrensningen ikke er tilstrekkelig vil dette kunne medføre en personvernsrettslig utfordring for arbeidstakerne.

Ordlyden «i virksomheten» avgrenser ikke mot kameraovervåkning av pauserom, ved kassen og liknende. Dette betyr at ordlyden isolert sett har en stor rekkevidde og forstås vidt. Et resultat av dette er at arbeidstakers personvern kan bli utsatt for inngrep på steder hvor arbeidstakeren skal kunne slippe å bli overvåket. Dette vil typisk gjelde pauserom hvor arbeidstaker ikke ekspederer kunder og hvor man har lunsjpauser. At ordlyden må forstås vidt støttes av at Departementet uttaler at begrepet i prinsippet vil gjelde «*alle steder hvor arbeidstakerne arbeider*» og at det vil gjelde «*kameraovervåkning i virksomheter generelt*»[89]

Likevel understrekes det at Departementet ønsker å videreføre reglene som har vært, slik at områder på arbeidsplassen hvor det ferdes en begrenset krets av personer vil være underlagt ytterligere reguleringer.[90] Dette vil forhåpentligvis innskrenke det stedlige virkeområdet «i virksomheten» i noen grad.

[86] Høringsnotat 6 juli 2017 Snr. 17/4200 s. 133
[87] Se til det blant annet høringssvarene fra Datatilsynet, Kripos, Juristforeningen og Sporveien Oslo AS, jf. Prop. 56 LS (2017-2018) s. 175
[88] Prop. 56 LS (2017-2018) s. 177
[89] Prop. 56 LS (2017-2018) s. 177
[90] Prop. 56 LS (2017-2018) s. 177 sammenholdt med Lov 14.04.2000 nr. 31 § 38

En annen innskrenkning som vil følge av de nasjonale reguleringene er at det kun er arbeidsgiver sine kameraer som vil falle innenfor reglene. Det betyr at dersom andre kameraer enn arbeidsgiver sine kameraer registrerer personer på arbeidsplassen, vil ikke reglene hindre et inngrep i personvernet til den enkelte.[91] Til illustrasjon vil ikke et kamera som er montert ute i gaten falle innenfor personvernsreglementet selv om det fanger opp inngangspartiet til arbeidsplassen, med mindre dette er arbeidsgivers kamera. Dette er derfor en innskrenkning som i utgangspunktet ikke styrker personvernet. På den andre siden er arbeidstaker i det minste sikret mot at arbeidsgiver ikke misbruker den informasjonen utenforliggende kameraer fanger opp. Følelsen av forsikring forutsetter selvsagt at arbeidstaker har oversikt over hvilke kameraer som tilhører arbeidsgiver og ikke.

I høringssvaret til Sporveien uttrykkes det tvil om Departementet er i tråd med forordningen ved bruk av ordet «arbeidsplass». Som nevnt åpner forordningen artikkel 88 for nasjonale regler hva angår *ansettelsesforhold*. Kameraovervåkning på arbeidsplassen vil derimot stadig omfatte mer enn kun ansettelsesforhold, siden kameraer ofte brukes av sikkerhetsmessige hensyn. Overvåkningens formål er med andre ord i utgangspunktet ikke rettet mot de ansatte. Sporveien mener derfor at departementets formuleringer i utkastet til bestemmelser om kameraovervåkning går for langt i lys av den åpningen artikkel 88 hjemler.[92]

Ettersom utkastet til reglene om kameraovervåkning vil bli videreført gjennom forskrift tilknyttet arbeidsmiljøloven, er det per i dag ikke mulig å se hvorvidt Departementet har tatt stilling til Sporveien sine innsigelser om reglenes rekkevidde. Imidlertid virker ikke endringen fra «arbeidsplass» til «i virksomheten» isolert sett til å bidra til en klargjøring på dette området. Det faktum at Departementet i proposisjonen som nevnt uttaler at reglene vil gjelde «*kameraovervåkning i virksomheter <u>generelt</u>*» (min understrekning), kan riktignok trekke i retning av at dette ikke er blitt gjort.[93]

4.3.3 Oppsummering

Det synes vanskelig å se hvordan vilkåret «i virksomheten» skal kunne begrense og klargjøre anvendelsesområdet for reglene i større grad enn det vilkåret «arbeidsplass» gjør. Likevel vil

[91] Prop. 56 LS (2017-2018) s. 177
[92] Sporveien sitt høringssvar til Høringsnotat 6 juli 2017, s. 3
[93] Prop. 56 LS (2017-2018) s. 177

denne begrepsbruken være mest hensiktsmessig, da den vil være mer i tråd med øvrige relevante bestemmelser og lovens system. Uklarheten rundt vilkåret «i virksomheten» kan videre tyde på at det kreves en del presiseringer i den kommende forskriften, som skal særregulere kameraovervåkning, før disse reglene vil være i tråd med forordningen. Slik reglene stiller seg per i dag, sett i lys av utkastet som er vedlagt høringsnotatet, vil kameraovervåkningen på arbeidsplassen kunne gripe inn i personvernet i større grad enn det forordningen legger opp til. Se til det Sporveien sin ovenfor nevnte bekymring i høringssvaret til Departementets Høringsnotat 6. juli 2017.

4.4 Retten til egne opplysninger

4.4.1 Personvern til besvær?

I utgangspunktet skal alle fysiske personer kunne bestemme over egne opplysninger.[94] Det kreves derfor et rettslig grunnlag for å kunne behandle personopplysninger om andre. Etter pol. § 8 fremkommer det at personopplysninger kun kan behandles dersom den registrerte har samtykket, det foreligger adgang etter loven for den aktuelle behandlingen, eller at behandlingen anses nødvendig etter bokstav a – f.

Arbeidsgivers adgang til å monitorere arbeidsplassen ved bruk av kameraovervåkning følger av arbeidsmiljøloven.[95] Siden adgangen til å utføre kontrolltiltak reguleres gjennom lov, vil arbeidstaker i prinsippet aldri kunne påvirke kameraovervåkningen på arbeidsplassen gjennom et samtykke. Resultatet er med andre ord at arbeidstaker i de fleste tilfeller må godta at det skjer overvåkning av arbeidsplassen.

Dette er et godt eksempel på at personvernet ikke er absolutt. I GDPR fortalepunkt 4 andre punktum fremgår det at

> *«Retten til vern av personopplysninger er ikke en absolutt rettighet; den må ses i sammenheng med den funksjon den har i samfunnet, og veies mot andre grunnleggende rettigheter i samsvar med forholdsmessighetsprinsippet».*

[94] NOU 1997:19 s. 130-131.
[95] Lov 17.05.2005 nr. 62 § 9-1.

En personvernsrettslig utfordring kan derfor være at arbeidsgiver står for fritt til å iverksette kameraovervåkning på arbeidsplassen med sikkerhetsmessige årsaker som begrunnelse. Overvåkning med sikkerhet som formål vil ha en samfunnsmessig positiv funksjon, og vil antagelig stå sterkere enn den enkelte arbeidstakers personvern i en forholdsmessighetsvurdering. Maktforholdet mellom arbeidsgiver og arbeidstaker synes tydelig i dette tilfellet.

Dersom arbeidsgiver benytter seg av intelligent videoanalyse vil inngrepet i den enkeltes personvern øke ytterligere. At inngrepet i personvernet er større ved bruk av IVA, er fordi arbeidsgiver kan samle inn mer informasjon om sine ansatte enn ved bruk av tradisjonelle kamerasystemer. Resultatet er at arbeidstakers rett til egne opplysninger blir enda mer utvasket overfor arbeidsgivers handlingsrom hva angår kontrolltiltak i virksomheten. I realiteten kan man stille spørsmål om hvor mye av retten til egne opplysninger som gjenstår.

4.4.2 Overblikk

Retten til egne opplysninger vil som illustrert i mange tilfeller reduseres kraftig. På arbeidsplassen vil arbeidsgiver ha stort spillerom for hvilke kontrolltiltak man velger å innføre, gjennom lovreguleringen i arbeidsmiljøloven. Resultatet er at arbeidstaker ikke har noe han skulle sagt, da samtykke er unødvendig. Forutsetningen er selvsagt at arbeidsgiver opptrer i tråd med lovverket.

Utfordringene med retten til egne opplysninger lempes imidlertid noe gjennom GDPR art. 15 hvor det presiseres at den registrerte skal ha rett til vite om virksomheten sitter på informasjon om en selv, samt få innsyn i de aktuelle opplysningene. Det samme gjelder for retten til korrigering i artikkel 16 og retten til å bli slettet etter artikkel 17.

4.5 Formålsbegrensende behandling av personopplysninger

4.5.1 Bakgrunn

Ved behandlingen av personopplysninger vil forordningens prinsipp-bestemmelse stå sentralt. Det er den som legger retningslinjene for hvordan man skal behandle personopplysninger. Prinsippene står nedskrevet i GDPR artikkel 5. Her fremkommer det at behandlingen av personopplysninger skal skje på en «*lovlig, rettferdig og åpen måte med hensyn til den registrerte*».[96]

Først og fremst betyr det at man må ha et klart og definert formål for hvorfor virksomheten samler inn de aktuelle opplysningene.[97] Dette er fordi alle skal kunne forstå hvordan deres personopplysninger vil bli behandlet og hvorfor. Virksomheten kan allikevel benytte seg av innsamlet informasjon til et annet formål enn det som er oppgitt. Dette forutsetter imidlertid at begrunnelsen for den nye behandlingen er forenelig med det originale formålet.[98] Med andre ord må det foreligge en sterk tilknytning mellom hovedformålet og det nye formålet for at behandlingen skal være i tråd med personvernreglene.

4.5.2 Uautorisert bruk?

En utfordring tilknyttet behandlingsformålet vil være hvorvidt formålsbestemmelsen reelt sett blir overholdt. I dagens samfunn stilles det stadig spørsmål om personopplysninger er den nye oljen.[99] Dette er ikke uten grunn. Den teknologiske utviklingen har gjort at personopplysninger har fått en stor kommersiell verdi.[100] Dette er en av hovedgrunnene til at Facebook er en gratis tjeneste; de selger opplysninger om sine forbrukere videre til annonsører.[101] Et godt eksempel på opplysningers kommersielle verdi, er forskningen til psykolog Michal Kosinski. Han har analysert mennesker med utgangspunkt i deres Facebook-aktivitet. Av analysene fant han ut at det skal kun 10 «liker-klikk» til for å kunne si noe mer om et menneske enn hva den alminnelige arbeidskollegaen kan. Videre vil 300 «liker-klikk»

[96] Regulation 2016/679 Art. 5 punkt 1 bokstav a)
[97] Regulation 2016/679 Art. 5 punkt 1 bokstav b)
[98] Regulation 2016/679 Art. 5 punkt 1 bokstav b)
[99] Se bla. Statssekretær Chaffeys innlegg (2018) på www.regjeringen.no
[100] Datatilsynets årsmelding (2016) s. 36
[101] Gundersen (2018)

kunne fortelle mer om dette mennesket enn personens livspartner.[102] Dette er fordi mennesket stort sett trykker «liker» og klikker seg videre på sosiale medier ved impuls.[103] At personopplysninger er blitt en stor kommersiell verdi, er derfor ikke vanskelig å forstå. Men betydningen av dette er at det kan bli lukrativt å misbruke behandlingen av personopplysninger, ved å selge dem videre til tredjeparter.

Muligheten for misbruk vil være særlig relevant for virksomheter som benytter seg av intelligent videoanalyse, da systemene samler inn informasjon som det ellers ville tatt lang tid å logge. Resultatet er at man sitter på store menger opplysninger som kan være av en høy kommersiell verdi.
Dette vil nok blant annet være av stor interesse ved kunderelaterte arbeidsplasser, som butikker. Dersom kameraene fanger opp store deler av butikkområdet, vil butikken sitte på verdifull informasjon om hvor mange kunder som er innom, hvor lenge de står ved de forskjellige seksjonene, om de er stamkunder m.v.[104] Slik informasjon vil for eksempel være av stor interesse for kleskjeden som en helhet.

En av hovedoppgavene til virksomhetens behandlingsansvarlige, er imidlertid å sikre at behandlingen av opplysninger skjer i tråd med de aktuelle formålene.[105] Den behandlingsansvarlige må med andre ord passe på at virksomheten ikke bruker opplysningene fra overvåkningen på en måte som vil stride mot personvernreglementet. Det er derfor grunn til å tro at den behandlingsansvarlige vil fungere som et sikkerhetsnett for misbruk, og at videresalg av opplysninger ikke vil forekomme.

I kjølvannet av at personopplysninger har fått en kommersiell verdi, kan ytterligere et problem oppstå. Dersom virksomheten benytter seg av kameraer med IVA-teknologi, vil virksomheten sitte på enorme mengder med lagrede opplysninger til enhver tid. For hackere vil dette være en gullgruve. I utgangspunktet kan man se for seg at jo mer verdifull informasjon virksomheten samler inn, jo større sjanser er det for at de kan bli hacket. Siden intelligent videoanalyse representerer en økning i hackerens angrepsflate mot virksomheten,

[102] Grassenger og Krogerus (2017)
[103] Datatilsynets og Teknologirådets rapport (2018) s. 11-12
[104] Datatilsynets rapport (2016) s. 14 og 16
[105] Regulation 2016/679 Art. 5 punkt 2 jf. punkt 1

vil bruk av IVA åpne for at det blir lettere å trenge igjennom til virksomhetens informasjon for hackeren.[106]

I tråd med den teknologiske utviklingen er også hacking blitt en mer tilgjengelig mulighet for det gjennomsnittlige mennesket. Et av de mest kjente eksemplene fra senere tid, er lekkasjen fra det amerikanske forvaltningsorganet National Security Agency (NSA) programvare EternalBlue. Dette muliggjorde at «vanlig» hackere som innehar et relativt grunnleggende kunnskapsnivå om hacking, kunne benytte seg av programvare som var utviklet av USAs beste IT-menn på sikkerhets-software.[107] Resultatet er følgelig at flere kan utføre mer avansert hacking. Faren for å bli utsatt for et angrep antas å stige tilsvarende. På den annen side jobbes det hele tiden med å tette åpningene for hacking i systemene, slik at teknologien ikke bare tilgjengeliggjør hacking for allmennheten, men også forsøker å hindre angrep i økt grad.

4.5.3 Sammenfatning

Dersom virksomheten ønsker å benytte seg av intelligent videoanalyse uten å øke faren for hacking-angrep, finnes det imidlertid en løsning. Man kan benytte seg av lokal lagring. Dersom datamaskinen som styrer programmet og lagrer informasjonen aldri har vært tilknyttet et nettverk, vil ikke hackeren kunne komme inn på maskinen, med mindre man befinner seg i samme rom som maskinen og får fysisk tilgang.[108] Det kan derfor være fordelaktig for virksomheten å ha en datamaskin som kun tar hånd om overvåkningen, for å sikre seg best mulig.

Hva angår uautorisert bruk av overvåkningsdataene, finnes det imidlertid ikke en like enkel løsning. Her må det likevel antas at den behandlingsansvarlige utfører en god jobb og sikrer at virksomheten overholder de formålene som er satt for behandlingen.

[106] Se til det blant annet artikkelen til Schneier (2017) som tar for seg uttrykket «Internet of Things»
[107] Newman (2018)
[108] Guta (2017)

4.6 Gjennomsiktig bruk av personopplysninger

4.6.1 Rettslig utgangspunkt

Som nevnt i punkt 4.5.1, krever personvernforordningen at behandling av personopplysninger skjer ved åpenhet jf. art. 5 punkt 1 bokstav a). Dette omtales også i GDPR Fortalepunkt 39. Videre er det et krav etter pol. § 40 at det foretas skilting, eller tilsvarende, for å gjøre personer oppmerksomme på at det forekommer overvåkning av området. Skiltingen må videre opplyse om hvem som er behandlingsansvarlig av opptakene samt om de inkluderer lydopptak. Disse reglene ser ut til å bli videreført i utkastet om bestemmelser om kameraovervåkning på arbeidsplassen § 3.[109] Det antas derfor at disse blir tatt med i en eventuelt forskrift tilknyttet arbeidsmiljøloven.[110]

I veilederen om kameraovervåkning mener Datatilsynet at en varslingsplikt etter pol. § 40 er nødvendig for at «*informasjonen skal nå frem til alle som blir berørt, og for at overvåkingen skal kunne virke forebyggende*». I dette ligger det derfor også et krav om at skiltene må være av en viss størrelse og være plassert slik at de er godt synlige. I den sammenheng er det naturlig at skiltingen også opplyser om hvilke områder som overvåkes på virksomheten. En konkretisering av hvilke områder som overvåkes kan være nødvendig da dette ikke alltid er like åpenbart.[111]

4.6.2 Økt opplysningskrav ved bruk av IVA?

De nevnte krav bør være relativt oppnåelige ved bruk av tradisjonell kameraovervåkning. Per i dag er dette fortsatt den formen for overvåkning som vi forventer at virksomheten bruker. Grunnen er at dette fortsatt anses som normalen. Vi kan derfor enkelt forutse hvordan våre personopplysninger vil bli behandlet gjennom skilting, men også gjennom år med kjennskap til denne typen overvåkning i praksis.

Situasjonen stiller seg imidlertid noe annerledes ved bruk av intelligent videoanalyse. Siden denne formen for overvåkning er relativt ny, vil man sjeldnere forvente at dette er tatt i bruk. Som en forlengelse av dette, vil det videre være mindre forutberegnelig for den enkelte

[109] Høringsnotat 6 juli 2017 Snr. 17/4200 s. 133
[110] Prop. 56 LS (2017-2018) s. 177 punkt 31.3.3.3
[111] Datatilsynets veileder (2016) s. 19

hvilken informasjon som faktisk behandles og lagres. Dette er fordi intelligent videoanalyse i utgangspunktet kan lagre alle former for detaljer i bildet. Informasjonen som hentes inn antas imidlertid å bli begrenset gjennom virksomhetens formål med overvåkningen. Et spørsmål er således om det kan være relevant å opplyse om formålet for overvåkningen på skiltene. Dette vil gjøre det enklere for den enkelte å forutse hvilke opplysninger som vil bli behandlet.

Et påfølgende spørsmål vil i så fall bli om skilting av formålet vil oppfylle kravene til åpenhet etter personvernsreglementet. Til illustrasjon tenker vi oss at en virksomhet benytter seg av overvåkning med IVA, hvor formålet er å ivareta sikkerheten på arbeidsplassen. I hvilken grad vil dette formålet kunne begrense innhentingen av opplysninger? Av sikkerhetsmessige grunner vil det være relevant å samle inn flest mulig detaljer, slik at mulighetene for å oppklare en situasjon vil være størst mulig. Realiteten er med andre ord at formålet ikke begrenser innhentingen og behandlingen av opplysninger i særlig grad.

Det synes videre å være en dårlig løsning å måtte opplyse om enhver form for innhenting av informasjon på skiltene. Resultatet ville blitt en lang oppramsing av persondetaljer. For at en slik oppramsing skulle vært hensiktsmessig å foreta, måtte den videre ha vært uttømmende. Er den ikke det, vil man fortsatt være usikre på hva som reelt blir behandlet. Men på den andre siden vil det være risikofylt for virksomheten å operere med en uttømmende liste, da det kan være enkelt å glemme en enkelt detalj. Videre vil dette kunne bli dyrt dersom man endrer formålet, eller utvider/innskrenker databehandlingen, da dette vil kreve innkjøp av nye skilt.

Datatilsynet virker imidlertid til å ha funnet en løsning. Overvåkning på virksomhetens områder innebærer at det stort sett er de samme menneskene som blir fanget opp på kameraene. Det er derfor enkelt å finne ut hvilke personer som blir særlig berørt av overvåkningen. Disse menneskene kan derfor få tildelt mer utfyllende informasjon om hvordan kameraovervåkningen fungerer på den enkelte arbeidsplass. Eksempelvis vil et informasjonsskriv være en relevant løsning.[112]

4.6.3 Sammenfatning

Personvernrettslig ser man at intelligent videoanalyse kan utfordre kravet om åpenhet etter GDPR, hva angår bruk av denne formen for overvåkning sett i sammenheng med skilting på

[112] Datatilsynets veileder (2016) s. 19

virksomheten. I lys av Datatilsynets løsningsforslag om nærmere opplysninger til de særlig berørte, virker det likevel ikke til å være behov for å øke opplysningskravet ved skilting av kameraovervåkning, selv ved bruk av intelligent videoanalyse. En mulig mellomløsning kan imidlertid være å kreve at det opplyses om bruk av IVA på skiltingen, i de tilfeller dette er tatt i bruk. Dette forutsetter imidlertid at alle faktisk er innforstått med hva IVA betyr og innebærer.

4.7 Prinsippet om «dataminimering»

4.7.1 Hva «dataminimering» innebærer

Prinsippet om dataminimering innebærer at behandlingen av personopplysninger skal begrenses til å kun omfatte det som er nødvendig for at formålene de behandles etter oppfylles. Behandlingen skal videre være adekvat og relevant. Dette står hjemlet i forordningen artikkel 5 bokstav c, og er en regel som er særlig relevant for kameraovervåkningen på arbeidsplassen.

I ordet «nødvendig» ligger det en begrensning som innebærer at arbeidsgiver ikke har lov til å fange opp mer informasjon med kameraet enn det som det er behov for, for å sikre at formålet med overvåkningen ivaretas. Datatilsynet og Personvernnemnda har i den anledning behandlet flere saker. I en klagesak innsendt fra en ansatt ved GullAdam i Tromsø, presiserer Datatilsynet blant annet at det skal mer til for å overvåke områder av arbeidsplassen der arbeidstaker oppholder seg primært i løpet av dagen. Med dette som utgangspunkt fant Datatilsynet at det ikke var grunnlag for overvåkning av butikkområde som kun var tilgjengelig for de ansatte.[113] Dette var med andre ord ikke «nødvendig» for å hindre eller oppklare tilfeller av tyveri og ran i GullAdam. Personvernnemnda fant derimot Datatilsynets avgjørelse for streng, og mente at det i denne saken forelå «særskilt behov» etter pol. § 38 for å opprettholde kameraovervåkningen.[114]

Et annet tilfelle hvor Datatilsynet har ønsket å innsnevre kameraovervåkningen til det nødvendige, er klagen vedrørende overvåkning på Bakehuset Kafé AS.[115] Her hadde kaféen,

[113] PVN-2013-3 punkt 5 sammenhold med klagens innledende sammendrag
[114] PVN-2013-3 punkt 6 og 7
[115] Klagesak 09/2004

etter samtale med Datatilsynet, satt opp tre kameraer ved kassen med formål om å avdekke svinn og underslag fra de ansatte. Da problemet ikke forsvant, valgte kaféen å montere ytterligere to kameraer i lokalet. Disse ble festet slik at kameraene fanget opp veien fra kassen til tellerommet. Formålet var å avdekke om det forekom underslag på strekningen. Personvernnemnda sluttet seg til Datatilsynets vedtak. Begge klageorgan anså grensen for tillatt kameraovervåkning som overtrådt i det aktuelle tilfellet.[116]

4.7.2 Krav om bruk av minste inngripende tiltak

En personvernsrettslig utfordring med utspring i dataminimeringsprinsippet, er at det kan være vanskelig å vite hva kameraene reelt får med seg. Arbeidsgiver plikter å stille inn kameraene slik at de ikke får tilgang til mer informasjon enn det formålet tilsier. Men hvordan kan man som ansatt vite om arbeidsgiver overholder dette?
En butikkansatt som store deler av dagen står i kassen, vil formodentlig ha fått beskjed om at det foretas overvåkning av kasseområdet med formål om å forebygge ran ol. Men i hvor stor grad vil kameraene også registrere den ansattes handlinger bak kassen?

I klagesaken om GullAdam uttaler Datatilsynet at det kan oppleves som et betydelig inngrep i arbeidstakers personvern dersom man blir overvåket kontinuerlig i løpet av arbeidsdagen. Dette gjelder uavhengig av om formålet med overvåkningen er rettet mot de ansatte eller ikke. Personvernmessig vil det med andre ord føles like inngripende å bli overvåket selv om formålet med overvåkningen er begrunnet i hensynet til sikkerhet. Dette er fordi man vil ha et behov for frihet på arbeidsplassen, selv om man står til disposisjon hos arbeidsgiver.[117]

I lys av GullAdam-saken kan man se at prinsippet om dataminimering er særlig relevant for personer som jobber i butikk. Dersom arbeidsgiver overvåker store deler av arealet i butikken, er det naturlig at også den ansattes handlinger blir hyppig registrert av kameraene. Det sentrale vil derfor være å minimere bruken av overvåkning i størst mulig grad. Holder det å overvåke inngangspartiet, bør man unngå overvåkning i resten av butikken.

Dersom arbeidsgiver likevel har behov for å overvåke hele eller store deler av lokalet, finnes det imidlertid flere tiltak som kan redusere inngrepet i personvernet. I kravet om «nødvendig» behandling av personopplysninger ligger det en forutsetning om at man skal velge det tiltaket

[116] PVN-2004-9
[117] PVN-2013-3 punkt 5

som vil være minst inngripende. Det er derfor viktig at arbeidsgiver tar stilling til disse tiltakene ved vurderingen av kameraovervåkning på arbeidsplassen. Eksempelvis kan det være nok at man har en monitor som viser hva som skjer, slik at det ikke lagres opptak fra overvåkningen. Et annet tiltak kan være å benytte seg av overvåkning som kun registrerer bilde uten at lyden fanges opp. Eller ha tidsstyrt overvåkning, slik at overvåkningen kun er aktiv når det er størst behov.[118]

Skulle arbeidsgiver mot formodning ikke overholde reglene for kameraovervåkning på arbeidsplassen, vil resultatet bli at arbeidstakers personvern blir svekket. Ved bruk av tradisjonell kameraovervåkning vil inngrepet i personvernet knytte seg til faren for misbruk av lagrede opptak. Eksempelvis at arbeidsgiver ser på opptak som er lagret på bakgrunn av sikkerhetsmessige formål, for å vurdere hvordan den ansatte arbeider eller utfører jobben.[119] Har arbeidsgiver i tillegg overvåket større områder enn det som er nødvendig, vil inngrepet i personvernet øke tilsvarende.

Inngrepet i personvernet utfordres ytterligere dersom arbeidsgiver benytter seg av kameraer med intelligent videoanalyse. I tillegg til misbruk av overvåkningen ved tradisjonell kameraovervåkning, vil man ved bruk av IVA sitte med automatisk lagrede data som arbeidsgiver potensielt kan benytte seg fritt av – dog ikke i tråd med regelverket. Resultatet er at arbeidsgiver kan tilegne seg store mengder informasjon om sine ansatte han ikke har rett på.

4.7.3 Oppsummering

Som Datatilsynet nevner i sin rapport fra 2016, er det gode grunner til å anta at bruken av kameraer med intelligent videoanalyse vil øke i tiden fremover. Ikke bare blir teknologien billigere, men en ser også at IVA fører til nye bruksområder som vil være av stor verdi for arbeidsgiver. Spesielt vil dette være aktuelt ved innsamling av kundedata, hvor man kan sitte på tall for når det er stor pågang, hvor lenge man blir stående ved hver seksjon osv.[120]
I lys av dataminimeringsprinsippet kan dette bli svært interessant. Det er viktig at man utvikler gode rutiner for sikring av personvern, samt at det skal være enkelt å begrense hvilken informasjon kameraene med intelligent videoanalyse registrerer.

[118] Datatilsynets veileder (2016) s. 15-16
[119] Datatilsynets veileder (2016) s. 17
[120] Datatilsynets rapport (2016) s. 16

4.8 Menneskelige svakheter i teknologien?

4.8.1 Indirekte diskriminering

I tråd med den teknologiske utviklingen kommer det smarte løsninger som gjør hverdagen enklere og mer effektiv både for arbeidsplassen og privatlivet. Man har for eksempel kommet langt i utviklingen av virtuelle mennesker ved bruk av kunstig intelligens. Dette har de blant annet testet ut i psykiatrien. Det interessante er at mennesket viser seg å åpne seg mer overfor en robot utstyrt med kunstig intelligens, enn en utdannet psykolog. Dette er fordi man slipper følelsen av å bli iakttatt og dømt fra den andre siden av bordet dersom man snakker med en robot som kun analyserer svarene.[121]

At teknologien kan hjelpe mennesker til å være mer åpne i situasjoner man trenger det mest, slik som i psykiatrien, anses som et stort gode og et steg i riktig retning. Men selv om teknologien gir oss muligheter som virtuelle mennesker og automatisk analyserende systemer som IVA, er det viktig å ikke glemme at det befinner seg mennesker som deg og meg bak disse teknologiske fremskrittene.

Teknologien kan bare bli så moralsk og dydig som mennesket bak den er. Dette er et naturlig resultat av at det er personer som utvikler teknologien, og med det bestemmer hvordan systemer og algoritmer skal fungere og reagere basert på den informasjonen den blir sammensatt av.

Problemet med teknologiske hjelpemidler, slik som intelligent videoanalyse, er følgelig at man kan ende opp med utilsiktet diskriminering. Datatilsynet presiserer at siden systemets objektive vurderinger baserer seg på hvilke opplysninger mennesket fôrer det med, er det viktig at systemet også læres opp i hva som anses som relevant informasjon, samt hvilke opplysninger som kan tillegges vekt og ikke, i analysen. Hvis «*treningsdataene gir et skjevt bilde av virkeligheten*» kan analysen fort gi et unyansert eller diskriminerende resultat.[122]

Ved bruk av intelligent videoanalyse kan arbeidsgiver stille inn programmet til å varsle dersom nærmere spesifiserte karakteristikker registreres i bildet. En karakteristikk kan blant annet være kjønn, «*hudfarge, alder, og om bilen personen kjører er dyr eller ikke*».[123] Dersom

[121] Lucas mfl. (2014)
[122] Datatilsynets rapport (2018) s. 15
[123] Datatilsynets rapport (2016) s. 16

varslingen medfører en form for diskriminering, vil den ikke være i samsvar med prinsippet om rettferdighet.[124] Det er derfor klart at denne typen bruk av systemet anses som et brudd på personvernreglementet.

På den andre siden er det nettopp registreringen av personers karakteristikker som muliggjør hurtigsøking i lagrede opptak. Karakteristikkene gjør at arbeidsgiver, som nevnt i punkt 4.2.2, kun ser de delene av opptaket som er i samsvar med det aktuelle søket. Siden denne funksjonen ivaretar den enkeltes personvern i større grad enn tradisjonell kameraovervåkning, er det viktig at man kan lagre opplysninger om den enkeltes karakteristikker. Mye kan derfor tale for at det er selve varslings-innstillingene som vil være i strid med reglene, forutsatt at systemet kun behandler de karakteristikkene som er lovlig.

At diskriminering kan forekomme ved misbruk av intelligent videoanalyse, setter den enkelte i en sårbar posisjon. I mange tilfeller vil analysene foregå i det skjulte, og det vil derfor være svært vanskelig å oppdage diskrimineringen. Dette er også en naturlig følge av at det er uvisst hvilke opplysninger som blir samlet inn til behandling.[125]

4.8.2 Sammenfatning

Det er enkelt å tenke at teknologien er 100% objektiv, og dermed mer stabil enn hva mennesket er. Men det som er forsøkt belyst her, er at teknologien baserer seg på samfunnets oppfatninger og holdninger. Teknologien bygger på menneskelig intuisjon og forutsetninger. Og faktum er at det finnes intet menneske uten fordommer, dette til tross for at vi ikke føler oss fordomsfulle. Og det finnes intet menneske som er 100% objektiv.

Systemutviklerne har et stort ansvar for å hindre at teknologien muliggjør diskriminerende analyser. I den anledning må de tilpasse systemene slik at brukerne av de teknologiske produktene i minst mulig grad kan stille inn systemet på en måte som kan resultere i diskriminering. Imidlertid kan det diskuteres hvorvidt brukerens etiske valg skal begrenses og reguleres av systemutviklerne. Dette er en problemstilling som vil fortsette å være svært aktuell i tråd med den teknologiske utviklingen, da man i større grad baserer seg på maskinlæring ol. Det er derfor viktig å gjøre seg kjent med hva som skal til for å hindre at

[124] Regulation 2016/679 Art. 5 punkt 1. Bokstav a)
[125] Datatilsynets årsmelding (2016) s. 36

dette problemet øker i fremtiden.

4.9 Innebygd personvern som europeisk standard

4.9.1 Rettslig grunnlag

Etter GDPR artikkel 25 oppstilles det et krav om «*innebygd personvern og personvern som standardinnstilling*». At personvernet skal være «innebygd» tilsier at ethvert ledd i utviklingen av nye tekniske fremstillinger skal ha fokus på personvern. Dette er fordi personopplysninger skal vernes, ikke bare ved bruken av produktene, men også under utviklingen av produktet. En standardinnstilling om innebygd personvern skal med andre ord sikre at informasjonssystemene som virksomhetene benytter seg av, oppfyller personvernreglementets prinsipper og at de registrertes rettigheter blir tilstrekkelig ivaretatt.[126]

4.9.2 Utfasing av eldre teknologi

I årsmeldingen for 2017 peker Datatilsynet på en sentral personvernrettslig utfordring knyttet til innebygd personvern. Problemet kan deles inn i to. For det første vil gamle systemer mangle innebygd personvern. Dette er systemer som har vært installert for mange år tilbake, og som antagelig ikke har vært i samsvar med personverndirektivet heller. For det andre har det vist seg at flere miljøer synes å være konservative, hva angår tilbøyeligheten til utskiftning av gamle systemer.[127]

Ut i fra denne informasjonen er det derfor grunn til å tro at mange virksomheter vil fortsette å benytte seg av utdaterte systemer også etter forordningen trer i kraft. Sett opp mot kravet om innebygd personvern i GDPR art. 25, vil disse systemene innebære en enda større trussel for inngrep i den enkeltes personvern enn det ny teknologi vil, til tross for dets økte bruksområde. Dette er fordi ny teknologi i stor grad antas å oppfylle de rettslige kravene, slik at det i utgangspunktet må skje en form for misbruk av teknologien før personvernet blir truet. Dette vil ikke gjelde ved bruk av gammel teknologi, da denne aldri har vært i samsvar med gjeldende lovverk uavhengig av dets bruk.

[126] Datatilsynets veileder (2017) s. 5
[127] Datatilsynets årsmelding (2017) s. 29

På den annen side er det blitt billigere å benytte IVA i dag.[128] Det vil derfor være rimelig å anta at de fleste virksomheter som kan få bruk for denne typen kameraovervåkning vil gå til innkjøp av dette i nærmeste fremtid. Med andre ord vil det gradvis sikres at flere og flere virksomheter er i samsvar med personvernreglene. En forutsetning er imidlertid at programutviklerne er raske til å tilby teknologi som samsvarer med kravet om innebygd personvern på markedet.

4.9.3 Oppsummering

At virksomheten behandler opplysninger i tråd med personvernsreglementet tilkommer den behandlingsansvarlige å sikre.[129] Dersom virksomheten ikke opererer i samsvar med forordningen kan de bli ilagt et overtredelsesgebyr på inntil 20 millioner euro, eller 4% av årsomsetningen dersom overtreder er et foretak.[130] Det bør utgjøre et incentiv til å oppgradere overvåkningssystemet i virksomheten. Alt i alt vil dette trolig bli en billigere kostnad enn et overtredelsesgebyr. Datatilsynet synes videre å forutsette at de behandlingsansvarlige skal iverksette en fremdriftsplan på hvordan virksomheten skal oppdatere systemene som ikke er i tråd med forordningen. Dette skal sikre at personvernet blir ivaretatt på en tilstrekkelig måte.[131] Det er derfor viktig at den enkelte virksomhet får en oversikt over hvilke systemer som ikke er i tråd med forordningen per i dag, og hva som skal til for å sikre et tilfredsstillende personvern i nærmeste fremtid.

4.10 Slettefrister for datalagring

4.10.1 Bakgrunn

Etter GDPR art. 5 fremkommer det at opplysninger ikke skal lagres lenger «*enn det som er nødvendig for formålene som personopplysningene behandles for*» jf. bokstav e. Etter ordlyden å dømme synes slettefristen derfor å være relativ. Dersom opplysningene er uriktige i lys av formålet skal de slettes uten opphold, jf. bokstav d. Videre fremgår det av artikkel 17 at personer som er blitt registrert, har rett til å få opplysningene om seg selv slettet «uten

[128] Datatilsynets rapport (2016) s. 14
[129] Regulation 2016/679 Art. 25 punkt 2 jf. Art. 4 punkt 7.
[130] Regulation 2016/679 Art. 83 punkt 5
[131] Datatilsynets årsmelding (2017) s. 29

ugrunnet opphold». Den behandlingsansvarlige skal videre slette opplysninger om en person dersom de blant annet ikke er nødvendige lenger, er blitt behandlet ulovlig eller samtykket er tilbaketrukket, jf. art. 17 punkt 1, bokstav a – f.

Et unntak fra slettefristen er at virksomheten kan sitte på opplysninger av et statistisk formål, jf. GDPR art. 5 bokstav e. Forutsetningen er at de lagrede opplysningene er blitt avidentifisert og derfor ikke lenger kan identifisere et enkelt menneske.

Hva angår slettefrister for kameraovervåkning, ønsker Departementet å fastsette en frist på tre måneder ved virksomheter som faller innunder ordlyden «*utsalgssted som benytter betalingskort*». Dette er fordi det ofte vil ta lenger tid enn én uke før man oppdager misbruk. Departementet presiserer imidlertid at slettefristen på tre måneder kun anses som en absolutt frist for sletting, slik at virksomheten fritt kan slette opptak før det er gått tre måneder.[132]

4.10.2 Overholdes fristene?

Et spørsmål i tilknytning til slettefristene er imidlertid hvorvidt man kan stole på at informasjonen om seg selv blir slettet. Ser man slettefristen i lys av forordningen, er det vanskelig å anslå hvor lenge virksomheten blir sittende med informasjonen.

Den enkelte person kan imidlertid føre en viss kontroll med hvilke opplysninger virksomheten sitter på om seg selv. Etter GDPR art. 15 har den registrerte rett til innsyn i hvilke personopplysninger virksomheten har lagret. I forlengelsen av dette har man også rett til å vite hvilke formål som ligger til grunn for behandlingen, hvor opplysningene er eller vil bli utlevert, samt hvor lenge det er forventet at virksomheten har opplysningene lagret, jf. art. 15 bokstav a – h.

4.10.3 Sammenfatning

Dette er et personvernsrettslig problem som vil tre frem i større grad ved bruk av intelligent videoanalyse i forhold til tradisjonell kameraovervåkning. Det er fordi kameraer med IVA automatisk samler inn mer informasjon om den enkelte enn hva et vanlig kameraopptak gjør. Potensialet for at virksomheten blir sittende på mer informasjon om sine arbeidstakere er følgelig større ved bruk av IVA. At slettefristen utvides fra en uke til tre måneder for

[132] Prop. 56 LS (2017-2018) s. 178

utsalgssteder som benytter seg av betalingskort, er videre med på å øke virksomhetens informasjonslager.

5 Avsluttende bemerkninger

Etter å ha sett nærmere på personvernsrettslige utfordringer som oppstår, eller kan oppstå, ved bruk av kameraovervåkning på arbeidsplassen, er det flere problemer som kan være høyst aktuelle utfordringer i forhold til regelverket. Videre har gjennomgangen ovenfor vist at de personvernrettslige utfordringene blir større dersom virksomheten benytter seg av intelligent videoanalyse. Dette så man spesielt ved vurderingen av kravet om skilting av overvåkning på virksomheten, og hvorvidt det er behov for å øke informasjonskravet ved bruk av IVA.

En problemstilling som i særlig grad belyser utfordringene ved bruk av intelligent videoanalyse, sammenlignet med tradisjonell kameraovervåkning, er forholdet til menneskelige svakheter i forbindelse med den teknologiske utviklingen. For eksempel vil spørsmålet om teknologisk diskriminering i mindre grad være aktuelt ved tradisjonell kameraovervåkning, da dette ikke er systemer som skal læres opp til annet enn å observere.

I realiteten vil det kun være i forbindelse med kravet om innebygd personvern tradisjonell kameraovervåkning anses som en større utfordring enn IVA, i forhold til personvernet til den enkelte arbeidstaker. Utfordringen antas imidlertid å bli stadig mindre jo lenger tid som går og oppdateringer av virksomhetens systemer finner sted.

Ved fokus på kameraovervåkning på arbeidsplassen ved bruk av intelligent videoanalyse, blir det tydelig hvordan ny teknologi vil påvirke arbeidsplassen i tiden fremover, og hvilke utfordringer man kan støte på personvernrettslig. Dette er likevel kun en liten del av kontrolltiltakene arbeidsgiver kan benytte seg av, samt en liten del av teknologien som befinner seg på arbeidsplassen. De personvernsrettslige utfordringene antas derfor å være mange flere, spredt over flere teknologiske flater i virksomheten.

I tiden fremover vil ytterligere ny teknologi bli presentert. Og i tråd med dette, nye personvernsrettslige utfordringer. Det blir interessant å se hvordan GDPR vil håndtere fremtidens nyutviklinger. Ikke minst blir det interessant å se hvordan resten av verden blir påvirket av Europas strengere regler om vern av den enkeltes personopplysninger. Vi ser konturene av denne utviklingen allerede i dag.[133]

[133] Siden forordningens geografiske virkeområdet omfavner all behandling av Unionens personopplysninger, uavhengig av hvor behandlingen skjer, forventes påvirkningen å øke ytterligere, jf. GDPR art. 3.

6 Litteraturliste

6.1 Norske rettskilder

6.1.1 Lover

Aml. (2005)	Lov 17. juni 2005 nr. 62 om arbeidsmiljø, arbeidstid og stillingsvern mv. (Arbeidsmiljøloven)
Arbtvl. (2012)	Lov 27. januar 2012 nr. 9 om arbeidstvister (arbeidstvisteloven)
EØS (1992)	Lov 27. November 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven)
Popplyl. (2000)	Lov 14. april 2000 nr. 31 om behandling av personopplysninger (Personopplysningsloven)
Mrl. (1999)	Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (Menneskerettighetsloven)
Grl. (1814)	Lov 17. mai 1814 Kongeriket Norges Grunnlov

6.1.2 Forarbeider

NOU-2009-1	Personvernkommisjonen. «Individ og integritet – Personvern i det digitale samfunnet»
NOU-2004-5	Arbeidslivslovutvalget. Et arbeidsliv for trygghet, inkludering og vekst
NOU-1997-19	Et bedre personvern. Forslag til lov om behandling av personopplysninger
Ot.prp.nr 49 (2004-2005)	Om lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven)
Ot.prp.nr 92 (1998-1999)	Om lov om endringer i lov aav 4 februar 1977 om arbeidervern og arbeidsmiljø m.v.

Prop. 56 LS (2017-2018)	Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en belsutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personovernforordning) i EØS-avtalen.
Prop. 47 L (2011-2012)	Endringer i personopplysningsloven, 16 desember 2011
Dok.nr.16 (2011-2012)	Rapport fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven

6.1.3 Rettspraksis

HR-2016-2286-A	«Rygge kommune»
HR-2016-1366-A	«Avlaster II»
Rt. 2009 s. 1465	«Senvakt»
Rt. 2008 s. 856	«Theatercafé»
Rt. 2001 s. 688	«Tippekassekjennelsen»
Rt. 2000 s. 1602	«Nøkk»
Rt. 1991 s. 616	«Gatekjøkkenkjennelsen»
Rt. 1986 s. 1322	«Norsk stålpress»
Rt. 1977 s. 902	«Hammerverk»
Rt. 1952 s. 1217	«To mistenkelige personer»
ARD 1922 s. 86	

6.1.4 Forvaltningspraksis

PVN-2013-3	«GullAdam»
PVN-2004-9	«Bakehuset Kafè AS»
Klagesak 09/2004	«Bakehuset Kafè AS»

6.1.5 Juridisk litteratur

Aall (2015)	Aall, Jørgen. (2015) *Rettsstat og menneskerettigheter*. 4. utgave, Bergen: Fagbokforlaget
Evju (2010)	Evju, Stein. (2010) *Arbeidsrett: utvalgte artikler 2001-2010.* Oslo: Universitetsforlaget
Kjølaas (2010)	Kjølaas, Christian. (2010) *Personvern i arbeidsforhold*. 1. utgave, Oslo: Universitetsforlaget
Lomell (2010)	Lomell, H. M. (2010) Videoovervåkning – myter og realiteter. I: Schartum, D. W. red. *Overvåkning i en rettsstat*, Bergen: Fagbokforlaget Vigmonstad & Bjørke AS, s. 243 - 261
Schartum og Bygrave (2016)	Schartum, D.W., og Bygrave, L.A. (2016) *Personvern i informasjonssamfunnet.* 3. utgave, Bergen: Fagbokforlaget
Schartum (2010)	Schartum, D. W. (2010) Overvåkning i en rettsstat. I: Schartum, D. W. red. *Overvåkning i en rettsstat*, Bergen: Fagbokforlaget Vigmonstad & Bjørke AS, s. 17 - 36
Skjønberg mfl. (2017)	Skjønberg, A. N., Hognestad, E. og Hotvedt, M.J. (2017) *Individuell arbeidsrett.* 2. utgave, Oslo: Gyldendal Juridisk
Svendsen (2010)	Svendsen, L.F.H., (2010) Hvorfor personvern? Om frihet og retten til privatliv. I: Clemet, K. og Egeland J.O. (red.), *Til forsvar for personvernet*. Oslo: Universitetsforlaget

6.2 Internasjonale rettskilder

6.2.1 Internasjonale regler

Regulation 2016/679	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) (Personvernforordningen)
Direktiv 95/46/EF	Europaparlamentets og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse md behandling av personopplysninger og om fri utveksling av slike opplysninger (Personverndirektivet)

EMK	Den europeiske menneskerettighetskonvensjon, vedtatt av Europarådet 4. november 1950

6.2.2 Artikkel 29-gruppen

Artikkel 29-gruppen (2017)	Article 29 Data Protection Working Party, «Opinion 2/2017 on data processing at work", WP 249, 8 June 2017
Artikkel 29-gruppen (2007)	Article 29 Data Protection Working Party, «Opinion 4/2007 on the concept of personal data" WP 136, 20th June 2007

6.3 Andre kilder

6.3.1 Rapporter, veiledere ol.

Datatilsynets rapport (2018)	Datatilsynets rapport *«Kunstig intelligens og personvern»*, Oslo, Januar 2018
Datatilsynet og Teknologirådets rapport (2018)	Datatilsynet og Teknologirådet, «*Personvern 2018 Tillitt og følelser»*, Oslo, Januar 2018
Datatilsynets veileder (2017)	Datatilsynets veileder, *«Vurdering av personvernkonsekvenser etter nytt regelverk»*, Juni 2017
Datatilsynets årsmelding (2017)	Datatilsynets årsmelding, «*Årsmelding for 2017. Hva preget året som gikk på personvernfeltet, og hvilke utfordringer ser Datatilsynet fremover?»*, Oslo, Mars 2018
Datatilsynets rapport (2016)	Datatilsynets rapport, «*Sporing i det offentlige rom. Bruk av WiFi, Bluetooth, nettvarder (beacons) og intelligent videoanalyse*», September 2016
Datatilsynets veileder (2016)	Datatilsynets veileder, «*Kameraovervåkning – hva er lov?»*, April 2016
Datatilsynets årsmelding (2016)	Datatilsynets årsmelding, «*Årsmelding for 2016. Hva skjer på personvernfeltet, og hvilke utfordringer ser vi fremover?»*, Oslo, Mars 2017

Deloitte personvernundersøkelse (2017) Deloittes personvernundersøkelse 2017 «*Styrket personvern, svekkede bedrifter?*» Februar 2017

Regjeringens høringsnotat Snr. 17/4200 Høringsnortat 6. juli 2017 Snr. 17/4200 «Ny personopplysningslov – Gjennomføring av personvernforordningen i norsk rett».

6.3.2 Nettsider

Apple.no — Apple sin hjemmeside med spesifikasjoner på iPhone X. https://www.apple.com/no/iphone-x/specs/ (sist besøkt 29.05.2018)

Aquabyte.no — Aquabytes hjemmeside med informasjon om hva de gjør. https://www.aquabyte.no/ (sist besøkt 29.05.2018)

Datatilsynet.no — Datatilsynets artikkel «*Søkemotorers plikter – Artikkel 29-gruppen*». Publisert 12. juni 2008. https://www.datatilsynet.no/regelverk-og-skjema/lover-og-regler/uttalelser-fra-artikkel-29-gruppen/artikkel-29-gruppen-sokemotorers-plikter/ (Sist besøkt 29.05.2018)

Eugdpr.org — Informasjonsportal over GDPR-reglementet. https://www.eugdpr.org/ (sist besøkt 29.05.2018)

Justis- og beredskapsdepartementet (2018) Justis og beredskapsdepartementets nyhet «*Når får vi ny personopplysningslov?*» Publisert 26. april 2018. https://www.regjeringen.no/no/aktuelt/nar-far-vi-ny-personopplysningslov/id2599511/ (sist besøkt 29.05.2018)

Regjeringen.no — Regjerningens pressemelding 6. juli 2017, «Ny lov om behandling av personopplysninger på høring». https://www.regjeringen.no/no/aktuelt/ny-lov-om-behandling-av-personopplysninger-pa-horing/id2564315/ (sist besøkt 29.05.2018)

6.3.3 Diverse

Chaffey (2018) — Chaffey, P. (2018) *En ny gullstandard for personvern* [Internett] Regjeringen.no. Tilgjengelig fra: https://www.regjeringen.no/no/aktuelt/en-ny-gullstandard-for-personvern/id2598120/ (sist besøkt 29.05.2018)

Dagens Næringsliv NTB, «*Amazon åpner kasseløs matbutikk*». Publisert 22. januar 2018. Tilgjengelig fra Dagens Næringsliv: https://www.dn.no/nyheter/2018/01/22/0553/Teknologi/amazon-apner-kasselos-matbutikk (sist besøkt 29.05.2018)

Datatilsynets punktliste Datatilsynets punktliste «*Nye personvernregler fra 2018, Hva betyr det for din virksomhet?*» Datatilsynet.no. Tilgjengelig fra: www.datatilsynet.no/globalassets/global/regelverk-skjema/forordningen/punktliste-til-ny-forordning_web.pdf (sist besøkt 29.05.2018)

Grassenger og Krogerus (2017) Grassenger, H. og Krogerus, M. (2017) *Dataene som snudde verden på hodet* [Internett]. NRKbeta. Tilgjengelig fra: https://nrkbeta.no/2017/02/04/dataene-som-snudde-verden-pa-hodet/ (Sist besøkt 29.05.2018)

Gundersen (2018) Gundersen, M. (2018) *Overvåkningsmaskinen Facebook* [Internett]. NRKbeta. Tilgjengelig fra: https://nrkbeta.no/2018/03/24/overvakningsmaskinen-facebook/ (Sist besøkt 29.05.2018)

Guta (2017) Guta, Michael (2017) *Can a Computer Be Hacked If It's Not Connected to the internet?* [Internett]. 23. Mars. Small Business trends. Tilgjengelig fra: https://smallbiztrends.com/2017/03/can-an-offline-computer-be-hacked.html (Sist besøkt 29.05.2018)

Lucas m.fl. (2014) Lucas, G. M., Gratch J., King, A., Morency, L-P. (2014) It's only a computer: Virtual humans increase willingness to disclose. *Computers in Human Behavior* [Internett], nummer 37 (2014), s. 94 - 100. Tilgjengelig fra: https://ac.els-cdn.com/S0747563214002647/1-s2.0-S0747563214002647-main.pdf?_tid=a0d189e3-c35e-4cad-b695-2edd889016a2&acdnat=1524853623_45af08698d391e2804c97c61a15eb157 (sist besøkt 29.05.2018)

Newman (2018) Newman, L. H. (2018), The leaked NSA spy tool that hacked the world. *Wired Magazine* [Internett] 7. Mars. Tilgjengelig fra: https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/ (Sist besøkt 29.05.2018)

Orwell, G. (2016) *1984*. Penguin Books Ltd.
Først publisert 1949, London: Secker & Warburg

Plikk (2018) Plikk, N. (2018). *Facebook-krisen forklart* [Internett]. Tek.no. Tilgjengelig fra: https://www.tek.no/artikler/facebook-krisen-forklart/433196 (Sist besøkt 29.05.2018)

Schneier (2017) Schneier, B. (2017), Click Here to Kill Everyone. *New York Magazine* [Internett] 27. januar. Tilgjengelig fra: http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html (sist besøkt 29.05.18)

Sporveien sitt høringssvar til Høringsnotat 6. juli 2017. Tilgjengelig fra: https://www.regjeringen.no/contentassets/680f4798492a4f13bffa226a8f6fda0a/sporveien.pdf?uid=Sporveien (sist besøkt 29.05.2018)