Arbeidsgivers adgang til å kontrollere og overvåke sine ansatte

Med hovedvekt på grunnvilkårene for behandling av personopplysninger i arbeidslivet

Veileder: Gjermund Mathisen (JD)

Leveringsfrist: 10.11.2003

Til sammen 39826 ord

14. oktober 2003

Innholdsfortegnelse

1 Innledning

1.1 Problemstilling og avgrensning

Siktemålet med denne avhandlingen er å redegjøre for private arbeidsgiveres rettslige adgang til å kontrollere og overvåke sine ansatte på arbeidsplassen.[1] Avhandlingen er i hovedsak knyttet opp mot *lov om behandling av personopplysninger* av 14. april 2000 nr. 31 (personopplysningsloven, popplyl.) og de ulovfestede arbeidsrettslige reglene som gjør seg gjeldende på dette området. Temaet relaterer seg til forholdet mellom partene i arbeidslivet og deres rettigheter og plikter overfor hverandre. De rettslige spørsmålene som oppstår har derfor forankring i arbeidsretten. Kontroll- og overvåkingstiltak bringer imidlertid på banen en rekke personvernrettslige problemstillinger, og det personvernrettslige regelverket fungerer derfor side om side med arbeidsretten på dette området.[2] Forholdet mellom regelverkene vil derfor stå sentralt i denne avhandlingen.

Avhandlingen består av en redegjørelse for de rettslige grunnlagene for behandling av personopplysninger i arbeidslivet. De rettslige grunnlagene finnes dels i det ulovfestede arbeidsrettslige regelverket, og dels i popplyl. § 8.[3] Videre blir det redegjort for

---

[1] Begrepet "kontroll" har i teorien vært tillagt et noe annet innhold enn begrepet "overvåking". Jeg er av den oppfatning at begrepene går over i hverandre på en slik måte at det ikke er hensiktsmessig å operere med noe aktivt skille i denne avhandlingen. "Kontrolltiltak" vil i de fleste sammenhenger bli brukt som en samlebetegnelse.

[2] Begrepene "personvern", "personvernhensyn" mv. vil bli brukt i forholdsvis stor grad. Det kan derfor være hensiktsmessig å beskrive kort hva begrepet "personvern" omfatter. Begrepet er i NOU 1997: 19 på side 21 (punkt 3.3.1) omtalt på følgende måte: *"På et helt generelt plan kan personvernet sies å gjelde krav til behandling av personopplysninger når kravene er begrunnet ut i fra visse ideelle (ikke-økonomiske) interesser som en tillegger fysiske (og eventuelt juridiske) personer"*.

[3] I popplyl. § 9 oppstilles en rekke tilleggskrav for behandling av såkalte *sensitive personopplysninger*. Denne typen personopplysninger vil ikke bli behandlet særskilt her, da det normalt er snakk om

begrensningene i kontrolladgangen. Disse følger blant annet av grunnkravene for behandling av personopplysninger i popplyl. § 11, ulovfestede arbeidsrettslige prinsipper, arbeidsmiljøloven og arbeidsavtalen.[4] Det finnes i tillegg flere ulovfestede *personvernrettslige* prinsipper som kan tenkes å være relevante, men disse vil ikke bli behandlet særskilt i denne avhandlingen. Avgrensningen skyldes i hovedsak at oppgavens størrelsesmessige rammer setter visse begrensninger med hensyn til bredden i fremstillingen, og det er derfor foretatt en prioritering av de ulovfestede *arbeidsrettslige* prinsippene som anses å være særlig viktige i forhold til avhandlingens tema. Avslutningsvis vil det bli gjort rede for arbeidsgivers plikt til å varsle de ansatte før det settes i verk kontrolltiltak på arbeidsplassen.

Personopplysningsloven har både regler om adgangen til å *sette i verk* behandling av personopplysninger, regler som skal ivareta personvernhensyn *under behandlingen* og regler som skal sikre ivaretakelsen av de samme hensyn ved å *avslutte* en behandling. Det er hovedsakelig den rettslige adgangen til å *iverksette* kontrolltiltakene som er temaet for denne avhandlingen. Enkelte regler om etterfølgende bruk av innsamlede opplysninger vil likevel bli behandlet, siden slik bruk ofte er en forutsetning for å oppnå formålet med innsamlingen. Det domstolskapte arbeidsrettslige regelverket er ikke utformet med en tilsvarende grad av nyansering. Domstolene har utformet de rettslige

---

forholdsvis trivielle opplysningstyper i forbindelse med den typen kontrolltiltak som skal behandles i denne avhandlingen.

[4] Det kan tenkes å ligge visse begrensninger også i menneskerettighetene, og da særlig i Den Europeiske Menneskerettighetskonvensjon (EMK) art. 8 og FN-konvensjonen om Sosiale og Politiske Rettigheter (SP) art. 17. Konvensjonene ble inkorporert i norsk lovgivning gjennom vedtakelsen av menneskerettsloven av 21. mai 1999 nr. 30. Det er imidlertid usikkert hvorvidt de nevnte bestemmelsene oppstiller konkrete rettigheter og plikter i forholdet mellom private aktører, eller om de kun oppstiller skranker for den nasjonale lovgivningen. I NOU 1997: 19 på side 41 har utvalget tatt det standpunkt at EMK art. 8 kan få anvendelse på områder som omfattes av personopplysningslovens bestemmelser, men at overholdelse av personverndirektivet og den implementerte lovgivningen også vil innebære overholdelse av EMK art. 8. Utvalget hevdet videre at personverndirektivet og den tidligere personregisterloven gikk lengre i beskyttelsen av enkeltindividenes rettigheter enn SP art. 17. Jeg finner det ikke hensiktsmessig å drøfte problemstillingen nærmere, da dette ville sprenge de størrelsesmessige rammene for denne avhandlingen.

utgangspunktene for kontrolltiltakene og begrensningene i disse. Det opereres imidlertid ikke eksplisitt med egne regler for iverksettelse av tiltakene og etterfølgende bruk av innhentede opplysninger. De ulovfestede prinsippene vil imidlertid kunne innebære tilsvarende begrensninger i den etterfølgende bruken som personopplysningslovens bestemmelser i så henseende.

Avhandlingen er sentrert rundt en særskilt form for kontrolltiltak; kontroll av e-post og datalogger.[5] Avgrensningen skyldes i hovedsak aktualitetshensyn. Emnet har de siste årene vært viet stor oppmerksomhet, både i juridiske kretser og i massemedia.[6] Den teknologiske utviklingen har åpenbart skapt behov for rettslig regulering av adgangen til å foreta denne typen inngrep overfor arbeidstakerne. Bedriftene blir stadig mer avhengige av IT-utstyr på arbeidsplassene, og datamaskiner, internett og e-post blir ofte brukt av ansatte i langt større omfang enn det som anses påkrevd og tillatt etter arbeidsavtalen.[7] Det er ikke vanskelig å tenke seg at arbeidsgiver har et reelt behov og ønske om å føre en viss kontroll av IT-bruken. Arbeidsgiver kan også med forholdsvis enkle grep kontrollere nær sagt alle IT-relaterte aktiviteter via bedriftens datasystem, forutsatt at kunnskapen og ressursene er til stede. Den innsamlede informasjonen vil potensielt kunne brukes mot de ansatte i forbindelse med konkrete personalkonflikter, i forbindelse med *utvelgelsen* ved påkrevde rasjonaliseringstiltak, som ledd i avgjørelsen av hvem som skal forfremmes eller som ledd i forfølgelse av straffbare handlinger. Dette bringer på banen viktige problemstillinger omkring vern av arbeidstakernes *"personlige integritet"*.[8] De rettslige spørsmålene omkring kontroll og overvåking av e-

---

[5] "Datalogger", eller "logger", er mapper/kataloger hvor innsamlede opplysninger registreres og lagres i datasystemet. Selve innsamlingen kalles "logging", og er nærmere beskrevet i punkt 5.1 nedenfor.

[6] Se eksempelvis <http://www.dagbladet.no/nyheter/2002/10/27/352281.html> (13.10.2003).

[7] Se for eksempel Rt. 2001 side 1589 (Raufoss-dommen) og Gulating lagmannsretts kjennelse av 19. februar 2003 (LG-2003-00090), samt <http://www.dagbladet.no/dinside/2002/10/29/352444.html> (13.10.2003).

[8] Begrepet "personlig integritet" er etter det jeg kjenner til ikke definert i verken lovgivningen, rettspraksis eller litteraturen. I SOU 2002: 18 (svensk utredning) på side 53 finnes imidlertid en forklaring som kan sies å omfatte det mest essensielle i begrepet: *"(...) begreppet personlig integritet innebär att alla människor har rätt till en personlig sfär där ett oönskat intrång, såväl fysisk som psykisk, kan avvisas"*. SOU 2002: 18 vil bli nevnt ved flere anledninger i denne avhandlingen. Utenlandske

post og logger er ennå ikke *eksplisitt* lovregulert, og kan heller ikke sies å være endelig avklarte i rettspraksis.

1.2 Oversikt over relevante rettskilder

1.2.1 Lovgivning, ulovfestet rett og forholdet mellom regelverkene

Det rettslige utgangspunktet for arbeidsgivers adgang til å kontrollere sine ansattes e-post og logger må i utgangspunktet søkes i det ulovfestede arbeidsrettslige regelverket, særlig da i *arbeidsgivers alminnelige styringsrett.*[9] Samtykke og lovhjemmel utgjør alternative rettslige grunnlag i så måte. Kontrolladgangen er begrenset gjennom ulovfestede arbeidsrettslige regler og prinsipper – i tillegg til den begrensning som følger av arbeidsavtalene, personopplysningsloven og lovverket for øvrig.

Lov om arbeidervern og arbeidsmiljø mv. av 4. februar 1977 nr. 4 (arbeidsmiljøloven, aml.), er også relevant for denne avhandlingen. Enkelte av bestemmelsene *kan* sies å regulere adgangen til kontroll og overvåking på arbeidsplassen, og disse vil hovedsaklig bli behandlet i punkt 4.5 og 6.3.2. Lovens mest sentrale forarbeider er inntatt i Ot.prp. nr. 3 (1975-76).

Personopplysningsloven (popplyl.) av 14. april 2000 nr. 31 avløste personregisterloven av 9. juni 1978 nr. 48, og har som et overordnet formål *"å beskytte enkeltindivider mot at deres personvern blir krenket som ledd i behandlingen av personopplysninger"*, jf. formålsbestemmelsen i § 1 (1).[10] Loven trådte i kraft 1. januar 2001, og ble vedtatt som

---

lovforarbeider er ikke rettslig bindende i norsk rett, men kan likevel ha stor argumentasjons- og illustrasjonsverdi.

[9] Styringsretten er definert i punkt 2.1.

[10] Det finnes rundt omkring i lovgivningen spesialbestemmelser som regulerer særskilte former for behandling av personopplysninger. Denne særlovgivningen vil gå foran personopplysningslovens bestemmelser, jf. *lex specialis-prinsippet.* I tillegg har man inntatt en egen "konfliktbestemmelse" i popplyl. § 5, som sier at personopplysningsloven gjelder om ikke annet følger av særskilt lovgivning. Bestemmelsen er inntatt med tanke på at personopplysningsloven er en generell lov, og at det kan være nødvendig med særregulering på visse samfunnsområder. Konsekvensen av popplyl. § 5 er at

ledd i implementeringen av EFs personverndirektiv, 95/46/EF ("direktivet").[11] Loven gjelder i utgangspunktet på alle samfunnsområder – inkludert arbeidslivet. Den regulerer kontrolltiltak i arbeidslivet som omfatter behandling av personopplysninger, og vil på denne bakgrunn være sentral i forhold til avhandlingens tema. Lovens forarbeider finnes i NOU 1997: 19 ("Et bedre personvern"), i Ot.prp. nr. 92 (1998-99) og i Innst. O. nr. 51 (1999-2000).

I popplyl. § 1 (2) fastslås at loven, som ledd i det nevnte overordnede mål, skal etablere regler som bidrar til *"at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger"*. Bestemmelsen har to hovedfunksjoner. Den skal for det første gi uttrykk for lovens overordnede målsetning. For det annet vil bestemmelsen i seg selv være en sentral tolkningsfaktor ved anvendelsen av lovens øvrige regler, jf. Ot.prp. nr. 92 (1998-99) på side 101. Popplyl. § 1 (2) viser til "grunnleggende personvernhensyn", noe som innebærer at festnede oppfatninger om personvern vil være sentrale i fortolkningen av lovens skjønnsmessige kriterier. Alminnelige arbeidsrettsrettslige prinsipper som beskytter arbeidstakernes personverninteresser vil derfor komme inn som begrensning i adgangen til å behandle personopplysninger gjennom denne bestemmelsen, jf. NOU 1997: 19 på side 130.

Personopplysningsloven inneholder en rekke nye bestemmelser, men innebærer samtidig en videreføring og videreutvikling av den tidligere personregisterlovens regler.

---

personopplysningsloven kun gjelder i den grad særlovgivningen ikke har regulert behandlingen. Popplyl. § 5 har ingen nevneverdige rettslige konsekvenser i forhold til denne avhandlingen, og vil ikke bli behandlet ytterligere.

[11] Også Danmark, Sverige og Finland har vedtatt generelle personopplysningslover som ledd i implementeringen av personverndirektivet. Finland har også vedtatt "lag om integritetsskydd i arbetslivet" av 8. juni 2001: 477, og er blant de få EU-landene som har særregulert adgangen til kontroll og overvåking i arbeidslivet. Bakgrunnen for dette var at direktivets bestemmelser, og således også lovgivning gitt i kraft av dette, ikke i tilstrekkelig grad ivaretar de særlige situasjoner og behov som oppstår i arbeidslivet. I Sverige foreligger et lovforslag ("Integritetsutredningen", SOU 2002: 18) som til dels bygger på den finske loven, men det kan se ut til at forslaget ikke vil få den fornødne oppslutning i den svenske nasjonalforsamlingen.

En forskjell mellom de to lovene er at personopplysningslovens hovedfokus er *elektronisk behandling av personopplysninger*, mens det i den tidligere loven var fokusert sterkt på bruken av *personregistre*, jf. Ot.prp. nr. 92 (1998-99) på side 7. Den nye loven bygger også i større grad på regler om hvordan de aktuelle parter skal opptre i forbindelse med innhenting, registrering mv. av personopplysninger. Den bygger på prinsippet om menneskers selvstendige rett til å bestemme over opplysninger som vedrører dem selv.

Personvernretten og arbeidsretten har utspring i to forholdsvis ulike rettsområder. Arbeidsretten springer ut fra den alminnelige formuesretten og er en forholdsvis gammel rettsdisiplin. Personvernretten er skapt på bakgrunn av et ønske om å beskytte enkeltindivider mot urettmessig behandling av personopplysninger. Rettsdisiplinen har derfor klare linjer mot offentligretten, til tross for at den klassiske offentligretten tar sikte på å regulere offentlige myndigheters virksomhet, mens personvernretten i like stor grad retter seg mot private rettssubjekter.[12] På bakgrunn av den enorme tekniske utviklingen, og da særlig innen EDB, har personvernretten møtt en rekke nye utfordringer. For å imøtekomme de nye utfordringene har man både i Norge og internasjonalt vedtatt en rekke lover og regler for å demme opp for potensielle skadevirkninger av denne utviklingen. Personvernretten, slik den fremstår i dag, er på denne bakgrunn en nyskapning i norsk og utenlandsk rett.

Personvernretten har et meget vidt nedslagsfelt. Dette er også et av hovedproblemene med personopplysningsloven – den kan tenkes å være litt for generell til å fungere tilstrekkelig i reguleringen av forholdet mellom partene i arbeidslivet. Arbeidsretten har på sin side et forholdsvis snevert og klart avgrenset virkeområde, og reglene er utformet deretter. Den regulerer alene forholdet mellom arbeidsgivere og arbeidstakere, samt forholdet mellom arbeidsgiver- og arbeidstakerorganisasjonene. Arbeidsgiverne må forholde seg til både personvernretten og arbeidsretten i forbindelse med kontrolltiltak på arbeidsplassen. De rettslige grunnlagene for kontrolltiltakene er imidlertid noe forskjellig utformet. Etter de arbeidsrettslige reglene utgjør styringsretten det mest

[12] Jf. Peter Blume og Jens Kristiansen (Danmark), "Databeskyttelse på arbejdmarkedet" på side 36 for dansk retts vedkommende.

sentrale hjemmelsgrunnlaget, og med de begrensninger som følger av lovfestede og ulovfestede regler og prinsipper, gir styringsretten arbeidsgiver en viss rett til å foreta kontrolltiltak overfor sine ansatte. I personopplysningsloven er utgangspunktet i stedet at enhver behandling av personopplysninger er forbudt – med mindre det finnes et konkret rettslig grunnlag. Personopplysningsloven fremtrer dermed som en sentral begrensning i styringsretten.

De ulovfestede arbeidsrettslige reglene utgjør relevante tolknings- og utfyllingsfaktorer ved anvendelsen av personopplysningslovens regler. Det vil derfor være sentralt i denne avhandlingen å foreta en sammenlikning av innholdet i personopplysningslovens regler og det ulovfestede regelverket. Til tross for manglende fokus på arbeidslivet under utarbeidelsen av personopplysningsloven, er det likevel klart at lovgiver har vært klar over eksistensen av det ulovfestede regelverket. I hvilken grad dette regelverket vil fremstå som en viktig tolkningsfaktor, vil imidlertid ikke bare avhenge av norske domstolers oppfatning av problemstillingen. Praksis fra EF-domstolen og EFTA-domstolen vil, her som for EØS-retten for øvrig, være en viktig brikke i samspillet mellom regelverkene. Det er på det rene at personopplysningsloven bygger på mange av de samme prinsipper og utgangspunkter som man finner i det arbeidsrettslige regelsettet. Til tross for at lovgiver neppe har intendert å endre rettstilstanden vesentlig i forhold til de arbeidsrettslige prinsippene, vil praktiseringen av personopplysningslovens bestemmelser i stor grad måtte bygge på praksis fra EF-domstolen. Det kan derfor tenkes at skillet mellom de to regelsettene vil bli større i fremtiden enn det er nå.

Det arbeidsrettslige regelverkets betydning for fortolkningen av personopplysningsloven vil videre avhenge av hvor presist reglene i loven er utformet. Der lovteksten er klar og detaljert, vil betydningen bli mindre. Store deler av loven består imidlertid av vage og skjønnsmessige begreper – så som *berettiget interesse, nødvendig, saklig, relevant* mv. Her vil de korresponderende ulovfestede reglene kunne komme inn som viktige tolkningsfaktorer. Lovens ordlyd er i mange tilfeller heller ikke identisk med ordlyden i direktivet, og dette kan gi grobunn for et en viss selvstendig nasjonal fortolkning – innenfor visse rammer. Hvis for eksempel et kontrolltiltak er ansett som nødvendig og forholdsmessig etter de ulovfestede reglene, vil dette kunne

være utslagsgivende i en konkret sak hvor tiltaket er basert på hjemmelen i popplyl. § 8 bokstav f).[13] I avveiningen mellom eventuelle motstridende regler, vil personopplysningslovens formål måtte tillegges betydelig vekt. Dersom bruk av de ulovfestede regler og prinsipper som tolkningsfaktor i det enkelte tilfelle ville gi arbeidstakerne et utvidet vern, er dette noe som i aller høyeste grad faller innenfor personopplysningslovens formål. Lovgiver har imidlertid kompetanse til ved lov, eventuelt bestemmelser gitt i medhold av lov, å endre ulovfestet rett. Det kan således tenkes at vedtakelsen av personopplysningsloven innebærer visse begrensninger i forhold til den kontrolladgang som følger av ulovfestede arbeidsrettslige regler og prinsipper. Rettskildeprinsippene setter således visse begrensninger; i de tilfeller eldre ulovfestede arbeidsrettslige prinsipper taler for én løsning, mens personopplysningsloven klart taler for en annen, må loven gå foran, jf. *lex posterior - prinsippet*.

1.2.2 Folkerettslige forpliktelser

1.2.2.1 Europarådskonvensjonen av 28. januar 1981 nr. 108

Europarådskonvensjonen av 28. januar 1981 nr. 108 om personvern i forbindelse med elektronisk databehandling av personopplysninger ble ratifisert av Norge 20.02.1984, og innebærer en folkerettslig forpliktelse for Norge. Konvensjonen regulerer rettslige spørsmål omkring lagring og håndtering av personopplysninger ved hjelp av EDB-utstyr, og fastsetter visse minimumskrav i forbindelse med personopplysnings-behandling for de statene som har ratifisert den.[14] Konvensjonen har gitt grunnlag for en rekke *rekommandasjoner* på personvernområdet, men disse har ikke vært undersøkt i forbindelse med denne avhandlingen.[15] Bakgrunnen for at konvensjonen nevnes her, er

---

[13] Bestemmelsen er beskrevet nærmere i punkt 3.4.3 nedenfor.

[14] At konvensjonen oppstiller *minimumskrav* innebærer at den enkelte stat kan gi de som opplysningene gjelder, flere og mer omfattende rettigheter enn det som følger av konvensjonen, jf. NOU 1997: 19 på side 37 (punkt 7.2).

[15] Rekommandasjonene er kun anbefalinger til de ulike statene, og er ikke folkerettslig bindende. De er imidlertid politisk bindende, jf. NOU 1997: 19 på side 37 (punkt 7.3). International Labour Organisation (ILO) er en organisasjon som også har utarbeidet rekommandasjoner på dette området (se ILO's Code of

at den har vært et viktig utgangspunkt for utarbeidelsen av EFs personverndirektiv, som igjen dannet utgangspunkt for personopplysningsloven.[16]

1.2.2.2 EFs personverndirektiv

Personverndirektivet (*EF-direktivet om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, 95/46/EF*) har som formål å etablere felles reguleringsprinsipper og et ensartet vern for behandling av personopplysninger i hele EU-området.[17] I artikkel 1 nr. 1 er det fastslått at direktivet skal sikre fysiske personers grunnleggende rettigheter og friheter, spesielt retten til privatlivets fred, i forbindelse med behandling av personopplysninger. Det er videre lagt stor vekt på at direktivet skal sikre fri utveksling av personopplysninger mellom medlemsstatene, jf. artikkel 1 nr. 2.

Direktivet forplikter statene til å gjennomføre lovgivning som tilfredsstiller kravene i direktivet.[18] I tillegg skal direktivet fremme en formålsorientert fortolkning av nasjonale personvernrettslige regler. Dette betyr at også særlovgivningen må bygges på og tolkes i samsvar med direktivets prinsipper. Som det meste av fellesskapsrettens regler, er direktivet ment å ha en dynamisk funksjon; det skal tolkes i takt med utviklingen og

---

Conduct/Code of Practise). Retningslinjene fungerer som rettesnorer for medlemsstatenes lovgivning, samt også for utformingen av kollektive avtaler i arbeidslivet. ILO har ikke utformet noe regelverk omkring kontroll av e-post og logger på arbeidsplassen som folkerettslig sett binder Norge. Hensiktsmessigheten av å redegjøre for organisasjonen og dens regelverk er derfor liten i denne avhandlingen. ILOs retningslinjer stod imidlertid sentralt for utarbeidelsen av den finske loven om personvern i arbeidslivet. Se også ILOs "Protection of worker's personal data" fra 1997.

[16] Jf. NOU 1997: 19 på side 37 (punkt 7.2).

[17] Jf. Ot.prp. nr. 92 (1998-99) side 13 (punkt 2.4).

[18] Direktivet utgjør minimumsstandarder for de statene som er bundet av det. Dette betyr at det i utgangspunktet ikke er noe i veien for at nasjonal lovgivning vedtar lover, forskrifter mv. som styrker personvernet i forhold til direktivets bestemmelser. En begrensning må likevel presiseres; vernet kan ikke bli så sterkt at det hindrer oppfyllelsen av målsetningen om fri flyt av personopplysninger mellom medlemsstatene, jf. NOU 1997: 19 på side 38 (punkt 8.1) og direktivet art. 1 nr. 2.

utbyggingen av regelverket for øvrig. Direktivet er inntatt i EØS-avtalen, noe som innebærer at også Island, Liechtenstein og Norge er bundet av dets bestemmelser.[19]

Direktivets forarbeider har ikke vært benyttet *direkte* i denne avhandlingen. Noe av bakgrunnen er at forarbeidene er vanskelig tilgjengelige, og det er ikke snakk om forarbeider tilsvarende de man har i norsk rett.[20] Direktivets forarbeider antas heller ikke å ha særlig stor betydning for EF-domstolens fortolkning av direktivets bestemmelser. Direktivets ordlyd og formålsbestemmelsen står mer sentralt i så henseende.[21]

1.2.3 Rettspraksis

1.2.3.1 Nasjonal rettspraksis

I dette avsnittet vil det kort bli redegjort for i hvilken grad de problemstillinger som er skissert i punkt 1.1 kan belyses ved hjelp av eksisterende rettspraksis.[22] Den rettspraksis det er referert til i denne avhandlingen er funnet ved søk på Lovdata. Til dels er dommene funnet ved frisøk etter særskilte emner og/eller lovbestemmelser, men enkelte av dem er også funnet gjennom referanser i litteraturen.

Innen emnet kontroll og overvåking i arbeidslivet er mengden av rettsavgjørelser forholdsvis liten – særlig fra perioden etter vedtakelsen av personopplysningsloven. Når det gjelder praksis omkring kontroll av e-post og datalogger, finnes det ikke tilstrekkelig rettspraksis til at man uforbeholdent kan si at rettsstillingen er vel etablert og stabil. Det finnes imidlertid enkelte avgjørelser fra de alminnelige domstoler og Arbeidsretten som kan ha overføringsverdi på dette området. Blant annet finnes det noe relevant

---

[19] Direktivet ble inntatt i EØS-avtalens vedlegg XI om telekommunikasjonstjenester ved EØS-komiteens beslutning av 25. juni 1999 (nr. 83), jf. St.prp. nr. 34 (1999-2000) på side 1. Se <http://odin.dep.no/ud/norsk/publ/stprp/032005-034007/index-hov001-b-n-a.html> (13.10.2003).

[20] Jf. NOU 1997: 19 på side 38 (punkt 8.3).

[21] Les mer om dette i Lee Bygraves doktoravhandling, "Data Protection Law – Approaching its rationale, logic and limits" på side 36.

strafferettslig praksis omkring avskjæring av illojale og/eller ulovlig ervervede bevis (eksempelvis ulovlig fjernsynsovervåking på arbeidsplassen), samt noe arbeidsrettslig praksis omkring bevisavskjæring i oppsigelses- og avskjedssaker. Det er verdt å påpeke at enkelte av dommene er forholdsvis gamle, og at avveiningen mellom hensynet til arbeidsgivers styringsrett og personvernhensynene kanskje ville slått annerledes ut i dag. Det er imidlertid forholdsvis klart at denne rettspraksisen vil kunne ha stor *argumentasjonsverdi*, til tross for at avgjørelsene kanskje ikke har prejudikatstatus eller for øvrig er tungtveiende etter alminnelige rettskildemessige betraktninger.[23]

Det finnes enkelte underrettsdommer på området, og noen av disse er behandlet i denne avhandlingen. Vekten av en underrettsdom er normalt forholdsvis liten, særlig der det er snakk om dommer avsagt av tingretten (tidligere by- eller herredsretten). I mangel av sentral høyesterettspraksis er det likevel nødvendig å se hen til disse avgjørelsene. Normalt vil underrettspraksis også ha større vekt der det ikke finnes praksis av "høyere rang".

1.2.3.2 Praksis fra EF-domstolen

Personverndirektivets bestemmelser og overholdelsen av disse håndheves av Kommisjonen og EF-domstolen innen EU, og av EFTA-domstolen og EFTAs Overvåkingsorgan overfor EFTA-statene i EØS. EF-domstolens praksis har vært undersøkt i forbindelse med denne avhandlingen, men uten at dette har resultert i funn av dommer med direkte relevans for dette emnet.[24] I det følgende blir det likevel kort

---

[22] For en generell fremstilling av rettspraksis som rettskildefaktor, se Torstein Eckhoff, "Rettskildelære" , på side 155 flg.

[23] Rettspraksis fra de øvrige nordiske landene kan også tenkes å få betydning for rettstilstanden i Norge – sett hen til at man i stor grad har forsøkt å oppnå samsvarende regelverk i EØS-området. Internasjonal rettspraksis er imidlertid ikke direkte bindende her til lands. Det antas også at man blant annet i Sverige og Danmark har gitt arbeidsgiver noe videre rammer til å utføre kontrolltiltak i kraft av sin styringsrett enn hva som er situasjonen i Norge. Se side 37 i rapporten "Kontroll og overvåking i arbeidslivet" fra underutvalget til arbeidslivslovutvalget av 20. juni 2002 (heretter kalt *"underutvalgets rapport"*). Dette er følgelig noe man må ta høyde for når man henviser til nordisk rettspraksis på dette området.

[24] Søk via Lovdata og via EF domstolens websider <http://europa.eu.int/cj/> (13.10.2003), samt litteratur omkring direktivet og personopplysningsloven.

redegjort for betydningen av EF-domstolens praksis innenfor personverndirektivets område. Dette anses hensiktsmessig, siden det lett kan tenkes å komme sentrale dommer fra domstolen i tiden etter ferdigstillelsen av denne avhandlingen.

Fellesskapsretten er dynamisk, og direktivene skal fortolkes i samsvar med EF-domstolens fortolkning av deres bestemmelser. Betydningen av domstolens praksis for norsk retts vedkommende er forsøkt regulert i EØS-avtalen artikkel 6 (jf. også EØS-loven[25] § 2, og ODA[26] artikkel 3 nr. 1). EØS-avtalen art. 6 fastslår at avtalens bestemmelser skal tolkes i samsvar med EF-domstolens praksis omkring de korresponderende bestemmelser i fellesskapsretten.[27] EØS-avtalen er i forholdet mellom Norge og EF kun en folkerettslig avtale, noe som innebærer at Norge kun har påtatt seg en folkerettslig forpliktelse til å fortolke EØS-avtalen og dens vedlegg (herunder personverndirektivet) i samsvar med EF-domstolens praksis. Avtalen er imidlertid inkorporert i norsk rett ved vedtakelsen av EØS-loven, og norske domstoler er også på denne bakgrunn forpliktet til å overholde avtalens bestemmelser, herunder artikkel 6. I utgangspunktet er det kun EF-domstolens avgjørelser *forut for undertegningen* av EØS-avtalen som er bindende i forhold til EØS-avtalen art. 6. Høyesterett har imidlertid lagt til grunn at EF-domstolens praksis generelt skal tillegges betydelig vekt i tolkingen av EØS-rettslige bestemmelser, jf. eksempelvis Rt. 2002 side 391 (”God Morgen-dommen”) og Rt. 1997 side 1954.

Når direktivet er implementert gjennom personopplysningsloven, vil det være personopplysningslovens ordlyd som i utgangspunktet er avgjørende for rettsanvendelsen i Norge. Lovens ordlyd er imidlertid på mange punkter skjønnsmessig og vag, og de norske forarbeidene er på flere punkter mangelfulle. Norske rettsanvendere er på denne bakgrunn ofte nødt til å se hen til direktivets ordlyd, dets

---

[25] Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det Europeiske Økonomiske Samarbeidsområde (EØS) mv. av 27.november 1992 nr. 109.

[26] ODA – Avtale mellom EFTA-statene om opprettelse av et Overvåkingsorgan og en Domstol.

[27] Artikkel 6 åpner for en rekke tolkningsproblemer som det ikke er hensiktsmessig å gå nærmere inn på her. For ytterligere redegjørelse, se eksempelvis ”EØS-rett” av Sejersted, Arnesen, Rognstad, Foyn og Stemshaug på side 161 flg.

forarbeider og EF-domstolens praksis omkring direktivet for å kunne kartlegge det nærmere innholdet i den norske lovens bestemmelser.

1.2.4 Datatilsynets praksis og retningslinjer

Datatilsynet er forvaltningens tilsynsorgan i forbindelse med håndheving av personopplysningslovens bestemmelser, jf. popplyl. § 42. Tilsynets rolle er særlig markant gjennom lovens melde- og konsesjonspliktsystem. Utover dette kan tilsynet utstede pålegg om opphør eller endring av ulovlige behandlinger (jf. popplyl. § 46) og ilegge tvangsmulkt (jf. popplyl. § 47) i de tilfeller den ulovlige behandlingen ikke endres eller opphører.

Personvernnemnda er fast klageorgan i saker etter personopplysningsloven, jf. popplyl. § 42 (4) og § 43. Nemnda behandler derfor klager på Datatilsynets vedtak, og har full kompetanse i klagesaker, jf. NOU 1997: 19 på side 119 (punkt 18.3.9.5). Praksis fra denne nemnda ville kunne vært interessant i forhold denne avhandlingens emne. Nemnda har imidlertid foreløpig ikke behandlet saker omkring kontroll av e-post og logger. [28]

Datatilsynets *retningslinjer* for behandling av personopplysninger vil bli trukket frem i avhandlingen. Retningslinjene er ikke bindende for domstolene, men kan likevel tenkes å ha stor praktisk betydning. Tilsynets *forvaltningspraksis* har ikke vært undersøkt. Offentlige myndigheters praksis har normalt heller ingen stor rettskildemessig vekt etter det tradisjonelle rettskildebildet. Likevel kan praksisen ha stor argumentasjonsverdi. Datatilsynets avgjørelser og retningslinjer er presumptivt basert på *kvalifiserte* oppfatninger av rettstilstanden. Det kan derfor lett tenkes at domstolene influeres av de oppfatninger Datatilsynet legger til grunn i sin praksis og sine retningslinjer.[29]

---

[28] Se <http://www.personvernnemnda.no/klagesaker/klagesaker.html> (13.10.2003).

[29] For ordens skyld presiseres at innholdet i Datatilsynets praksis og retningslinjer ikke nødvendigvis alltid samsvarer. Retningslinjene skal kun fungere som rettesnorer for samfunnsaktørene, og innebærer ikke nødvendigvis en sammenfatning av den praksis tilsynet utøver i sin saksbehandling.

1.3 Oversikt over den videre fremstillingen

I kapittel 2 gjøres det rede for de arbeidsrettslige utgangspunktene for kontrolltiltak i arbeidslivet og for personopplysningslovens saklige og geografiske virkeområde. I kapittel 3 gis en redegjørelse for personopplysningslovens vilkår for behandling av personopplysninger, samt betydningen av arbeidsavtalene og interne instrukser på arbeidsplassen. Ulovfestet arbeidsrett vil her bli trukket inn der det er naturlig og hensiktsmessig. Personopplysningslovens vilkår for behandling av personopplysninger (popplyl. § 8) innebærer i seg selv en viss begrensning i arbeidsgivers styringsrett, jf. nedenfor. I kapittel 4 gis imidlertid en redegjørelse for de øvrige lovfestede og ulovfestede begrensningene i kontrolladgangen, herunder saklighetsprinsippet, proporsjonalitetsprinsippet og arbeidsmiljølovens relevante bestemmelser. Kapitlene 2-4 inneholder forholdsvis generelle redegjørelser for de regler og prinsipper som kommer til anvendelse i forbindelse med kontrolltiltak i arbeidslivet. På bakgrunn av den avgrensning som er foretatt innledningsvis, er det imidlertid nødvendig med en konkretisering av kontrolladgangen i forhold til e-post og datalogger. Denne redegjørelsen er inntatt i kapittel 5. I kapittel 6 gjøres det rede for arbeidsgivers informasjonsplikt i forbindelse med kontrolltiltakene.

2 Rettslige utgangspunkter

2.1 Innledning

Ethvert kontrolltiltak krever en eller annen form for rettslig grunnlag, jf. *legalitetsprinsippet.*[30] Vi har ingen generell arbeidsrettslig lovgivning som konkret hjemler arbeidsgivers adgang til å kontrollere og overvåke sine ansatte. Kontrolladgangen er imidlertid regulert gjennom alminnelige regler om arbeidsgiveres og arbeidstakeres rettigheter og plikter overfor hverandre, samt gjennom lovfestede og ulovfestede personvern- og arbeidsrettslige regler og prinsipper.

Adgangen til å iverksette kontrolltiltak i arbeidslivet kan blant annet baseres på samtykke fra arbeidstakerne og på hjemmel i lov eller bestemmelser gitt i medhold av lov (forskrift). Disse rettslige grunnlagene finner man også igjen i personopplysningsloven, jf. popplyl. § 8. Det kanskje mest sentrale arbeidsrettslige hjemmelsgrunnlaget er likevel arbeidsgivers *alminnelige styringsrett*. Styringsretten er definert som *"arbeidsgivers rett til å lede, fordele og kontrollere arbeidet".*[31] Det finnes en rekke rettsavgjørelser hvor det er slått fast at arbeidsgiver i kraft av styringsretten har rett til å foreta kontrolltiltak overfor sine ansatte. Se for eksempel Rt. 2000 side 1602 og Rt. 2001 side 418, jf. nedenfor. I de tilfeller arbeidsgiver ikke makter å påvise noe annet rettslig grunnlag for kontrollen, vil spørsmålet normalt bli hvorvidt styringsretten gir ham den fornødne kompetanse. Spørsmålet er således ikke om arbeidsgiver i kraft av styringsretten *er berettiget* til å foreta kontrolltiltak eller ikke; spørsmålet er hvilke begrensninger og hvilke krav til prosedyre som gjelder.[32]

Styringsretten er begrenset av flere lovfestede og ulovfestede materielle regler og prinsipper. Blant disse kan nevnes saklighetsprinsippet, proporsjonalitetsprinsippet,

---

[30] Den tradisjonelle beskrivelsen av den materielle siden av legalitetsprinsippet går ut på at ethvert inngrep i borgernes rettssfære krever rettslig hjemmel. Se Torstein Eckhoff, "Rettskildelære", på side 313.

[31] Jf. underutvalgets rapport side. 26 (punkt 5.2.1), Jakhelln i "Fjernarbeid" på side 143 og Nøkk-saken (Rt. 2001 side 418).

[32] Jf. Jakhelln i "Fjernarbeid" på side 144.

lojalitetsplikten mellom partene i arbeidslivet, menneskerettighetene, arbeidsmiljøloven og individuelle og kollektive arbeidsavtaler. Adgangen til å foreta kontrolltiltak i arbeidslivet kan også være underlagt de begrensninger som følger av personopplysningsloven. Denne loven oppstiller en rekke vilkår for behandling av personopplysninger, og gjør på denne måten et innhugg i de beføyelser arbeidsgiver har i kraft av sin styringsrett. Den innebærer i så måte en *lovfestet begrensning i styringsretten*. Det første spørsmålet som må avklares i denne sammenheng er da hvilke saklige og stedlige forutsetninger som må foreligge for at loven skal komme til anvendelse. Lovens saklige og geografiske virkeområde vil derfor bli behandlet i de neste avsnittene, mens en utførlig redegjørelse for personopplysningslovens rettslige grunnlag for behandling av personopplysninger er inntatt i kapittel 3.

2.2 Personopplysningslovens virkeområde

2.2.1 Saklig virkeområde – popplyl. § 3

Personopplysningsloven regulerer *"behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler",* jf. § 3 (1) bokstav a)*,* og *"annen behandling av personopplysninger når disse inngår eller skal inngå i et personregister",* jf. § 3 (1) bokstav b). For å forstå rekkevidden av popplyl. § 3 er det en forutsetning å kjenne til innholdet i de begreper som er brukt i bestemmelsen. Begrepene er legaldefinert i § 2.[33]

Begrepet *"personopplysning"* er meget sentralt i personopplysningsloven, og innholdet i dette begrepet vil være helt essensielt i forhold til hvilke kontrolltiltak arbeidsgiver kan sette i verk overfor arbeidstakerne i kraft av lovens bestemmelser. Redegjørelsen nedenfor vil i første omgang omhandle det i forarbeidene fastsatte innhold av begrepet. I tillegg gis noen praktiske eksempler på kontrolltiltak som antas omfattet av loven.

[33] Definisjonene i § 2 følger mønsteret i direktivets artikkel 2, og er i det vesentlige sammenfallende med denne.

Personopplysninger er i § 2 nr. 1 definert som "*opplysninger og vurderinger som kan knyttes til en enkeltperson (...)".* Begrepet "enkeltperson" er således avgjørende for vurderingen av hvorvidt det foreligger en personopplysning i lovens forstand. Behandling av opplysninger som gjelder en konkret, navngitt person faller klart innenfor lovens virkeområde. Videre vil også behandling av opplysninger som på en mer indirekte måte identifiserer en enkeltperson omfattes – eksempelvis der personen ikke er navngitt, men hvor det finnes beskrivelser eller andre momenter som gjør det mulig å knytte opplysningene til denne bestemte personen.[34] Den tidligere *personregisterloven* omfattet opplysninger om både fysiske og juridiske personer. Den omfattet opplysninger og vurderinger som direkte eller indirekte kunne knyttes til identifiserbare enkeltpersoner, sammenslutninger eller stiftelser, jf. § 1 (2).[35] EF-direktivet omfatter enhver form for informasjon om identifiserte eller identifiserbare *personer*, jf. art. 2 bokstav a). Det er i forarbeidene til personopplysningsloven lagt til grunn at det ikke er noe i veien for å gi lovgivningen på nasjonalt plan anvendelse også overfor juridiske personer.[36] Løsningen ble likevel at loven kun retter seg mot *fysiske* personer. Dette følger for så vidt av lovens ordlyd, da personopplysninger som nevnt er opplysninger og vurderinger som kan knyttes til en *enkeltperson*. Juridiske personer faller således i utgangspunktet utenfor lovens virkeområde, med den reservasjon at kun opplysninger som gjelder juridiske personer *som sådanne* faller utenfor. Dersom opplysningene i realiteten kan knyttes til ansatte eller andre som er tilknyttet den juridiske personen, vil loven kunne gjelde fullt ut for behandlingen av disse opplysningene, jf. også NOU 1997: 19 på side 54. På samme side i utredningen bemerker utvalget at opplysninger om enkeltmannsforetak alltid vil være opplysninger om fysiske personer, og at loven derfor gjelder for behandling av slike opplysninger.

Forutsetningen for at det skal dreie seg om en personopplysning er at det foreligger en kobling mellom opplysningene/vurderingene og en fysisk person, jf. § 2 nr. 1. Opplysningene må med rimelig grad av sikkerhet *kunne* knyttes til en eller flere

---

[34] Jf. "Personopplysningsloven Kommentarutgave" av Wiik Johansen, Kaspersen og Bergseng Skullerud på side 68. Boken vil i det følgende bli kalt "Kommentarutgaven".

[35] Jf. Ot.prp. nr. 92 (1998-99) på side 25 (punkt 4.2.1), jf. også NOU 1997: 19 på side 52 (punkt 10.1.1.1).

[36] Jf. Ot.prp. nr. 92 (1998-99) på side 25 (punkt 4.2.2).

bestemte personer. Bakgrunnen for at lovens virkeområde er begrenset på denne måten, er at dersom opplysningene er knyttet til en stor krets av personer – uten at det er mulig å finne ut hvilken fysisk person det er snakk om – vil det sjelden være personvernhensyn som står i veien for behandlingen. Loven skal forhindre urettmessig bruk av opplysninger om den enkelte, og hvis denne ikke kan identifiseres har vedkommende ikke samme behov for vern.

> Datatilsynet har på sine seminarer (”overvåking på arbeidsplassen”) uttalt at loven også gjelder dersom opplysningene kan knyttes til en liten krets av personer – selv om det er usikkert konkret hvem de knytter seg til. Dette synspunktet mangler holdepunkter i lovens forarbeider. I NOU 1997: 19 på side 53 (punkt 10.1.1.2) har utvalget tvert i mot uttalt at vurderingene ville bli meget vanskelige dersom man åpnet for en slik løsning, og *”slike opplysninger vil meget sjelden kunne oppfattes som strengt personlige på samme måte som opplysninger om enkeltpersoner (...)”*. Datatilsynets oppfatning bør derfor modereres i henhold til uttalelsene i forarbeidene. Lee Bygrave og Dag W. Schartum har i sin forelesningsserie i personvernrett ved Universitetet i Oslo uttalt et syn som jeg mener har gode grunner for seg: Dersom opplysningene er knyttet til et IP-nummer, og datamaskinen har flere brukere, kan det tenkes at identifikasjonen er for fjerntliggende. Opplysningene kan således knyttes til hvilken som helst av brukerne – forutsatt at det kun er IP-nummeret som er registrert. Dersom det er 3-4 forskjellige brukere av den enkelte datamaskin, vil identifikasjonskravet neppe være oppfylt. Annerledes vil det stille seg dersom de 3-4 brukerne er av samme husstand. Her vil familien som enhet komme inn i vurderingen. Opplysninger om familien *som sådan* kan være sensitive og verneverdige – selv om man ikke har maktet å identifisere opplysningene med det enkelte familiemedlem. Heller ikke dette synet kan forankres direkte i forarbeidene, og synes å være uttrykk for Bygraves og Schartums de lege ferenda synspunkter, snarere enn en redegjørelse for rettstilstanden de lege lata. Familien som enhet bør imidlertid etter min oppfatning kunne gis en viss beskyttelse i tråd med dette synspunktet, sett hen til at familien som enhet atskiller seg vesentlig fra andre sosiale grupperinger, eksempelvis en gruppe arbeidstakere. Det kan synes som om Datatilsynets oppfatning til dels samsvarer med Bygraves og Schartums uttalelser. Datatilsynet har imidlertid ikke tatt forbehold for de tilfeller at den lille sammenslutningen av enkeltpersoner må være tilknyttet en familiær enhet.

På en liten eller mellomstor arbeidsplass vil det kunne være forholdsvis enkelt å knytte opplysningene opp mot enkelte arbeidstakere, da gruppen av ansatte her normalt utgjør en forholdsvis oversiktlig og enhetlig gruppe enkeltpersoner. Situasjonen kan imidlertid være annerledes hvis de ansatte bruker bedriftens datamaskiner om hverandre – uten å måtte logge seg på med private brukernavn og passord, jf. petitavsnittet ovenfor. Det er

likevel ikke noe krav at opplysningene rent faktisk er knyttet til en enkeltperson; det er tilstrekkelig at de *kan* knyttes til en sådan. I NOU 1997: 19 på side 131 er det uttalt at *"også opplysninger som for den behandlingsansvarlige fremstår som anonymiserte kan være "personopplysninger" i lovens forstand dersom det finnes referanser eller andre tilknytningspunkter som gjør identifisering mulig"*. Det oppstilles altså visse kvalifikasjonskrav, eller *identifikasjonskrav.* Det foreligger ingen rettspraksis som stiller opp retningslinjer for denne grensedragningen. I Ot.prp. nr. 92 (1998-99) på side 101 har imidlertid departementet (tilsynelatende) lagt listen høyt. Departementet uttaler at man i vurderingen vil måtte ta i betraktning *"alle hjelpemidler som det er rimelig å tro at noen kan komme til å anvende for identifiseringsformål (...)"*. Videre er det uttalt at det vil dreie seg om en personopplysning dersom man med en bestemt "nøkkel", eksempelvis en tallkode, kan knytte opplysningene til en bestemt person. Krypterte opplysninger vil også være omfattet av begrepet, *"dersom noen kan gjøre opplysningene lesbare og dermed identifisere personene som opplysningene vedrører"*. Det spiller heller ingen rolle om identifiseringen kun vil være mulig for et begrenset antall personer. Også opplysninger som en arbeidstaker legger igjen på en internettside vil være omfattet, selv om det i realiteten kun er leverandøren av siden som har muligheter til å foreta identifikasjonen – og ikke eksempelvis vedkommendes arbeidsgiver. Departementet har likevel satt en grense – som for så vidt også følger av lovens ordlyd: dersom opplysningene er anonymisert på en slik måte at den opplysningene gjelder ikke lenger kan identifiseres, er det ikke snakk om personopplysninger. De lege ferenda bør det imidlertid ikke stilles så strenge krav. Det kan eksempelvis tenkes at man bør foreta en proporsjonalitetsvurdering; desto viktigere eller mer sensitive opplysningene er for arbeidstakeren, desto mindre innsats i identifikasjonsprosessen kreves før man vil ha med en personopplysning å gjøre. Og motsatt; dersom opplysningene er av liten betydning for arbeidstakeren, trenger det ikke være snakk om en personopplysning til tross for at identifikasjonen forholdsvis lett kan gjøres. I sondringen/tolkingen vil det være nødvendig å gjøre aktivt bruk av lovens formålsbestemmelse, samt hensynene bak lovens avgrensninger forøvrig, jf. Ot.prp. nr. 92 (1998-99) på side 101. Departementet uttalte her at det kan tenkes tilfeller hvor ordlyden i popplyl. § 2 nr. 1 kan peke i retning av at det er snakk om personopplysninger, men hvor personvernhensynene ikke kan begrunne at opplysningene skal vernes. Et slikt tilfelle kan nettopp være at de aktuelle

opplysningene riktignok kan knyttes til en bestemt person, men hvor opplysningenes innhold på ingen måte kan "skade" den aktuelle personen eller påføre denne ubehag. Loven ville i motsatt fall lett få et langt videre nedslagsfelt enn lovens formål og lovgivers intensjoner skulle tilsi.

> Et eksempel kan være på sin plass. Gitt at arbeidsgiver ønsker å finne ut hva slags aviser hans ansatte liker best å lese – slik at han kan bestemme hvilke aviser som skal kjøpes inn for de ansatte. I stedet for å spørre hver enkelt ansatt, går arbeidsgiver inn i datasystemets aktivitetslogger for å sjekke hvilke av nettavisene som er hyppigst besøkt av de ansatte. Loggopplysningene kan ofte med enkle grep knyttes opp mot den enkelte ansatte, ved bruk av IP-adressene e.l. Dersom det ikke er forsøkt å foreta noen identifikasjon, og opplysningene etter å ha blitt brukt til sitt formål slettes, er det få personvernhensyn som tilsier at opplysningene er personopplysninger i lovens forstand. Etter ordlyden er det klart at opplysningene er omfattet. Reelle hensyn og formålsbetraktninger – sett i sammenheng med departementets uttalelser ovenfor – tilsier likevel at opplysningene og behandlingen ikke bør være omfattet av lovens saklige virkeområde.

"Behandling av personopplysninger" er i popplyl. § 2 bokstav b) definert som *"enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter"*. Definisjonen bygger på direktivet artikkel 2 b).[37] Begrepet står sentralt i den nye loven, og er nytt i og med denne. Den tidligere personregisterloven var som nevnt sentrert rundt bruken av personregistre, mens *elektronisk behandling av personopplysninger* nå er den mest sentrale formen for behandling, jf. § 3 (1) bokstav a). Endringen har medført at personopplysningsloven har fått et vesentlig videre anvendelsesområde enn personregisterloven, da førstnevnte også omfatter kontroll og overvåking av moderne tekniske innretninger, så som e-post, datalogger mv. Noe av bakgrunnen er at man ville unngå en altfor utvidende tolkning av personregisterbegrepet, noe den tekniske

---

[37] Direktivet artikkel 2 bokstav b) lyder: *""Behandling av personopplysninger" ("behandling"): enhver operasjon eller rekke av operasjoner som med eller uten elektroniske hjelpemidler utføres i forbindelse med personopplysninger, for eksempel innsamling, registrering, systematisering, oppbevaring, tilpasning eller endring, gjenfinning, søking, bruk, videreformidling, ved overføring, spredning eller andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, sperring, sletting eller tilintetgjøring"*. Flere av disse eksemplene ble utelatt i den norske loven av lovtekniske hensyn, men gjelder likevel fullt ut (jf. *"enhver bruk"*), jf. NOU 1997: 19 på side 132.

utviklingen ellers ville nødvendiggjort. Behandling av opplysninger i registre er fortsatt omfattet av loven – også ved *manuell* behandling av personopplysninger, jf. § 3 (1) bokstav b). Elektronisk behandling av personopplysninger som inngår i personregistre er selvsagt også omfattet av loven, men dette følger av bokstav a).

Loven likestiller hel og delvis elektronisk behandling av personopplysninger, jf. popplyl. § 3 (1) bokstav a). Det spiller således ingen rolle om deler av behandlingen foregår manuelt. Loven gjelder for hele behandlingsprosessen, jf. NOU 1997: 19 på side 135.

”Behandling” sikter til ulike operasjoner som utføres i forbindelse bruken av personopplysningene. Loven nevner en rekke eksempler på slik bruk eller denne typen operasjoner, jf. ovenfor. Disse er imidlertid kun eksempler på bruk av personopplysninger som faller innenfor lovens virkeområde, og listen er ikke uttømmende. Dette følger av at det både står ”f.eks.”, samt at det eksplisitt er angitt i teksten at *enhver* bruk av personopplysninger rammes, jf. popplyl. § 2 nr. 2.

Elektronisk behandling av personopplysninger omfatter også opplysninger utover de som er nedfelt i alminnelige skriftlige dokumenter, så som for eksempel lyd og bilde, jf. Ot.prp. nr. 92 (1998-99) på side 101. Hvilket lagringsmedium som benyttes er uten betydning, så lenge identifikasjonen er mulig. Når arbeidsgiver kontrollerer sine ansattes e-post ved hjelp av en datamaskin, hva enten han/hun går inn på vedkommendes e-postprogram og leser e-posten eller kontrollerer den ved hjelp av e-postloggene på arbeidsgivers server, er dette elektronisk behandling av personopplysninger som omfattes av loven, jf. NOU 1997: 19 på side 132 og Rt. 2002 side 1500. Forutsetningen er da at de opplysningene som innhentes, lagres e.l., kan knyttes til den enkelte arbeidstaker. Tilsvarende gjelder kontroll av de øvrige loggene på serveren.

Loven gjelder for behandlingen enten den utføres av privatpersoner, forvaltningen eller private sammenslutninger, jf. Ot.prp. nr. 92 (1998-99) på side 104.

Et eksempel kan klargjøre grensedragningen mellom elektronisk behandling som omfattes av loven, og situasjoner som ikke omfattes. Dersom arbeidsgiver oppdager barnepornografi på arbeidstakerens datamaskin gjennom søk på bedriftens server eller på arbeidstakerens datamaskin, er dette behandling av personopplysninger i lovens forstand. Dersom han derimot går forbi den ansattes kontor og ser at vedkommende ser på barnepornografi, og deretter sprer (muntlige) rykter om vedkommende på arbeidsplassen, er dette ikke omfattet. Annerledes stiller det seg dersom vedkommende deretter lagrer opplysninger om hendelsen på en datafil eller videresender opplysningene pr. e-post, eventuelt noterer hendelsen ned i vedkommendes (manuelle) personalmappe.[38] I sistnevnte tilfelle er det snakk om manuell behandling av personopplysninger som inngår i et personregister, og situasjonen omfattes av loven dersom registreringen åpner for *" (...) at opplysninger om den enkelte kan finnes igjen"*, jf. popplyl. § 2 nr. 3. Se popplyl. § 3 (1) bokstav b), jf. Ot.prp. nr. 92 (1998-99) på side 104.[39]

Behandling av personopplysninger for rent private/personlige formål omfattes ikke av loven, jf. § 3 (2).[40] Dersom arbeidsgiver som privatperson behandler opplysninger om en av sine ansatte på sin private hjemmeside, er dette i utgangspunktet ikke omfattet av loven.[41] Det vil her kunne oppstå vanskelige grensedragninger. I hvilke tilfeller opptrer arbeidsgiver som nettopp arbeidsgiver, og i hvilke tilfeller må hans aktiviteter sees på som private? Spørsmålet er ikke løst i forarbeidene. De lege ferenda bør det imidlertid kunne oppstilles visse retningslinjer. Dersom arbeidsgivers aktiviteter på ingen måte knyttes opp mot bedriften eller dens virksomhet, taler mye for at arbeidsgivers aktiviteter på sin hjemmeside er av privat karakter. Dersom hjemmesiden derimot

---

[38] Se underutvalgets rapport på side 41, annet avsnitt.

[39] I odelstingsproposisjonen er følgende uttalt: *"Særlig praktisk er manuelle personregistre, dvs tradisjonelle registre som finnes i papirform med personnavn eller –aliaser som søkenøkkel"*. I NOU 1997: 19 på side 55 (punkt 10.1.2.1.1) er det uttalt at det kreves opplysninger om flere personer (mer enn to-tre personer) for at arkivet skal være *register* i lovens forstand.

[40] Se også direktivets artikkel 3 nr. 2.

[41] Unntaket gjelder ikke for økonomiske aktiviteter som overstiger det som er vanlig for fritidsaktiviteter, og heller aktiviteter som enkeltpersoner måtte foreta i enkeltmannsforetak mv., jf. Ot.prp. nr. 92 (1998-99) på side 105.

brukes som medium for å formidle virksomhetsrelaterte opplysninger, slik at ansatte og/eller andre bruker nettsiden for å tilegne seg informasjon om bedriften og aktiviteter der e.l., taler dette for at unntaket i popplyl. § 3 (2) ikke kommer til anvendelse. Tilsvarende bør legges til grunn der nettsiden har kombinert private og virksomhetsrelaterte formål. Formålsbetraktninger kan imidlertid føre til motsatt resultat i det enkelte tilfelle, jf. petitavsnittet nedenfor.

> En Generaladvokat ved EF-domstolen (Antonio Tizzano) har gitt en forhåndsuttalelse (”Opinion of Advocate General”) i forbindelse med direktivets unntak for behandling av personopplysninger til ”rent personlige eller familiemessige aktiviteter”, jf. direktivets art. 3 nr. 2 (2) og punkt 12 i dets preambel. Saken gjaldt en kvinne (Lindquist) som hadde publisert opplysninger om sine medarbeidere på en internettside. Generaladvokaten hevdet her at direktivets unntak i utgangspunktet ikke kom til anvendelse, siden opplysningene hadde blitt gjort tilgjengelige for hele verden gjennom internettsiden. Handlingen var likevel ikke i strid med direktivet, da behandlingen var ledd i en virksomhet som lå utenfor fellesskapsrettens område. Det ble lagt vekt på at handlingen var utført uten økonomiske motiver, og at hennes stilling i virksomheten var basert på frivillig, gratis arbeide. Uttalelser fra Generaladvokaten er ikke bindende for EF-domstolen. Domstolen tillegger imidlertid hans uttalelser stor vekt, og det er derfor grunnlag for å hevde at de har en viss rettskildemessig vekt i EF-retten. Indirekte kan de derfor også få betydning for norsk rett via EØS-avtalen art. 6.[42]

I denne avhandlingen blir begrepene *behandlingsansvarlig* og arbeidsgiver brukt noe om hverandre. Det samme gjelder *registrert* og arbeidstaker. Dette er begrunnet med at begrepene behandlingsansvarlig og registrert brukes i personopplysningsloven. I popplyl. § 2 nr. 4 er ”behandlingsansvarlig” definert som *”den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes”*. Ved kontroll av e-post og logger på arbeidsplassen vil den behandlingsansvarlige i de fleste tilfeller være nettopp arbeidsgiver. Der arbeidsgiver er en juridisk person, vil den juridiske personen representert ved ledelsen være behandlingsansvarlig, jf. Ot.prp. nr.

[42] Uttalelsen er tilgjengelig på <http://www.personvern.uio.no/pvpn/avgjorelser/index.html> (13.10.2003).

92 (1998-99) på side 102.[43] Dersom den behandlingsansvarlige setter bort behandlingsoppdraget til andre, såkalt "outsourcing", vil han/hun fortsatt være behandlingsansvarlig. Den som har fått oppdraget vil imidlertid være *"databehandler"* etter popplyl. § 2 nr. 5, jf. Ot.prp. nr. 92 (1998-99) på side 103. Den behandlingsansvarlige vil i disse tilfellene fremdeles ha ansvaret for behandlingens rettmessighet.[44] I popplyl. § 2 nr. 6 er en "registrert" definert som *"den som personopplysningene kan knyttes til"*, og den registrerte vil i denne oppgaven være arbeidstaker. I de mer generelle redegjørelsene benyttes "behandlingsansvarlig" og "registrert" forholdsvis konsekvent, mens det andre steder brukes "arbeidsgiver" og "arbeidstaker". Det ligger imidlertid ingen føringer i bruken av begrepene.

2.2.2 Geografisk virkeområde – popplyl. § 4

Den norske personopplysningsloven gjelder for behandlingsansvarlige som er etablert i Norge, jf. popplyl. § 4 (1) første punkt.[45] Etableringsstedet er således avgjørende, ikke hvor behandlingen av personopplysninger rent faktisk finner sted. Loven gjelder i utgangspunktet ikke hvor den behandlingsansvarlige er etablert i utlandet, men hvor han/hun bruker en databehandler i Norge. Se imidlertid popplyl. § 4 (2), jf. nedenfor. En eksemplifisering kan være nødvendig. Sett at en arbeidsgiver er etablert i England, og gir en norsk person i oppdrag å behandle personopplysninger om en av sine engelske ansatte. Personopplysningsloven vil i dette tilfellet ikke komme til anvendelse, til tross for at behandlingen skjer her til lands. I de land som er bundet av personverndirektivet, vil lovgivningen likevel være noenlunde sammenfallende med norsk rett. Datatilsynet har rett til innsyn i behandlinger som har funnet sted i Norge, men må anvende det aktuelle lands nasjonale lovgivning på forholdet.[46] Hvis den behandlingsansvarlige derimot er etablert i Norge, vil den norske personopplysningsloven komme til anvendelse dersom hele eller deler av behandlingen skjer i Norge – uavhengig om

---

[43] Ledelsen skal være representert ved en fysisk person. Pliktene som behandlingsansvarlig kan ikke påligge hele styret e.l., men skal i stedet påligge en fysisk person eller en stilling (typisk en lederstilling som daglig leder, direktør e.l.), jf. NOU 1997: 19 på side 132.

[44] Jf. NOU 1997: 19 på side 132 (merknader til popplyl. § 2 nr. 4) og på side 90 (punkt 13.4.2)

[45] Se også direktivet artikkel 4.

[46] Se direktivet artikkel 28 og Ot.prp. nr. 92 (1998-99) på side 28.

innsamlingen skjer i et annet land. Den rettslige adgangen til innsamlingen vil imidlertid være regulert av utenlandsk rett.[47]

Det neste spørsmålet blir deretter hva som skal til før en behandlingsansvarlig skal sies å være *etablert* i Norge. I forarbeidene er det uttalt at det avgjørende er om den behandlingsansvarlige har tilstrekkelig tilknytning til Norge til å være etablert slik uttrykket forstås ut fra en *alminnelig språklig forståelse*, jf. Ot.prp. nr. 92 (1998-99) på side 105. Videre er det uttalt at etableringskravet er oppfylt dersom et utenlandsk selskap har et datterselskap i Norge, og en representant for datterselskapet behandler personopplysninger.[48] Tilsvarende gjelder for utenlandske selskaper som har en filial i Norge, jf. Ot.prp. nr. 92 (1998-99) på side 106. I NOU 1997: 19 på side 136 er det uttalt at etableringskravet forutsetter en helhetsvurdering, hvor det sentrale i vurderingen blir hvorvidt behandlingen som finner sted i Norge er så omfattende og permanent at den norske loven bør få anvendelse. Tilsvarende uttalelse finnes i EF-direktivets preambel punkt 19:

> *"Etablering på en medlemsstats territorium forutsetter at det faktisk utøves en virksomhet innenfor en fast struktur. En slik strukturs rettslige form, enten det dreier seg om bare en filial eller et datterforetak med status som juridisk person, er ikke av avgjørende betydning i denne forbindelse (...)."* [49]

Disse kriteriene er imidlertid ikke særlig egnet til å klargjøre spørsmålet. Er det således tilstrekkelig at bedriften har postadresse/kontoradresse i Norge? Kreves det registrering i Enhetsregisteret? Er det tilstrekkelig at bedriften er skattepliktig her til lands? Spørsmålene må sies å være uavklarte. Reelle hensyn taler imidlertid for at det må finnes personale *i Norge* som jobber fast i bedriften eller datterselskapet/filialen. På

---

[47] Jf. Kommentarutgaven på side 86.

[48] Dersom det utenlandske selskapet har en rekke filialer i Europa, eksempelvis en i Norge, en i Sverige og en i Danmark, vil henholdsvis norsk, svensk og dansk rett regulere behandlingen. Alle disse tre landene har implementert direktivets bestemmelser, og i forholdsvis stor grad forsøkt å operere med likartede bestemmelser og normer, jf. Ot.prp. nr. 92 (1998-99) på side 106.

[49] I Ot.prp. nr. 92 (1998-99) på side 105 er det uttalt at "strukturens" rettslige status, eksempelvis virksomhetens sammenslutningsform, ikke er avgjørende.

denne måten vil det finnes personer her som kan oppfylle den behandlingsansvarliges plikter etter personopplysningsloven. Datatilsynet og påtalemyndighetene vil da i tillegg ha noen å henvende seg til innenfor landets grenser, dersom personopplysninger blir behandlet i strid med loven.

Popplyl. § 4 (2) gjelder tilfeller hvor en arbeidsgiver fra områder utenfor EØS benytter hjelpemidler i Norge til å behandle personopplysninger.[50] Dette innebærer eksempelvis at en russisk arbeidsgiver som benytter hjelpemidler i Norge til å behandle personopplysninger, kan bli omfattet av den norske personopplysningslovens bestemmelser.[51] Lovens geografiske virkeområde utvides altså i disse tilfellene, og det gjøres til dels unntak fra etableringskravet. Dersom hjelpemidlene kun benyttes for å overføre personopplysninger via Norge, kommer unntaket likevel ikke til anvendelse. Tredje ledd bestemmer at behandlingsansvarlige som nevnt i annet ledd og som benytter hjelpemidler i Norge, skal ha en representant som er etablert i Norge. Bakgrunnen for denne bestemmelsen er at den behandlingsansvarlige skal ha en stedfortreder som kan oppfylle de alminnelige pliktene til en behandlingsansvarlig, blant annet melde- og konsesjonsplikten og plikt til å gi den registrerte innsyn etter lovens § 18. Datatilsynet kan i disse tilfellene holde både arbeidsgiveren (behandlingsansvarlige) og hans representant ansvarlige for brudd på lovens bestemmelser.

[50] Sml. pkt. 2.2.2, første avsnitt. Med "hjelpemidler" menes alt slags utstyr som kan benyttes i behandlingen, både elektronisk (eks. datamaskiner) og ikke-elektronisk, jf. Ot.prp. nr. 92 (1998-99) på side 106 og NOU 1997: 19 på side 59 (punkt 10.2.3).

[51] Jf. Ot.prp. nr. 92 (1998-99) på side 106.

3 Rettslige grunnlag for behandling av personopplysninger i arbeidslivet

3.1 Innledning

I kapittel 2 ble det gjort kort rede for arbeidsgivers styringsrett og hvordan personopplysningsloven innebærer en lovfestet begrensning i denne. Innfallsvinkelen var altså *arbeidsrettslig*. Siktemålet i kapittel 3 er å gi en nærmere oversikt over rettsgrunnlagene for behandling av personopplysninger i popplyl. § 8. Deretter vil det trekkes paralleller til det arbeidsrettslige regelverket. Innfallsvinkelen vil derfor her bli *personvernrettslig* – med arbeidsretten som influerende faktor.

Personopplysningsloven oppstiller i § 8 de alminnelige vilkårene for behandling av personopplysninger, og krever enten *samtykke* fra den registrerte, *lovhjemmel* eller at behandlingen er berettiget ut fra en *nødvendighetsavveining.* Minst ett av disse rettslige grunnlagene må foreligge før behandlingen iverksettes. Rettsgrunnlagene er behandlet i henholdsvis punkt 3.2, 3.3 og 3.4, mens forholdet mellom dem er behandlet i punkt 3.5. I punkt 3.6 blir det redegjort for den generelle betydningen av arbeidsavtalene og interne instrukser gitt i kraft av styringsretten.

3.2 Samtykke

3.2.1 Innledning

Det første alternative rettsgrunnlaget for behandling av personopplysninger i popplyl. § 8, er *samtykke* fra den registrerte.[52] Hovedspørsmålene i punkt 3.2 flg. er hvilke krav som stilles til samtykke som rettsgrunnlag, samt hvorvidt det eksisterer noen forskjeller mellom personopplysningslovens krav og kravene etter ulovfestet rett i denne

[52] Se den korresponderende bestemmelsen i direktivet art. 7 bokstav a), jf. art. 2 bokstav h).

sammenheng. I tillegg vil det bli drøftet hva som eventuelt blir de rettslige konsekvensene av et tilbakekalt samtykke.[53]

Å samtykke til et kontrolltiltak er det samme som å akseptere inngrepet. Partene har således inngått en avtale *i forkant*.[54] Samtykket kan gis på flere tidspunkter; ved inngåelsen av arbeidsavtalen, rett forut for kontrolltiltaket eller i tidsrommet mellom disse to.

Under arbeidet med personopplysningsloven var det lovgivers klare intensjon at behandling av personopplysninger skal forsøkes basert på den registrertes samtykke.[55] Sentralt ved de nye reglene er at den registrerte i størst mulig grad skal kunne ha kontroll med opplysninger om seg selv. Hvilke krav som skal stilles til samtykket har imidlertid vært gjenstand for atskillig diskusjon, både i Norge og innad i EU. Det var derfor både nasjonalt og innen Unionen et åpenbart behov for en klargjøring og konkretisering. EU falt ned på en løsning hvor samtykket ble legaldefinert i direktivet. Definisjonen ble også inntatt i personopplysningsloven[56] og innebar en nyskapning i norsk rett, til tross for at man også opererte med samtykke som hjemmelsgrunnlag i den tidligere personregisterloven.[57]

For at et kontrolltiltak skal være lovlig hjemlet i samtykke fra arbeidstakerne, må samtykket tilfredsstille de kravene som er oppstilt i popplyl. § 2 nr. 7. Legaldefinisjonen av et samtykke er:

---

[53] Det har i teorien vært reist spørsmål om umyndige kan samtykke til kontrolltiltak/behandling av personopplysninger. Det vil føre for langt å drøfte denne problemstillingen her. Departementets utgangspunkt er imidlertid at samtykke skal gis av den umyndiges verge, jf. Ot.prp. nr. 92 (1998-99) på side 103.

[54] Et samtykke er her ikke det samme som en *etterfølgende* aksept, dvs. en form for godtaking av inngrepet etter at det er foretatt.

[55] Jf. Ot.prp. nr. 92 (1998-99) på side 108.

[56] Ordlyden er ikke identisk, men det antas å være sammenfall i innholdet. Se Ot.prp. nr. 92 (1998-99) på side 103, merknadene til popplyl. § 2 nr. 7.

[57] Det er ikke holdepunkter i forarbeidene for at personopplysningslovens krav til samtykke avviker fra den tidligere personregisterlovens krav.

"en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv".

Det er i utgangspunktet arbeidstakeren selv som skal gi sitt samtykke. I forarbeidene er det likevel åpnet for at samtykket kan gis av *fullmektig* – på vegne av arbeidstakeren.[58] At det her åpnes for samtykke gjennom fullmektig, betyr trolig at en fagforeningsleder eller en tillitsvalgt på arbeidsplassen kan samtykke på vegne av en ansatt – forutsatt at det foreligger en gyldig fullmakt til å gjøre dette. *Rent praktisk* vil dette kunne være en hensiktsmessig løsning. Det vil i visse tilfeller kunne være uforholdsmessig arbeidskrevende om arbeidsgiver, eventuelt representert ved ledelsen, skulle måtte henvende seg til hver enkelt arbeidstaker for å innhente samtykke. Tillitsvalgte eller fagforeningsrepresentanter vil derfor kunne være praktiske mellomledd i så måte. De lege ferenda er dette likevel en dårlig løsning. Personvernhensyn og formålene med loven, jf. at den registrerte skal ha kontroll med opplysninger som vedrører han selv, tilsier at et samtykke bør avgis av den registrerte selv. Riktignok vil en arbeidsgiver ikke komme unna kravene i popplyl. § 2 nr. 7, men et fullmaktsforhold kan i verste fall føre til at fullmektigen går utenfor de fullmakter han er gitt.[59] Selv om en fullmektig i mange tilfeller vil være bedre egnet til å ivareta den registrertes personverninteresser, kan det også tenkes tilfeller i motsatt retning. Med tanke på den personvernrisiko eksempelvis kontroll av e-post og datalogger innebærer, er det derfor betenkelig at samtykke skal kunne gis gjennom en fullmektig. Hadde det *kun* vært snakk om en *videreformidling* av et samtykke som var uttrykkelig, frivillig og informert, ville betenkelighetene ha vært mindre. Den registrertes representant ville imidlertid da ikke være en fullmektig i avtalerettens forstand, men et slags *bud*. Det er heller ingen uttalelser i forarbeidene som tilsier at fullmaktsforholdet skal være begrenset på denne måten. Et fullmaktsforhold kjennetegnes gjerne ved at fullmektigen er gitt et visst spillerom, noe som ikke ville vært tilfelle dersom representanten kun videreformidlet arbeidstakerens samtykke. Det oppstilles ingen retningslinjer i forarbeidene for et eventuelt fullmaktsforhold. Kravene i § 2 nr. 7 vil imidlertid måtte rettes mot

[58] Jf. Ot.prp. nr. 92 (1998-99) på side 103 og NOU 1997: 19 på side 133

[59] Forholdet mellom rett og legitimasjon skal ikke problematiseres ytterligere her.

fullmektigen, og ikke mot den registrerte selv. Dette innebærer at *fullmektigen* må avgi et uttrykkelig, frivillig og informert samtykke. At den registrerte da kanskje ikke er fullt informert om rekkevidden og konsekvensen av behandlingen, må han bære risikoen for selv. Vedkommende har selv valgt å benytte seg av en fullmektig for å ivareta sine interesser.

> Dersom eksempelvis en tillitsvalgt eller en fagforeningsrepresentant har fått fullmakt fra flere ansatte om å samtykke til behandling av personopplysninger, må det stilles krav om at fullmektigen overfor arbeidsgiver gjør det klart for denne hvilke av de ansatte som har utstyrt dem med en slik fullmakt. Arbeidsgiver kan følgelig ikke basere seg på at fullmakten er gitt av den samlede massen av ansatte uten å ha uttrykkelige holdepunkter for dette.

Det har lenge vært lagt til grunn i praksis og teori at arbeidslivets parter på avtalemessig grunnlag kan bli enige om at arbeidsgiver kan foreta visse kontrolltiltak overfor sine ansatte. Personopplysningslovens samtykkekrav er imidlertid langt mer utførlig redegjort for i lovens forarbeider enn kravet er definert i arbeidsrettslig praksis. Man har nå eksplisitte krav til innholdet i og forutsetningene for et gyldig samtykke. Det har likevel blitt oppstilt enkelte krav til samtykket også etter de ulovfestede reglene. Blant annet må arbeidstakeren være klar over hva samtykket innebærer og rekkevidden av dette. I tråd med alminnelige avtalerettslige regler er det også en forutsetning at samtykket har kommet klart til uttrykk.[60] Det synes således å være tilnærmet samsvar mellom det ulovfestede og det lovfestede samtykkekravet. Det finnes imidlertid en tenkelig forskjell; det kan stilles spørsmål om et såkalt *kollektivt samtykke* tilfredsstiller kravene i popplyl. § 2 nr. 7. Dette skal drøftes særskilt nedenfor. Med unntak av denne problemstillingen vil redegjørelsen for samtykke som rettsgrunnlag være basert på personopplysningsloven og rettskildene rundt denne.

Det oppstilles ingen formkrav til et samtykke i personopplysningsloven; dette kan gis både muntlig, skriftlig og elektronisk.[61]

---

[60] Jf. underutvalgets rapport på side 27.

[61] Jf. Ot.prp. nr. 92 (1998-99) på side 103. Med elektroniske samtykker menes typisk avkrysning/ tastetrykk på internett e.l. At samtykket er nedfelt skriftlig letter arbeidsgivers bevisbyrde dersom det

I departementets kommentarer til popplyl. § 24, som gjelder krav til hvordan informasjon etter §§ 18 til 22 skal gis, er det også lagt til grunn at informasjonen kan gis elektronisk.[62] I denne forbindelse er det uttalt at det må kreves at den registrerte identifiserer seg på en tilstrekkelig sikker måte, eksempelvis gjennom bruk av *digitale signaturer*. Forarbeidene sier ikke noe tilsvarende i forhold til popplyl. § 8, jf. § 2 nr. 7. De lege lata er det derfor lite trolig at det kan stilles slike krav i forhold til elektroniske samtykker. Ved samtykke til behandling av opplysninger som ikke har store personvernmessige konsekvenser, bør det kunne være tilstrekkelig at samtykke avgis ved eksempelvis e-post, avkrysning på internett e.l. Det kan imidlertid tenkes behandlingssituasjoner hvor opplysningene er særlig følsomme (se eksempelvis popplyl. § 9). De lege ferenda burde man derfor innføre visse krav til avgivelsen av elektroniske samtykker i de tilfeller behandlingen kan ha store personvernmessige konsekvenser.

3.2.2 Frivillig samtykke

Det første formelle kravet til samtykket i popplyl. § 2 nr. 7 er *frivillighet*. I dette ligger et krav om at samtykket skal være avgitt uten press, tvang eller lignende, jf. Ot.prp. nr. 92 (1998-99) på side 103-104.[63] Dette vilkåret oppstilles overfor arbeidsgiver selv, men gjelder også overfor tredjemenn, jf. Ot.prp. nr. 92 (1998-99) på side 104. Dersom en venn, slektning, ansatt eller andre tredjemenn på vegne av arbeidsgiveren påfører arbeidstakeren press eller tvang, vil et påfølgende samtykke åpenbart ikke tilfredsstille frivillighetskravet. Det er imidlertid ikke noe krav om at presset, tvangen e.l. påføres *på vegne* av arbeidsgiver. Også der det foreligger press eller tvang fra en tredjemann uten arbeidsgivers viten, vil et samtykke avgitt på grunnlag av dette være ugyldig etter loven. Dette kan skape problemer der det foreligger et implisitt press fra den samlede massen av arbeidstakere om at alle ansatte skal samtykke i diverse typer kontrolltiltak på arbeidsplassen. Kontrolltiltakene kan være begrunnet med at de vil kunne øke effektiviteten, noe som igjen vil kunne forhindre oppsigelser mv. Departementet synes ikke å ha vurdert denne problemstillingen under utarbeidelsen av forarbeidene. Etter

---

oppstår tvil om hvorvidt det foreligger et gyldig samtykke i lovens forstand, jf. odelstingsproposisjonen på samme side.

[62] Jf. Ot.prp. nr. 92 (1998-99) på side 122.

[63] I NOU 1997: 19 la utvalget til grunn at kravet til frivillighet var så selvsagt at man ikke trengte å uttrykke det eksplisitt i loven. Lovgiver valgte likevel å presisere det i popplyl. § 2 nr. 7.

min mening kan det likevel tenkes situasjoner hvor presset eller tvangen fremtrer så markant at det påfølgende samtykket må underkjennes. Arbeidsgiver bør derimot ikke kunne straffes eller bli erstatningsansvarlig for å bygge på et slikt samtykke – med mindre han er inneforstått med de bakenforliggende omstendigheter.

Hvis arbeidsgiver truer den enkelte arbeidstaker med oppsigelse dersom vedkommende ikke underkaster seg kontrolltiltakene, vil et påfølgende samtykke ikke være gyldig. Et samtykke vil heller ikke være frivillig dersom det er knyttet negative konsekvenser til en eventuell nektelse.

> Det kan reises spørsmål om arbeidsgiver i stedet kan tilby arbeidstakeren fordelaktige gjenytelser dersom vedkommende samtykker, uten at dette kommer i strid med frivillighetskravet. Dersom arbeidstakeren nekter, vil imidlertid fraværet av den fordelaktige ytelsen kunne anses å være en negativ konsekvens. Til tross for at primærkildene ikke sier noe om denne problemstillingen, taler reelle hensyn for at heller ikke fordelaktige "lokkemidler" kan benyttes for å fremprovosere et samtykke fra arbeidstakeren.

Det er ikke alltid like enkelt å vurdere hvorvidt et samtykke har vært avgitt frivillig. Til tross for at samtykket kanskje er nedfelt skriftlig, kan det tenkes at arbeidsgiver forut for avgivelsen av samtykket har påført et press som ikke så lett lar seg kontrollere i ettertid. Blant annet kan det tenkes at vedkommende måtte samtykke for å få stillingen. Frivillighetskravet etter popplyl. § 8 har ikke blitt behandlet av domstolene. De lege ferenda bør imidlertid arbeidsgiver kunne stille visse vilkår om behandling av personopplysninger i selve arbeidsavtalen. En arbeidsavtale er en gjensidig kontrakt mellom arbeidsgiver og arbeidstaker. Dersom arbeidsgiver i arbeidsavtalen stiller som vilkår at "den arbeidssøkende" skal ha rett til innsyn i all e-post som sendes og mottas gjennom sitt nettverk, kan arbeidstakeren simpelthen la være å skrive under dersom han mener vilkårene er uholdbare. I sin ytterste konsekvens kan dette medføre at vedkommende ikke får jobben, men dette er etter min mening uten betydning i forhold til personopplysningsloven.[64] Derimot er det tvilsomt om arbeidsgiver gjennom en

[64] Man kan kanskje stille spørsmålstegn ved den *reelle* frivilligheten i disse tilfellene. Etter loven er frivillighetskravet likevel oppfylt dersom arbeidsavtalen inngås frivillig. Se også punkt 3.6 nedenfor.

ensidig instruks krever at alle *ansatte* samtykker i behandlingen. Her vil frivillighetskravet kunne komme på spissen. Stillingsvernreglene vil i sin tur kunne beskytte de som nekter å avgi samtykke på et slikt grunnlag, jf. eksempelvis aml. § 60 og § 66.

3.2.3 Informert samtykke

Kravet om at samtykket skal være *informert* innebærer at arbeidstakeren må være fullt klar over hva han samtykker i. Arbeidsgiveren pålegges her en *plikt* til å gi tilstrekkelig informasjon om faktiske forhold av betydning for den ansatte.[65] Datatilsynet har på sine nettsider oppstilt retningslinjer i forhold til forståelsen av dette kravet:

> "Samtykket skal være informert. Den som skal registreres må få tilstrekkelig informasjon til å forstå hva samtykket gjelder og hvilke konsekvenser det kan få. Informasjonen til den registrerte skal minst omfatte:
>
> 1. navn og adresse på den behandlingsansvarlige
> 2. hva opplysningene skal brukes til
> 3. om opplysningene vil bli utlevert til andre, og eventuelt hvem som er mottaker
> 4. om det er frivillig å gi fra seg opplysningene
> 5. informasjon som gjør den registrerte i stand til å bruke sine rettigheter etter personopplysningsloven på best mulig måte, som f.eks. retten til å kreve innsyn, retting og sletting
> 6. hvor lenge personopplysningene vil bli behandlet eller oppbevart" [66]

Retningslinjene synes å være bygget på bestemmelsen i popplyl. § 19. Denne bestemmelsen omhandler *informasjonsplikten* i forbindelse med behandling av opplysninger om den registrerte, og ikke konkret informasjonskravet i forbindelse med innhenting av samtykke. Bestemmelsen kan likevel ha overføringsverdi i forhold til popplyl. § 2 nr. 7, da kravene i § 2 nr. 7 og § 19 skal ivareta de samme

---

[65] Informasjonsansvaret kan eventuelt delegeres til tredjemann.

[66] Jf. Datatilsynets retningslinjer på <http://www.datatilsynet.no/arkiv/brosjyrer/pol/samtykke.html> (13.10.2003).

personvernhensyn; nemlig at den registrerte skal ha full oversikt over behandling av opplysninger om seg selv, og de konsekvenser behandlingen kan medføre for vedkommende.

Forarbeidene presiserer i liten grad informasjonskravet etter popplyl. § 2 nr. 7. I Ot.prp. nr. 92 (1998-99) på side 104 er det kun uttalt at kravet om at samtykket skal være informert *"medfører at den registrerte må gis tilstrekkelig informasjon slik at vedkommende vet hva det samtykkes i"*. I NOU 1997: 19 på side 133 uttales at *"den registrerte må forstå hva erklæringen gjelder, og hvilke konsekvenser denne får eller kan få"*. Uttalelsene bærer lite preg av å oppstille så stringente retningslinjer som de Datatilsynet har publisert. Særlig tvilsomt er det at et samtykke vil bli underkjent fordi arbeidsgivers adresse ikke blir opplyst. Navnet på den behandlingsansvarlige bør likevel opplyses, slik at arbeidstakeren vet hvem han skal forholde seg til. Dette er imidlertid opplysninger som arbeidstakeren normalt allerede kjenner til, særlig i mindre bedrifter. Alternativet vil derfor neppe ha nevneverdig betydning her. De øvrige kravene i § 19, og således også i Datatilsynets retningslinjer, synes for så vidt å være velbegrunnede. For å forstå rekkevidden av samtykket er det en forutsetning at arbeidstakeren er klar over formålet med behandlingen, at han vet hvem som får tilgang til opplysningene, at det er frivillig å gi fra seg opplysningene og hvor lenge opplysningene vil bli behandlet eller oppbevart. I tillegg vil det være en åpenbar fordel at arbeidstakeren gis tilstrekkelig informasjon til å kunne ivareta sine øvrige rettigheter etter loven. Hvorvidt Datatilsynets retningslinjer følger av lovens formelle *krav* til et informert samtykke, er imidlertid tvilsomt. Det er lite trolig at domstolene vil følge en slik liste slavisk. Det sentrale er imidlertid, som nevnt ovenfor, (1) at den registrerte er klar over *hva* han samtykker i og (2) *hvilke konsekvenser* et samtykke vil medføre for han. Datatilsynets liste gir likevel gode holdepunkter for å klargjøre hvilke momenter som vil kunne bidra til å oppfylle de to kravene i forarbeidene.

Det antas videre at arbeidsgiver plikter å informere om mulige negative personvernmessige følger av samtykket.[67] Dette kan være en viktig forutsetning for å kunne forstå rekkevidden av et kontrolltiltak. Dersom arbeidsgiver ikke opplyser at de opplysninger som fremkommer av kontrolltiltaket kan få personalmessige konsekvenser for vedkommende, kan det lett tenkes at samtykket vil bli underkjent. Særlig må dette gjelde der formålet med kontrolltiltaket var nettopp å samle inn opplysninger som ville kunne ramme vedkommende på denne måten. En slik plikt vil trolig også kunne utledes av den ulovfestede *lojalitetsplikten* mellom partene i arbeidslivet.

3.2.4 Utrykkelig samtykke

Et krav om *utrykkelig* samtykke innebærer at det må fremgå klart og utvetydig av erklæringen at arbeidstakeren samtykker i den aktuelle typen kontrolltiltak/behandling. I forarbeidene er det videre lagt til grunn at det av erklæringen *skal fremgå* klart og utvetydig at samtykket er informert, jf. punkt 3.2.3.[68] Departementet brukte ikke her ordet "informert", men uttalte i stedet at det må fremgå klart at den registrerte vet hva slags behandling samtykket omfatter og hvilke behandlingsansvarlige det er rettet til. Etter min mening burde det fremgå klarere at disse kravene i realiteten er rubrisert inn under kravet til informasjon, og ikke egentlig til uttrykkelighetskravet. På den annen side er det nærliggende at uttrykkelighetskravet skal sikre at informasjonskravet er overholdt; erklæringen skal ikke etterlate tvil om hvorvidt kravene til informert samtykke er oppfylt.

Kravet om uttrykkelighet innebærer videre at det ikke holder med passivt eller stilltiende samtykke, og heller ikke samtykke gjennom konkludent atferd.[69] Det er således ikke tilstrekkelig at arbeidstakeren unnlater å reagere etter at arbeidsgiveren har varslet om eller iverksatt et kontrolltiltak. Uttrykkelighetskravet fordrer en viss aktivitet fra den registrerte for at samtykket skal oppfylle kravene i popplyl. § 2 nr. 7.

---

[67] Jf. uttalelsene i NOU 1997: 19 på side 133 om at den registrerte må få informasjon om hvilke konsekvenser erklæringen får eller kan få. Se også Norsk Lovkommentar, note 11 til popplyl. § 2 nr. 7, ved Dag Wiese Schartum.

[68] Jf. Ot.prp. nr. 92 (1998-99) på side 103.

[69] Jf. NOU 1997: 19 på side 133.

3.2.5 Forholdet mellom individuelt og kollektivt samtykke

I arbeidsrettslig teori og praksis har det vært lagt til grunn at kontrolltiltak i arbeidslivet kan reguleres gjennom kollektive avtaler mellom arbeidsgiver- og arbeidstakerorganisasjonene. Avtalene oppstiller visse rammer for maktforholdet mellom arbeidsgiver- og arbeidstakergruppene, og er bindende for de arbeidstakere som har den nødvendige organisasjonstilknytningen. Spørsmålet jeg skal ta for meg i dette avsnittet, er om et *kollektivt samtykke* tilfredsstiller personopplysningslovens krav til et gyldig samtykke.

Det kreves *i utgangspunktet* individuelt samtykke etter popplyl. § 8 (1), jf. § 2 nr. 7.[70] Dette følger for det første av at § 2 nr. 7 krever en erklæring *"fra den registrerte"*. For det annet er det eksplisitt uttalt i forarbeidene at samtykket i utgangspunktet skal være individuelt, jf. NOU 1997: 19 på side 133, jf. nedenfor. For det tredje synes det kollektive samtykket å være uforenlig med den selvråderett over personopplysninger som var av så sentral betydning under utarbeidelsen av direktivet og personopplysningsloven.

I forarbeidene er det åpnet for at interesseorganisasjonene kan binde sine medlemmer gjennom kollektive samtykker, men det fremgår klart at denne adgangen er ment å være snever. I Ot.prp. nr. 92 (1998-99) på side 103 uttaler departementet følgende:

> *"(...) et kollektivt samtykke, f. eks. et samtykke av en organisasjon på vegne av alle medlemmene, vil bare unntaksvis være tilstrekkelig (...)".*

På samme side vises til NOU 1997: 19 side 133, hvor følgende kommentarer er gitt:

> *"Endelig må samtykket være individuelt (jf. uttrykket den registrerte), dvs at den enkelte registrerte selv (eller ved fullmektig) må ha avgitt erklæringen. Et "kollektivt samtykke", f.eks. slik at en organisasjon samtykker på vegne av alle medlemmene, vil i utgangspunktet*

[70] Jf. Ot.prp. nr. 92 (1998-99) på side 103 og NOU 1997: 19 på side 133. Tilsvarende oppstiller direktivet i utgangspunktet krav om individuelt samtykke, jf. artikkel 2 bokstav h).

> *ikke tilfredsstille kravet med mindre omstendighetene rundt innmeldingen i organisasjonen gjør at innmeldingen i seg selv tilfredsstiller kravene til samtykke (dvs. slik at det tydelig fremgår at innmeldingen medfører behandling av personopplysninger, og innmeldingserklæringen er informert)."*

I underutvalgets rapport på side 27 uttales det at det ut fra *en arbeidsrettslig innfallsvinkel* ikke kan være tvilsomt at man gjennom de kollektive avtalemekanismene i arbeidslivet kan etablere kontrollmekanismer som er bindende for den samlede massen av organiserte arbeidstakere. Underutvalget uttalte videre i denne sammenheng:

> *"(...) Fullmakten som gis foreningen ved den enkelte arbeidstakers medlemskap, omfatter i utgangspunktet også samtykke til avtalefestede kontrollordninger. Etablering og utforming av kontrolltiltak gjennom tariffavtale vil i alminnelighet sikre en betryggende saksbehandling og en forsvarlig interesseavveining. Dette kan tale for at en bør gå forholdsvis langt i å akseptere tariffavtale som et rettslig grunnlag for kontrolltiltak i arbeidslivet. Men det går likevel en grense, særlig inngripende kontrolltiltak må sannsynligvis forankres i et individuelt samtykke."*

I sin artikkel om "Fjernarbeid", tar Jakhelln på sidene 156-157 utgangspunkt i forskriften til den tidligere personregisterloven, hvor det var fastsatt at det *"etter avtaler mellom partene i arbeidslivet"* kunne bestemmes at opplysninger om de ansatte kunne registreres i større grad enn det som fulgte av forskriftens øvrige bestemmelser.[71] Denne kollektive avtalefriheten, hvor ellers ufravikelige bestemmelser ble fraveket, måtte etter Jakhellns oppfatning være hjemlet i de ulovfestede arbeidsrettslige reglene. Bakgrunnen var at de store interesseorganisasjonene representerte slik tyngde og innsikt at de ville være bedre egnet til å forsvare arbeidstakernes interesser enn arbeidstakerne selv.

> En slik avtale ville – dersom interesseorganisasjonen/fagforeningen representerte et flertall av arbeidstakerne – etter Jakhellns oppfatning også være bindende for uorganiserte arbeidstakere.[72] Sistnevnte standpunkt stiller jeg meg kritisk til. Man har i Norge organisasjonsfrihet, og dette innebærer for det første at man har rett til å organisere seg

[71] Henvisning til forskriften § 2-1 nr. 2 bokstav d), § 2-1 nr. 3 bokstav b) og § 2-12 (2).

[72] Jakhelln tar imidlertid forbehold for de tilfeller kollektivavtalene er inngått mellom mindre organisasjoner, der disse ikke representerte et flertall av arbeidstakerne. I disse tilfellene mener han betenkelighetene med å godta kollektiv avtalefrihet er vesentlig større.

> (positiv organisasjonsfrihet) og for det annet en frihet til å velge å ikke gjøre det (negativ organisasjonsfrihet). Når arbeidstakerne velger å stå utenfor organisasjonsstrukturen i arbeidslivet, ville det stå i konflikt med hensynene bak organisasjonsfriheten om denne typen rammeavtaler også skulle være bindende for dem. Jakhellns artikkel ble imidlertid skrevet før personopplysningsloven ble vedtatt, og en slik løsning kan ikke forsvares overfor kontrolltiltak som omfattes av denne loven. Det er tvert i mot i forarbeidene lagt til grunn at et eventuelt kollektivt samtykke kun skal omfatte organisasjonens *medlemmer*. Et slikt synspunkt kan derfor *ikke lenger* legges til grunn, og etter min mening *bør* det heller ikke legges til grunn – til tross for at personopplysningsloven er en generell lov som ikke tar høyde for de særlige omstendigheter som gjør seg gjeldende i arbeidslivet. De lege ferenda bør heller ikke kollektive, avtalefestede kontrollordninger som *ikke* omfattes av personopplysningsloven, være bindende for uorganiserte arbeidstakere.

Det finnes flere hensyn som taler for å tillate kollektive samtykker innen arbeidslivet – uavhengig av om det rettslig sett skulle være uforenlig med personopplysningslovens regler. De store interesseorganisasjonene, eksempelvis LO og NHO, besitter et stort og ressurssterkt apparat, og balansen mellom rettigheter og plikter i avtalene mellom dem ofte er nøye avveid. Den enkelte uorganiserte arbeidstaker vil normalt ikke sitte i en tilsvarende maktposisjon i forhold til sin arbeidsgiver, og vil på denne bakgrunn kanskje lettere godta forskjellige inngrep i sin personlige integritet. Dette er en av de klareste fordelene med kollektiv avtaleregulering av kontrolladgangen. En ulempe er at det kan finnes arbeidstakere som ikke ønsker å bli utsatt for den aktuelle typen kontrolltiltak. Det kan tenkes en rekke kontrolltiltak i arbeidslivet som er meget inngripende ovenfor den enkelte, og det kan derfor være uheldig om kollektive organer ved flertallsbeslutninger skal kunne binde arbeidstakerne overfor arbeidsgiver på denne måten. Ut fra forarbeidenes uttalelser kan man imidlertid ikke utelukke at domstolene vil godta slike kollektive samtykker. Forarbeidene oppstiller likevel klare begrensninger i denne adgangen, jf. NOU 1997: 19 på side 133. Utvalget la her til grunn at en organisasjon kunne samtykke på vegne av sine medlemmer dersom *"omstendighetene rundt innmeldingen i organisasjonen gjør at innmeldingen i seg selv tilfredsstiller kravene til samtykke (...)"*. Utvalget synes å sikte til en slags videreformidling av et individuelt samtykke som i seg selv tilfredsstiller kravene i popplyl. § 2 nr. 7. Ved innmeldingen gis organisasjonen imidlertid en slags fullmakt til å samtykke til behandling av personopplysninger på vegne av sine medlemmer. Situasjonen er derfor ikke mye forskjellig fra de alminnelige fullmaktsforholdene, slik disse er beskrevet

ovenfor. Se også underutvalgets rapport på side 27, jf. sitatet ovenfor. Forutsetningen er at det *"tydelig fremgår at innmeldingen medfører behandling av personopplysninger, og innmeldingserklæringen er informert"*. For at organisasjonens fullmakt skal være gyldig, er det derfor krav om at den registrerte vet hva slags type behandling organisasjonen kan samtykke til, konsekvensene av samtykket og at innmeldingen innebærer en fullmakt for organisasjonen til å samtykke til behandling av personopplysninger. Det riktige må imidlertid være å kreve at også det kollektive samtykket er uttrykkelig, frivillig og informert. Kravene i popplyl. § 2 nr. 7 må i disse tilfellene også rettes mot organisasjonen i de tilfeller den opptrer på vegne av sine medlemmer.

Dersom en arbeidstaker ikke ønsker å gi organisasjonen en slik fullmakt, kan han la være å melde seg inn i organisasjonen, eventuelt melde seg inn med forbehold i så henseende. Et forbehold vil i sin tur måtte være bindende for organisasjonen. Tar vedkommende ikke forbehold, må man legge til grunn tilsvarende risikobetraktninger som nevnt i punkt 3.2.1 i forbindelse med bruk av fullmektig. Går organisasjonen utover sine fullmakter, eventuelt utover hva fullmaktsgiver ønsker i det enkelte tilfelle, må dette bli fullmaktsgivers risiko.

> Dersom man tillater at innmeldingen i organisasjonen gir organisasjonen fullmakt til å samtykke til kontrolltiltak på vegne av medlemmene, må man samtidig gi medlemmene mulighetene til å trekke samtykket tilbake. Reelle hensyn tilsier at dette i så fall kan skje ved en ensidig erklæring fra den registrerte, og at man ikke krever utmelding av organisasjonen. De rettslige spørsmålene som oppstår ved tilbakekall av samtykke er behandlet i neste punkt.

De lege lata må det konkluderes med at et kollektivt samtykke under visse omstendigheter er forenlig med personopplysningsloven, så fremt innmeldingen i organisasjonen innebærer en opprettelse av et slags fullmaktsforhold i så måte. Rekkevidden av et kollektivt samtykke er imidlertid et uavklart spørsmål, jf. også underutvalgets rapport på side 48. De lege ferenda bør adgangen ikke være særlig stor. I de tilfeller det er snakk om kontrolltiltak i arbeidslivet som kan få alvorlige personvernmessige følger, tilsier lovens formål og reelle hensyn at man burde kreve individuelt samtykke, jf. også sitatet fra underutvalgets rapport på side 27, jf. ovenfor.

Kontroll av e-post og datalogger i den hensikt å overvåke ansatte på arbeidsplassen, er et klart eksempel på behandlingstyper som bør kreve individuelt samtykke.[73]

3.2.6 Tilbakekall av samtykke

Et samtykke kan tilbakekalles når som helst av den registrerte, jf. Ot.prp. nr. 92 (1998-99) på side 104. Tilbakekallet har den konsekvens at den behandlingsansvarlige ikke lenger kan behandle personopplysninger om den registrerte, med mindre det foreligger et annet rettslig grunnlag for behandlingen.[74] Det rettslige grunnlaget kan således være bortfalt både i forhold til behandling av allerede innsamlede opplysninger og i forhold til innsamling av nye opplysninger. Dette følger forutsetningsvis av popplyl. § 8, da enhver behandling krever et selvstendig rettslig grunnlag. Behandlingen som har foregått i perioden mellom avgivelsen av samtykket og tilbakekallet vil imidlertid være lovlig.[75] Spørsmålet som skal drøftes i punkt 3.2.6, er hvilke rettslige konsekvenser et tilbakekall får for opplysninger om en arbeidstaker som allerede er samlet inn.

Samtykket etablerer en avtale mellom arbeidsgiver og arbeidstaker, og dersom vedkommende arbeidstaker skulle angre, er dette i utgangspunktet en risiko han selv må bære. Forfatterne av Kommentarutgaven hevder likevel på side 78 at det må være et visst rom for å feile, og at tilbakekallet vil kunne få betydning for allerede innsamlet materiale. På side 99 hevder de videre at behandlingen må stanses, og at opplysningene må anonymiseres eller slettes. Denne slutningen følger verken av ordlyden i popplyl. § 2 nr. 7 eller § 8, men følger forutsetningsvis av forarbeidene og andre bestemmelser i loven.

I NOU 1997: 19 gikk utvalget inn for en bestemmelse om retting, sletting eller supplering av mangelfulle personopplysninger, jf. lovforslaget § 25, jf. side 149-150 i

---

[73] Det finnes også andre rettslige grunnlag for behandlingen enn individuelt samtykke, eksempelvis lovhjemmel eller popplyl. § 8 bokstavene a) til f), jf. nedenfor.

[74] Jf. for så vidt departementets uttalelser omkring popplyl. § 8 bokstav f) i Ot.prp. nr. 92 (1998-99) på side 109.

[75] Jf. Ot.prp. nr. 92 (1998-99) på side 108.

utredningen. Sletting mv. skulle utføres av den behandlingsansvarlige dersom han hadde registrert opplysninger om den registrerte som var uriktige, ufullstendige eller som det ikke var adgang til å registrere. Departementet valgte å følge hovedtrekkene i utvalgets forslag, men endret likevel noe på utformingen av bestemmelsen i popplyl. § 27, jf. Ot.prp. nr. 92 (1998-99) på side 48. Utgangspunktet etter popplyl. § 27 (1) (”Retting av mangelfulle personopplysninger”), er at opplysningene skal *rettes* dersom de er uriktige, ufullstendige eller dersom det ikke er adgang til å behandle dem. I den situasjonen jeg har skissert ovenfor vil det være sistnevnte alternativ som er mest relevant, nemlig at det ikke er adgang til å behandle opplysningene.

> Ordlyden i første ledd synes ikke å være tilstrekkelig gjennomtenkt. Den lyder som følgende: *”Dersom det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, skal den behandlingsansvarlige av eget tiltak eller på begjæring av den registrerte rette de mangelfulle opplysningene”*. Det vil imidlertid ikke nødvendigvis være snakk om ”mangelfulle opplysninger” fordi det ikke var adgang til å behandle dem. Ordlyden må her tolkes slik at retteplikten også omfatter tilfeller hvor det ikke er snakk om mangelfulle opplysninger, men hvor det ikke foreligger noe rettslig grunnlag for behandlingen, jf. *”(...) eller som det ikke er adgang til å behandle (...)”*.
>
> Overskriften til bestemmelsen passer også dårlig i slike situasjoner. Heller ikke den kan gi grunnlag for å tolke § 27 (1) innskrenkende; det følger klart av ordlyden at bestemmelsen også omfatter retting av opplysninger som det ikke er adgang til å behandle.

Etter ordlyden er det *retting* som skal foretas i disse tilfellene. Begrepet legger etter min mening visse føringer om at det skal foretas en endring av opplysningene, ikke nødvendigvis at de skal fjernes. Når det ikke er adgang til å behandle opplysningene, vil imidlertid ikke en endring, supplering e.l. være tilstrekkelig for den registrerte. Ut fra departementets uttalelser i Ot.prp. nr. 92 (1998-99) på side 124 synes det imidlertid som om retting kan skje ved sletting. Dette synes også å være lagt til grunn i Kommentarutgaven på side 202, hvor følgende er skrevet:

> *”Den behandlingsansvarlige plikter også å slette opplysninger som det ikke er adgang til å behandle. Dette kan være opplysninger som den behandlingsansvarlige ikke hadde anledning til å samle inn, eller som opprinnelig var lovlig samlet inn, men vilkårene for å behandle dem senere har falt bort, jf. § 8 og § 9 (...)”*.

Departementet har i Ot.prp. nr. 92 (1998-99) på side 109 gitt en uttalelse som også støtter dette synet. Uttalelsen gjaldt i realiteten popplyl. § 8 bokstav f), men kan kanskje også få betydning for tolkningen av § 27 (1). Departementet drøftet betydningen av at den registrerte eksplisitt ga uttrykk for at han ikke ønsket at behandlingen skulle *"gjennomføres eller fortsette"*. Dette ville få betydning for avveiningen etter § 8 bokstav f), jf. punkt 3.4.3. Departementet uttaler ikke eksplisitt at det er snakk om tilbakekall av samtykke. At den registrerte uttrykker at han ikke ønsker at behandlingen skal *fortsette* kan imidlertid også omfatte tilbakekallstilfellene. Nedenfor uttaler departementet følgende:

> *"Hvis ikke behandlingen kan hjemles i noen av de andre vilkårene i §8, vil den behandlingsansvarlige i slike tilfeller måtte avstå fra å behandle opplysningene, eller slette eller avidentifisere opplysninger som allerede er behandlet (...)".*

Departementet oppgir ikke her hjemmelen for sletteplikten eller plikten til å avidentifisere opplysningene, men det er nærliggende å legge til grunn at det er § 27 (1) det siktes til. Det er imidlertid en lite tilfredsstillende løsning at det i første ledd er lagt til grunn at opplysningene skal rettes, mens de i visse tilfeller også skal slettes. At retting kan skje ved sletting er en ting. En annen sak er at man bruker både "retting" og "sletting" i lovteksten for øvrig. Tilsvarende er både "retting" og "sletting" benyttet i direktivet, jf. art. 12 bokstav b).[76] For de som skal anvende lovverket hadde det vært enklere om sletteplikten fremgikk eksplisitt av ordlyden i § 27 (1).

> På den annen side fremgår det for så vidt også av § 27 (3) at retting kan skje ved sletting. Etter denne bestemmelsen kan Datatilsynet (uten hinder av annet ledd) pålegge den behandlingsansvarlige å rette personopplysninger ved sletting eller sperring, dersom tungtveiende personvernhensyn tilsier det.

Dersom samtykket til behandlingen er trukket tilbake, men opplysningene er utlevert til en tredjemann, har den behandlingsansvarlige etter § 27 (1) annet punkt en plikt til (om

[76] Dette reiser spørsmål om departementet her har strukket begrepet "retting" noe langt i forhold til hva som følger av direktivet. Det vil imidlertid føre for langt å forfølge dette videre her.

mulig) å sørge for at "feilen" ikke får betydning for den registrerte. Dette kan skje ved at den som opplysningene er utlevert til, varsles om at opplysningene skal slettes. Se også direktivet art. 12 bokstav c). Det er imidlertid ikke noe i veien for at denne likevel kan behandle opplysningene dersom det foreligger et selvstendig rettslig grunnlag for dette, eksempelvis popplyl. § 8 bokstavene a) til f).

Retting av opplysninger som det ikke er adgang til å behandle, kan også skje ved *avidentifisering* av opplysningene, jf. sitatet ovenfor fra Ot.prp. nr. 92 (1998-99) på side 109. Avidentifisering innebærer at de deler av opplysningene som for så vidt gjør opplysningene til personopplysninger, jf. popplyl. § 2 nr. 1, skal fjernes. På denne måten vil opplysningene i og for seg kunne lagres, men det skal ikke være mulig å knytte dem til den opprinnelig registrerte. Slik vil også de personvernmessige konsekvensene av behandlingen (lagringen) minimaliseres. Dersom avidentifisering ikke lar seg gjøre i tilstrekkelig grad, skal opplysningene likevel slettes.

Retting skal etter ordlyden i popplyl. § 27 (1) skje *"av eget tiltak eller på begjæring av den registrerte"*. Dersom den behandlingsansvarlige på egen hånd er blitt klar over at opplysningene ikke lenger kan behandles, noe som normalt vil være tilfellet når et samtykke er trukket tilbake, skal han likevel rette opplysningene av eget tiltak. Dette følger ikke av lovteksten, jf. *"eller"*, men av at departementet i Ot.prp. nr. 92 (1998-99) på side 124 har lagt til grunn at rettingen *"skal skje av eget tiltak"* i disse tilfellene. Det er på denne bakgrunn ikke nødvendig at den registrerte ber om retting. Begjæring om retting kan imidlertid være praktisk viktig i de tilfeller opplysningene er *mangelfulle* eller *uriktige*, men hvor den behandlingsansvarlige ikke kjenner til disse omstendighetene.

Når arbeidsgiver har samlet inn opplysninger som kan gi grunnlag for strafferettslige eller arbeidsrettslige sanksjoner, kan opplysningenes *innhold* i visse tilfeller få betydning for den videre behandlingen – til tross for at samtykket er trukket tilbake.[77] Dersom opplysningene kan gi grunnlag for strafferettslige sanksjoner, er det normalt politiet som skal foreta de videre undersøkelsene. Det kan imidlertid tenkes at popplyl.

[77] Eksempler på arbeidsrettslige sanksjoner kan være oppsigelse eller avskjed.

§ 8 bokstav f) hjemler ytterligere undersøkelser også fra arbeidsgivers side. Videre kan bevis for illojalitet e.l. gi arbeidsgiver en *berettiget interesse* til å behandle opplysningene videre, en interesse som i visse tilfeller kan overstige hensynet til den ansattes personvern. Arbeidsgiver kan derfor etter omstendighetene fortsette behandlingen med hjemmel i § 8 bokstav f). Et alternativt hjemmelsgrunnlag kan således åpne for videre behandling, selv om samtykket er trukket tilbake. Det kan også tenkes at det forelå såkalt "dobbel hjemmel" for kontrolltiltaket allerede i utgangspunktet, eksempelvis ved at arbeidsgiver har innhentet samtykke i tilfeller hvor han kunne ha behandlet opplysningene med hjemmel i popplyl. § 8 bokstav f). At samtykket trekkes tilbake kan imidlertid få betydning for interesseavveiningen, i den betydning at terskelen for å godta behandlingen blir høyere.[78]

3.3 Hjemmel i lov

I dette avsnittet skal det redegjøres for behandling av personopplysninger med hjemmel i lov, jf. popplyl. § 8. Begrunnelsen for dette alternativet er at loven ikke skal oppstille tilleggsvilkår for å behandle personopplysninger når lovgiver allerede har bestemt at behandlingen er nødvendig for å vareta viktige samfunnsinteresser.[79] Tiltaket er i disse tilfellene ikke ulovlig – til tross for at det kanskje strider mot personopplysningslovens øvrige regler. Dette følger forutsetningsvis av personopplysningslovens system (se popplyl. § 5) og av *lex specialis-prinsippet.*[80]

Lov-/forskriftsbestemmelser som rettslig grunnlag for kontrolltiltak er også et alternativ til styringsretten etter det arbeidsrettslige regelverket. Arbeidsmiljøloven (aml.) og forskriftsverket inneholder bestemmelser som pålegger arbeidsgiver plikt til å sørge for et forsvarlig arbeidsmiljø – en plikt som i visse tilfeller omfatter gjennomføring av

---

[78] Jf. Ot.prp. nr. 92 (1998-99) på side 109, hvor departementet om avveiningen etter popplyl. § 8 bokstav f) uttaler at *"dersom en registrert gir den behandlingsansvarlige beskjed om at han eller hun ikke vil at behandlingen skal gjennomføres eller fortsette, bør dette tillegges vesentlig vekt"*.

[79] Jf. Ot.prp. nr. 92 (1998-99) på side 108.

[80] Prinsippet går i korthet ut på at særlovgivning går foran generell lovgivning.

helseundersøkelser på arbeidsplassen mv.[81] Tilsvarende plikter følger også av annen lovgivning.[82] Pr. i dag finnes imidlertid ingen bestemmelser som konkret hjemler arbeidsgivers adgang til å kontrollere arbeidstakernes e-post og datalogger. Det vil derfor føre for langt å redegjøre for særlovgivningen her. Det sentrale her er i stedet å redegjøre for hvilke krav som stilles til lovhjemmelen etter personopplysningsloven.

Forarbeidene til personopplysningsloven gir få holdepunkter for hva som skal til for å tilfredsstille lovskravet i popplyl. § 8. Om behandlingen har tilstrekkelig lovhjemmel må imidlertid alltid avgjøres ved tolkning av den aktuelle loven, og vurderingen må foretas i forhold til den aktuelle behandlingssituasjonen. Kravet er relativt, i den forstand at jo viktigere personvernhensyn som kommer inn i bildet, desto strengere er kravet til klarhet i den aktuelle lovbestemmelsen, jf. Ot.prp. nr. 92 (1998-99) på side 108 og NOU 1997: 19 på side 139.[83] Lovteksten bør uttrykkelig bestemme hvem som er behandlingsansvarlig, jf. NOU 1997: 19 på side 132, annen spalte. Reelle hensyn taler også for at hjemmelen bør inneholde en klar angivelse av hva slags type behandling som er tillatt, samt av hvilke opplysningstyper som tillates behandlet. Dersom personvernspørsmål er drøftet i forarbeidene til hjemmelsloven, vil dette spille inn i vurderingen.[84] I de tilfeller loven klart uttrykker at et særskilt kontrolltiltak er lovlig, eller de tilfeller hvor arbeidsgiver i lov *pålegges* å utføre visse kontrolltiltak (se for eksempel aml. § 11 nr. 2), er saken grei. Arbeidsgiver kan da utføre kontrolltiltaket med hjemmel i særlovgivningen, jf. popplyl. § 8. Det kan imidlertid tenkes tilfeller hvor det kun foreligger implisitt hjemmel for kontrolltiltaket. Hvordan stiller dette seg da til personopplysningslovens krav til lovhjemmel? Den rettslige vurderingen vil da avhenge

---

[81] Se for eksempel aml. § 11 nr. 2 og § 14 bokstav c). Aml. § 11 nr. 2 pålegger virksomheter som bruker eller oppbevarer giftige eller helsefarlige stoffer en plikt til å foreta fortløpende kontroller av de ansattes helse. Aml. § 14 bokstav c) pålegger arbeidsgiver en plikt til å foreta fortløpende kontroller med de ansattes helse i tilfeller hvor arbeidsmiljøet på sikt kan påføre dem helseskader.

[82] Se for eksempel smittevernloven § 3-2 (jf. eksempelvis forskrift av 5/7 1996 nr. 700 om forhåndsundersøkelser av arbeidstakere i helsevesenet) og sjømannsloven § 26.

[83] Uttalelsen i NOU 1997: 19 gjelder i utgangspunktet behandling av sensitive personopplysninger, jf. lovforslagets § 9, men gode grunner taler for at tilsvarende også må kunne legges til grunn i forhold til lovskravet i popplyl. § 8.

[84] Jf. uttalelsen i NOU 1997: 19 på side 140, som også gjelder sensitive personopplysninger.

av kontrolltiltakets alvorlighetsgrad. Er hjemmelen "svak" og tiltaket meget krenkende overfor arbeidstakeren, vil det neppe godtas etter popplyl. § 8, jf. popplyl. § 1 og Ot.prp. nr. 92 (1998-99) på side 108. Legalitetsprinsippet setter også grenser for hvor svak rettslig forankring et kontrolltiltak kan ha. Er det få personvernmessige innvendinger mot kontrolltiltaket, taler dette imidlertid for å godta også implisitte lovhjemler som rettslig grunnlag.[85]

> Hvis man skal bruke kontroll av e-post og logger som eksempel, er dette tiltak som nok ville kreve klar lovhjemmel. Dette er en form for kontrolltiltak som normalt vil oppleves som meget inngripende overfor arbeidstakeren. Er det derimot snakk om innsamling av e-post adresser via internett for kommersiell bruk, vil dette i de fleste tilfeller innebære behandling av personopplysninger som ikke antas å være særlig inngripende overfor den enkelte.[86]

Dersom den behandlingsansvarlige ønsker å behandle opplysninger utover det som er tillatt etter særlovgivningen, må denne delen av behandlingen ha et selvstendig rettslig grunnlag.[87]

3.4 Nødvendighetskriteriet i popplyl. § 8

3.4.1 Innledning

For at et kontrolltiltak skal anses lovlig i de tilfeller hvor det verken foreligger samtykke eller konkret lovhjemmel, må minst ett av vilkårene i popplyl. § 8 bokstavene a) til f) være oppfylt. Fellesnevneren i a) til f) er at det etter alle bestemmelsene foreligger et *nødvendighetskrav*.[88] Det er arbeidsgiver som i første omgang må vurdere hvorvidt

---

[85] I disse tilfellene vil popplyl. § 8 bokstav f) også kunne gi arbeidsgiver tiltrekkelig hjemmel.

[86] Det siste eksemplet er ikke relevant i forhold til kontroll og overvåking på arbeidsplassen, og er kun brukt for å illustrere et tilfelle hvor også implisitte lovhjemler kan være tilstrekkelig.

[87] For eksempel popplyl. § 8 bokstavene a) til f) eller samtykke.

[88] Innholdet i nødvendighetskravet kan variere noe, avhengig av hvilke av bokstavene man knytter det opp mot. Teoretisk sett kan det således oppstilles 6 forskjellige nødvendighetskrav (a-f). Dette er

kontrolltiltaket er nødvendig eller ikke, og har bevisbyrden i så henseende. Datatilsynet kan imidlertid overprøve arbeidsgivers vurdering, jf. popplyl. § 46.

Nødvendighetskravet fordrer en konkret og skjønnsmessig vurdering i hver enkelt behandlingssituasjon. Forarbeidene nevner eksempelvis at en behandling kan være nødvendig dersom det er snakk om *innsamling*, men at det kanskje ikke er nødvendig med *utlevering.*[89] Begge deler omfattes av behandlingsbegrepet. Nødvendighetsbegrepet er ikke behandlet særlig inngående i forarbeidene til personopplysningsloven.[90] Det er understreket at begrepet åpner for bruk av skjønn, og at Datatilsynet er tiltenkt en sentral rolle i utformingen av innholdet i nødvendighetskravet, jf. Ot.prp. nr. 92 (1998-99) på side 108. Om bestemmelsene i popplyl. § 8 bokstavene a) til f) og nødvendighetsavveiningen er det uttalt at *"på sikt vil tilsynets praksis kunne utfylle de skjønnsmessige bestemmelsene og lette anvendelsen av dem (...)"*. Dette er etter min oppfatning en noe uheldig løsning. I forhold til kontrolltiltak i arbeidslivet vil hjemmelen ofte være popplyl. § 8 bokstav a) og/eller bokstav f), og det vanskeliggjør en fornuftig avveining når et så sentralt begrep ikke er presisert ytterligere i forarbeidene. Praksis fra Datatilsynet er i tillegg relativt vanskelig tilgjengelig, og det er ikke gitt at de ulike samfunnsaktørene kjenner til den.

Først og fremst må begrepet nødvendighet sies å oppstille visse *kvalifikasjonskrav*. Etter en rent språklig fortolkning, innebærer nødvendighetskravet at det må foreligge et reelt og kvalifisert behov for behandlingen av personopplysninger. Det er neppe krav om at behandlingen er eneste mulige alternativ, men det vil sjelden kunne være tilstrekkelig at den kun er hensiktsmessig.[91] Etter min mening vil behandlingens *saklighet* kunne være

---

imidlertid lite praktisk i forhold til denne avhandlingen. Oversikten nedenfor er generell, og bør kunne overføres til samtlige bokstavalternativer i § 8.

[89] Ot.prp. nr. 92 (1998-99) på side 108.

[90] Etter det jeg kjenner til finnes det heller ikke norsk rettspraksis som oppstiller retningslinjer for forståelsen av nødvendighetsbegrepet.

[91] Jf. også NOU 2003: 21 ("Kriminalitetsbekjempelse og personvern – politiets og påtalemyndighetenes behandling av personopplysninger") på side 170. Utvalget behandlet nødvendighetskravet generelt, og både i forhold til personopplysningsloven § 8 og forslaget til ny politiregisterlov. På samme side i utredningen blir kravet omtalt som et rettslig prinsipp, *"nødvendighetsprinsippet"*.

et sentralt moment i nødvendighetsvurderingen. Saklighetskravet er utførlig behandlet i kapittel 4, og vil derfor kun bli behandlet overfladisk her. Kravet innebærer i korthet at behandlingen må være egnet til å oppnå formålet med den, begrunnelsen for og formålet med behandlingen må være forsvarlig og det må foreligge et reelt behov. Rent språklig kan det ikke være tvil om at et krav om saklighet kan innfortolkes i nødvendighetsbegrepet. Man kan vanskelig tenke seg et tilfelle hvor kontrolltiltaket er usaklig, men hvor det likevel anses nødvendig etter § 8 bokstavene a) til f).

> Henning Jakhelln har uttrykt at et krav om nødvendighet også fulgte av det generelle saklighetskravet i den tidligere personregisterlovens § 6 (1).[92] Dette er en noe annen tilnærming til spørsmålet enn det jeg har valgt; Jakhelln hevder at det i kravet til saklighet også ligger et krav om nødvendighet, mens jeg her har antydet at det i kravet om nødvendighet også ligger et krav til saklighet. Den reelle forskjellen er imidlertid av liten praktisk betydning, og det kan tenkes at begrepene glir over i hverandre på en slik måte at det ikke er hensiktsmessig å operere med noe hoved- og underbegrep.
>
> Nå er det uansett slik at et krav om saklighet følger av en annen bestemmelse i samme lovkapittel. Etter § 11 bokstav b) kreves at behandlingen av personopplysninger må være basert på uttrykkelig angitte formål som er *saklig* begrunnet i den behandlingsansvarliges virksomhet. Vilkårene i § 11 er kumulative i forhold til § 8, dvs. at alle vilkårene i § 11 må være oppfylt i tillegg til at det foreligger et rettslig grunnlag for behandlingen. Dersom man *ikke* innfortolker saklighetskravet i § 8, og et kontrolltiltak fremstår som nødvendig etter et av de alternative grunnlagene i bokstav a) til f), er tiltaket likevel ikke rettmessig dersom det ikke er saklig begrunnet i arbeidsgivers virksomhet. Se nærmere om dette i pkt. 4.2.3.

I tillegg til et krav om saklighet, følger det etter min mening av begrepet *nødvendig* også en begrensning med hensyn til omfanget av behandlingen. Nødvendighetsbegrepet krever en form for forholdsmessighetsvurdering, og inngrepets karakter vil derfor være sentral i den rettslige vurderingen av behandlingen.[93] Tiltaket vil ikke være nødvendig i snever forstand dersom den behandlingsansvarlige går ut over det som kreves for å oppnå formålet med behandlingen. Med andre ord kan kravet sies å innebære at den behandlingsansvarlige plikter å anvende det tiltak som innebærer minst mulig

---

[92] Se ”Fjernarbeid” på side 153.

[93] Jf. NOU 2003: 21 på side 171.

belastning for den registrerte. En slik fortolkning stemmer også godt overens med lovens formål, jf. popplyl. § 1. Man ser således parallellen til *proporsjonalitetsprinsippet*, se punkt 4.3 nedenfor. Proporsjonalitet og nødvendighet er i utgangspunktet to forskjellige krav, men innholdet i de glir til en viss grad over i hverandre, slik at kravet om nødvendighet også stiller visse krav til behandlingens proporsjonalitet. Den behandlingsansvarlige vil således heller ikke kunne tilegne seg overskuddsinformasjon; han plikter å stoppe innsamlingen i det øyeblikk han har tilegnet seg tilstrekkelig informasjon til å oppnå formålet med behandlingen. Går den behandlingsansvarlige utover hva som anses nødvendig, kreves et selvstendig rettsgrunnlag for denne delen av behandlingssituasjonen. Som nevnt har departementet uttalt at nødvendighetskravet også begrenser hva slags type behandling som er tillatt, jf. eksemplet om at innsamling kunne være nødvendig, mens utlevering av opplysningene ville kunne være unødvendig sett hen til formålet med behandlingen. På tilsvarende måte kan det i en konkret sak være nødvendig med kontroll av *trafikkdataene* i bedriftens aktivitetslogger, mens kontroll av *innholdet* i de ansattes e-post ikke vil være nødvendig.[94]

I de påfølgende avsnitt skal det drøftes i hvilken grad nødvendighetsalternativet kan hjemle kontrolltiltak i arbeidslivet. Jeg har valgt å avgrense den videre redegjørelsen mot popplyl. § 8 bokstavene b) til e).[95] Bestemmelsene i § 8 bokstavene a) og f) synes å være de mest relevante bestemmelsene i forhold til denne avhandlingens tema, og disse skal behandles i punkt 3.4.2 og 3.4.3.

3.4.2 Popplyl. § 8 bokstav a)

Popplyl. § 8 bokstav a) hjemler behandling av personopplysninger i de tilfeller hvor det er nødvendig for å *"oppfylle en avtale med den registrerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås"*. En avtale med den registrerte kan

---

[94] Begrepet "trafikkdata" er beskrevet nærmere i fotnotene til punkt 5.1.1 nedenfor.

[95] Popplyl. § 8 bokstav b) til e) hjemler behandling av personopplysninger når dette er nødvendig; for at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse (bokstav b), for å vareta den registrertes vitale interesser (bokstav c), for å utføre en oppgave som er av allmenn interesse (bokstav d) og for å utøve offentlig myndighet (bokstav e).

være så mangt; i Kommentarutgaven er det eksempelvis pekt på avtaler om bestilling av varer mellom en behandlingsansvarlig og en registrert.[96] Behandlingen av personopplysningene utgjør ikke grunnlaget for avtalen, men opplysningene utgjør viktige forutsetninger for gjennomføringen av den. Det blir pekt på navn, adresse, ordrebekreftelser, faktura mv., jf. også Ot.prp. nr. 92 (1998-99) på side 109. Annet alternativ i bokstav a) omhandler behandling som er nødvendig for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås.[97] Dette alternativet vil typisk kunne komme til anvendelse ovenfor arbeidssøkende e.l. Avhandlingen er sentrert rundt eksisterende arbeidsforhold, og alternativet vil derfor ikke bli behandlet videre her. Spørsmålet som skal drøftes i det følgende er hvorvidt første alternativ i bokstav a) kan regulere adgangen til å foreta kontrolltiltak i arbeidslivet.

I underutvalgets rapport om kontroll og overvåking i arbeidslivet er følgende uttalt om denne bestemmelsen:

> *"Ved siden av samtykke er det først og fremst alternativene i § 8 a og f som er særlig aktuelle i arbeidsforhold. (...). Førstnevnte alternativ gjelder blant annet arbeidsavtaler (...)".*[98]

Det er tydelig at underutvalget har lagt til grunn at bestemmelsen er relevant i arbeidslivet. Det er trolig korrekt at en slik avtale kan være en arbeidsavtale. Men i hvilke tilfeller må det anses å være nødvendig med *kontroll* av e-post og datalogger for å kunne oppfylle en arbeidsavtale?

Det kan tenkes at det i arbeidsavtalen er inntatt klausuler som åpner for at arbeidsgiver kan sjekke arbeidstakerens e-post i forbindelse med at arbeidstakeren er syk, på ferie eller av andre grunner ikke er til stede. Arbeidsgiver kan følgelig ha en legitim interesse i å gjøre dette for å kunne opprettholde den ansattes virksomhetsrelaterte aktiviteter,

---

[96] Se side 100.

[97] I forarbeidene har departementet påpekt at behandling kredittopplysninger om den registrerte kan omfattes av denne bestemmelsen, dersom disse innhentes i forbindelse med tilbud om lån (finansieringsvirksomhet) e.l., jf. Ot.prp. nr. 92 (1998-99) på side 109.

[98] Se underutvalgets rapport på side 42.

eksempelvis i forhold til bedriftens samarbeidspartnere, kunder e.l. Men i de tilfeller adgangen er avtalebasert vil det kanskje være snakk om *rett til innsyn* i e-post snarere enn et typisk *kontrolltiltak*.

En annen tenkelig situasjon er hvor arbeidsgiveren – i kraft av å være systemansvarlig – har ansvaret for informasjonssikkerheten på arbeidsplassen. Datavirus, inngrep fra datahackere, tekniske feil mv., kan innebære en trussel for denne informasjonssikkerheten. Gitt at arbeidsgiver ved viruskontroll oppdager at en av sine ansatte har mottatt e-post med et hissig datavirus, eller at det oppdages at noen har "brutt seg inn" på hjemmeområdet til en av de ansatte. Det er ikke vanskelig å se at behovet for innsyn i e-post og logger da er til stede. Dersom arbeidsgiver og arbeidstaker har en avtale om at denne typen trusler mot informasjonssikkerheten er arbeidsgivers ansvar, vil antakelig innsyn i e-post og logger kunne hjemles i popplyl. § 8 bokstav a).[99] Arbeidsavtalen kan også ha klausuler som eksplisitt hjemler innsyn i disse tilfellene. Men også her vil det da snarere være snakk om en innsynsrett fremfor et kontrolltiltak.

Ovenfor er det nevnt et par eksempler hvor *innsyn* i e-post og logger er hjemlet i arbeidsavtalen, og hvor § 8 bokstav a) kan gi arbeidsgiver tilstrekkelig rettslig grunnlag for behandlingen. I disse eksemplene vil behandlingen normalt kunne innebære en fordel for arbeidstakerne. Bestemmelsen lyder *"for å oppfylle en avtale med den registrerte (...)"*, noe som rent intuitivt bringer tankene over i at den behandlingsansvarlige behandler personopplysninger for å utføre sine *plikter* etter avtalen. Det fremgår imidlertid ikke av ordlyden at behandlingen etter bokstav a) må innebære en fordel for den registrerte for å være tillatt, eller at den kun regulerer utøvelse av plikter ovenfor vedkommende. Det kan tenkes at bestemmelsen også omfatter utøvelse av *rettigheter* etter avtalen, og at den derfor også kan hjemle *kontrolltiltak* i arbeidslivet. Popplyl. § 8 bokstav a) bygger på og gjennomfører direktivets art. 7 bokstav b), men direktivet gir liten veiledning her.

---

[99] Selve loggingen er unntatt fra reglene om meldeplikt i de tilfellene hvor den skjer for å *"avdekke/oppklare brudd på sikkerheten i edb-systemet"*, jf. personopplysningsforskriften § 7-11 (2) bokstav b). Se punkt 5.1 flg.

Direktivbestemmelsen fastslår at behandling av personopplysninger bare kan utføres dersom *"behandlingen er nødvendig for å oppfylle en kontrakt som den registrerte er part i, eller for å iverksette tiltak på dennes anmodning før kontraktsinngåelsen (...)"*. Departementet har ikke behandlet spørsmålet, men forarbeidene stenger i hvert fall ikke eksplisitt for å tolke bestemmelsen dit hen at § 8 bokstav a) første alternativ også regulerer den behandlingsansvarliges rettigheter etter arbeidsavtalen. Det er ingen uttalelser der som tyder på at departementet har ment å begrense bestemmelsens rekkevidde i så henseende. Nedenfor gis derfor et par eksempler hvor bestemmelsen kan tenkes å hjemle kontroll av e-post og logger på arbeidsplassen, under forutsetningen av at § 8 bokstav a) første alternativ omfatter utøvelse av så vel rettigheter som plikter.

Én tenkelig situasjon er hvor arbeidsgiver har nedlagt forbud mot bruk privat bruk av IT-utstyr på arbeidsplassen. Forbudet kan være nedfelt i selve arbeidsavtalen, eller være gitt i interne instrukser e.l. i kraft av styringsretten. Hvis arbeidsgiver deretter får mistanke om brudd på dette forbudet, må han kunne utøve sine rettigheter etter arbeidsavtalen ved å kontrollere *trafikkdataene* i e-postloggene, samt loggene forøvrig. (Som det vil bli redegjort for i punkt 5.2 flg., er det ikke adgang til å kontrollere *innholdet i* privat e-post uten samtykke fra arbeidstakeren). Det kan også tenkes at partene i arbeidsavtalen har avtalt konkret at brudd på arbeidsreglementet, straffelovgivning e.l. utløser en rett til å kontrollere e-postloggene og de øvrige dataloggene. Dersom slike brudd oppdages vil et påfølgende kontrolltiltak være direkte hjemlet i arbeidsavtalen, og således også i § 8 bokstav a).

> Ved at partene har avtalt at arbeidsgiver kan foreta kontrolltiltakene, er det nærliggende å se på avtalen som en form for "samtykke til kontroll". Det kan derfor reises spørsmål om det er nødvendig å gå veien om bokstav a). Nå har det seg imidlertid slik at de formelle kravene til et samtykke i § 2 nr. 7 er forholdsvis strenge, og det er ikke gitt at disse er oppfylt i hvert enkelt tilfelle. Behovet for å påberope seg bokstav a) kan derfor likevel sies å være til stede.[100] Dersom disposisjonen likevel tilfredsstiller kravene i popplyl. § 2 nr. 7, vil også innholdet i den private e-posten kunne kontrolleres, jf. punkt 5.2.1. Kontrolltiltaket vil således være hjemlet i både et samtykke og i § 8 bokstav a).

[100] På den annen side vil situasjonen kunne fanges opp av "sekkebestemmelsen" i popplyl. § 8 bokstav f). Det er imidlertid ikke noe i veien for å behandle personopplysninger med "dobbelt hjemmel".

Det finnes foreløpig ingen publiserte rettsavgjørelser hvor popplyl. § 8 bokstav a) har blitt behandlet. Den konkrete rekkevidden av og innholdet i bestemmelsen er derfor uavklart. De lege ferenda er det imidlertid grunn til å innfortolke en rett for den behandlingsansvarlige til å utøve både rettigheter og plikter etter avtalen, slik at arbeidsgiver kan behandle personopplysninger om sine ansatte for å håndheve arbeidsavtalens bestemmelser, jf. mine eksempler ovenfor. En forutsetning for at § 8 bokstav a) skal kunne hjemle kontrolltiltak, er likevel at behandlingen av personopplysninger er *nødvendig*, og at lovens øvrige krav til behandlingen er oppfylt (eksempelvis grunnkravene i popplyl. § 11). I tillegg kan det tenkes at ulovfestede arbeidsrettslige prinsipper kommer inn som selvstendige begrensninger, jf. kapittel 4.

3.4.3 Popplyl. § 8 bokstav f)

Popplyl. § 8 bokstav f) er kanskje den mest interessante bestemmelsen i forhold til denne avhandlingens tema. Etter denne bestemmelsen kan den behandlingsansvarlige, eventuelt tredjepersoner som opplysningene utleveres til, behandle opplysninger om den registrerte i de tilfeller hvor dette er nødvendig for å ivareta en berettiget interesse, og hvor hensynet til den registrertes personvern ikke overstiger denne interessen.[101] Både *"nødvendig" og "berettiget interesse"* må drøftes i forhold til vurderingen av kontrolltiltakets rettmessighet – i tillegg til at fordelene og ulempene med kontrolltiltaket må veies mot hverandre.[102] I avveiningen mellom den behandlingsansvarliges og den registrertes interesser, vil kravene til saklighet og proporsjonalitet komme inn som sentrale momenter. Bestemmelsen er en sekkebestemmelse, og vil derfor til dels overlappe de øvrige alternativene i § 8 bokstavene a) til e), jf. Ot.prp. nr. 92 (1998-99) på side 109. På samme side er følgende uttalt om denne bestemmelsen:

---

[101] Bestemmelsen omfatter således også situasjoner der arbeidsgiver ikke selv har en tungtveiende/berettiget interesse, men hvor denne kan samle inn opplysninger på vegne av en tredjeperson som har en *berettiget interesse*. En tredjeperson som får opplysningene likestilles altså med den behandlingsansvarlige, jf. Ot.prp. nr .92 (1998-99) på side 109. En slik tredjemann kan for eksempel være en potensielt ny arbeidsgiver. Bestemmelsen gjennomfører personverndirektivet art. 7 bokstav f).

[102] Nødvendighetsbegrepet er drøftet i punkt 3.4.1.

"(...) Om behandlingen er tillatt eller ikke, avhenger av en avveining av den behandlingsansvarliges interesser i å gjennomføre behandlingen mot den registrertes interesse i at behandlingen ikke gjennomføres. På begge sider må både fordeler og ulemper med behandlingen tas i betraktning. Generelt må hensynet til privatlivets fred tillegges betydelig vekt i avveiningen mot kommersielle interesser. Dersom en registrert gir den behandlingsansvarlige beskjed om at han eller hun ikke vil at behandlingen skal gjennomføres eller fortsette, bør dette tillegges betydelig vekt (...)".

Selve begrepet *"berettiget interesse"* er ikke definert i forarbeidene, og litteraturen og rettspraksis er også sparsom på dette feltet.

I Høyesteretts kjæremålsutvalgs kjennelse av 22. november 2002, Rt. 2002 side 1500, gikk retten forholdsvis kortfattet inn på vurderingen av *berettiget interesse* i § 8 bokstav f). Kjæremålsutvalget sentrerte imidlertid drøftelsen rundt forholdet mellom virksomhetsrelatert og privat e-post, jf. punkt 5.2 nedenfor. Borgarting lagmannsrett hadde lagt til grunn at sondringen mellom privat- og virksomhetsrelatert e-post var sentral i forhold til kravet om *berettiget interesse*, noe kjæremålsutvalget sluttet seg til.[103]

Uavhengig av hva som vil være den rette forståelsen av *berettiget interesse*, er jeg av den oppfatning at begrepet i seg selv vil ha liten selvstendig betydning. Det mest sentrale i popplyl. § 8 bokstav f) synes å være den interesseavveining som skal foretas mellom hensynet til arbeidsgivers og arbeidstakers interesser for øvrig; altså avveiningen mellom fordelene for arbeidsgiver og ulempene for arbeidstaker. *Berettiget* har imidlertid den betydning at den legger visse føringer på hva slags interesser på arbeidsgivers side som er relevante i avveiningen. Ikke enhver interesse vil kunne gi grunnlag for kontrolltiltak. Blant annet vil arbeidsgivers interesse i å drive generell overvåking av arbeidstakerne neppe være berettiget, med mindre virksomheten er av en slik art at overvåking er strengt påkrevd. Normalt vil heller ikke overvåking begrunnet i et ønske om å si opp eller avskjedige enkelte arbeidstakere anses berettiget, med mindre

[103] Se LB-2002-02299.

overvåkingen er begrunnet i konkrete mistanker om straffbare forhold, jf. eksempelvis RG 2002 side 162, jf. nedenfor.

Uttalelsene i Ot.prp. nr. 92 (1998-99) på side 109, jf. ovenfor, gir liten veiledning utover ordlyden i § 8 bokstav f) i forhold til interesseavveiningen. Det er imidlertid understreket at hensynet til privatlivets fred må veie tungt i avveiningen mot arbeidsgivers kommersielle interesser. Dette vil særlig ha betydning i forhold til kontrolltiltak som tar sikte på å måle arbeidstakernes effektivitet e.l. Dataloggene kan gi arbeidsgiver en pekepinn på hvilke internettsider arbeidstakerne har vært inne på, hvor ofte de er inne på sider som ikke er jobbrelaterte, hvor mye tid som brukes på privat e-post osv. Slike effektivitetsmålinger kan trolig rubriseres under begrepet *kommersielle interesser*. Uttalelsene bærer med andre ord bud om at kontroll av e-post og logger ikke kan foretas for å kartlegge effektivitet på arbeidsplassen i de tilfeller viktige personvernhensyn taler i mot det. Effektivitetsmålinger er imidlertid kun ett eksempel på kommersielle interesser, og det vil kunne være en lang rekke kontrolltiltak som kan tenkes å være uforenlige med personopplysningsloven ut fra denne uttalelsen i forarbeidene. Uttalelsen sier imidlertid ikke eksplisitt at hensynet til privatlivets fred vil måtte gå foran kommersielle interesser – kun at førstnevnte hensyn vil måtte tillegges betydelig vekt. Det kan derfor tenkes at departementet her kun ønsket å understreke at selv betydelige økonomiske interesser *etter omstendighetene* vil måtte vike for hensynet til den enkeltes personvern. I avveiningen vil lovens formål komme inn som viktig tolkningsfaktor. Loven er ment å skulle styrke den enkeltes personvern, jf. § 1, og det er derfor også her gitt føringer for at personverninteressene vil måtte veie tungt.

Departementet uttaler videre på side 109 at arbeidstakerens oppfatning av inngrepet vil ha betydelig vekt. Dersom arbeidstakeren føler inngrepet krenkende, og sier fra om dette, vil terskelen for å påvise interesseovervekt i favør av arbeidsgiver være høyere. Tilsvarende synspunkt er lagt til grunn i de tilfeller hvor samtykke er forsøkt innhentet, men nektet.

Mengden av rettsavgjørelser omkring § 8 bokstav f) er foreløpig for liten til at man har fått oppstilt noen klare retningslinjer for avveiningen mellom de motstridende interessene. Nedenfor gis et par *praktiske eksempler* hvor problemstillingen har dukket

opp, og disse kan illustrere den avveining som vil måtte foretas etter popplyl. § 8 bokstav f).[104]

I ett tilfelle hadde en arbeidstaker – i arbeidstiden og med arbeidsgivers IT-utstyr – "surfet" på en rekke grovt pornografiske sider, og registrert sin jobbrelaterte e-post adresse på flere av disse. Arbeidsgiver hadde nedlagt et klart forbud i bedriftens interne instrukser mot surfing på pornografiske websider. Registreringens formål var i fremtiden å kunne motta e-post med pornografisk innhold fra leverandøren av siden. Arbeidsgiver ble ved en tilfeldighet oppmerksom på disse aktivitetene, og fikk undersøkt vedkommendes e-postlogger. Der fremgikk det at vedkommende allerede hadde mottatt e-post med pornografiske vedlegg, og at arbeidsgivers domenenavn var registrert hos leverandørene av disse sidene. Noen tilsvarende problemstilling har ikke blitt behandlet av domstolene, men min oppfatning av de rettslige spørsmålene er likevel klar. I dette tilfellet hadde arbeidstakeren knyttet bedriftens navn opp mot sider som etter manges oppfatning er moralsk forkastelige. E-post adressen var registrert på en e-post liste, noe som gjorde det mulig å knytte bedriftens navn til den type virksomhet som de ulike leverandørene drev. Bedriftens navn og rykte kunne derfor bli forbundet med denne typen virksomhet, noe som kunne skade bedriftens renommé.[105] I dette tilfellet vil arbeidsgiver etter min oppfatning kunne ha en klar og *berettiget interesse* i å kunne kontrollere loggene. Det kan også tenkes at kontrolltiltaket ville vært omfattet av bokstav a), jf. eksemplene i punkt 3.4.2, da forholdet også innebar et klart brudd på bedriftens interne instrukser.

---

[104] Eksemplene er gitt i anonymisert form av advokater som jobber innenfor dette fagområdet. Avveiningen etter det første eksemplet blir noe forskjellig fra det andre eksemplet, da førstnevnte gjelder brudd på arbeidskontrakten, mens sistnevnte i tillegg gjelder brudd på straffelovgivningen. Personvernhensyn vil lettere måtte vike når straffelovgivningen er brutt, jf. Oslo tingretts dom av 24.04.2002 (Oslo Sporveier) og RG 2002 side 162.

[105] Eksempelvis kan det tenkes at arbeidstaker@firma.no finnes i et register hos leverandøren av siden, og at dette registeret er tilgjengelig for både leverandøren og øvrige brukere av siden. I de tilfeller e-post adressene er synlige i adressefeltet, og samtlige mottakere dermed kan se hvem som har mottatt e-post fra den aktuelle leverandøren, vil arbeidsgivers interesse i å få kontrollert og stoppet aktivitetene være særlig fremtredende.

En annen sak gjaldt et tilfelle hvor arbeidsgiver ble gjort oppmerksom på at en av de ansatte hadde hatt befatning med barnepornografisk materiale på bedriftens datamaskin. Arbeidsgiver tok deretter utskrift av loggene, og disse viste at store mengder barnepornografi var lagret på bedriftens server. Besittelse av barnepornografi er ikke bare moralsk forkastelig, men også straffbart, jf. straffeloven § 204. Saken har ikke vært behandlet i domstolsapparatet, men etter min oppfatning vil arbeidsgiver også i et slikt tilfelle ha en klar og berettiget interesse i kunne kontrollere dataloggene. Se i denne sammenheng Oslo tingretts dom av 24.04.2002 (Oslo Sporveier) og RG 2002 side 162, jf. nedenfor. Arbeidsgiver kan straffes etter straffeloven § 204 (3) dersom han unnlater å forhindre befatning med barnepornografi. Dette er et moment som åpenbart må telle med i interesseavveiningen etter § 8 bokstav f).

Domstolene har ved flere anledninger behandlet saker hvor kontrolltiltak på arbeidsplassen har vært begrunnet med behov for å avdekke straffbare forhold. Se blant annet Rt. 1991 side 616 (Gatekjøkken-kjennelsen), Rt. 2001 side 668 (Tippekasse-kjennelsen), RG 2000 side 664 og Agder lagmannsretts kjennelse av 05.10.1992 (Tappetårn-saken).[106] I alle disse sakene ble hemmelige videoopptak på arbeidsplassen avskåret som bevis som følge av at denne form for overvåking var i strid med personvernrettslige regler. Det finnes imidlertid rettspraksis hvor hemmelig videoovervåkning har blitt tillatt, blant annet på bakgrunn av konkret mistanke om straffbare forhold. Se i denne sammenheng Gulating lagmannsretts kjennelse fra 15.10.2001, inntatt i RG 2002 side 162. Lagmannsretten mente her det måtte skilles mellom generell hemmelig overvåking og overvåking på bakgrunn av konkrete mistanker.[107] Arbeidsgiver hadde i denne saken sterke mistanker om at hans ansatte hadde begått straffbare handlinger, og behovet for å sikre seg bevis måtte etter rettens mening gå foran hensynet til de ansattes personvern. Retten foretok her en konkret

---

[106] Se Lov&Data nr. 34, mars 1993 (Tappetårn-saken).

[107] Lagmannsretten skilte mellom 1) alminnelig akseptert overvåking av butikklokale rettet mot kunder, 2) overvåking som de ansatte var kjent med og har akseptert, 3) skjult overvåking av tilsatte uten konkret mistanke om misligheter og 4) skjult overvåking av tilsatt(e) etter forutgående konkret mistanke om underslag eller andre straffbare forhold. Alternativ 3 skulle normalt avskjæres som bevis, mens 1 og 2 ikke kunne avskjæres. Alternativ 4 var mest relevant i denne saken, og bevisene kunne tillates ført dersom kontrolltiltaket ikke gikk lenger enn det som var nødvendig.

forholdsmessighetsvurdering, og fant at videoopptakene i denne saken ikke representerte inngrep i den personlige integritet som oversteg det som måtte tåles i et rettssamfunn.

Ingen av de kjennelsene som ble trukket frem ovenfor, gjaldt popplyl. § 8. Domstolenes resonnementer kan likevel ha overføringsverdi i forhold til avveiningen etter popplyl. § 8 bokstav f). RG 2002 side 162 bærer bud om at *konkrete mistanker* om straffbare forhold kan senke terskelen for hva som er tillatt av kontrolltiltak i arbeidslivet. *Avdekking* av kriminalitet og *avkrefting av mistanke mot uskyldige* måtte etter rettens mening være *legitime formål* i et samfunnsmessig perspektiv. RG 2002 side 162 gjelder videoovervåking, men begrunnelsen for å tillate bevisene ført må kunne ha overføringsverdi i forhold til andre typer kontrolltiltak. Det kan derfor tenkes at konkrete mistanker om straffbare forhold kan gjøre kontroll av e-post og logger rettmessig etter popplyl. § 8 bokstav f), forutsatt at det aktuelle kontrolltiltaket ikke går lenger enn det formålet gjør påkrevd, og at kontrolltiltaket er egnet til å samle inn bevis for de straffbare handlingene.

Det er arbeidsgivers ansvar at hjemmelen "holder", og det vil normalt ikke være lett for den enkelte arbeidsgiver å foreta en objektiv og nøytral vurdering i slike tilfeller, hvor egeninteressen i tiltakene normalt vil være en tung påvirkningsfaktor. Datatilsynet vil måtte innta en sentral rolle i utformingen av retningslinjer for avveiningen etter denne bestemmelsen, jf. Ot.prp. nr. 92 (1998-99) på side 109, jf. popplyl. § 42 (3) (særlig nr. 4, 6 og 7).

3.5 Forholdet mellom de rettslige grunnlagene i popplyl. § 8

Det har i teorien vært reist spørsmål om arbeidsgiver har en plikt til først å forsøke å innhente samtykke fra arbeidstakerne før han iverksetter kontrolltiltak på arbeidsplassen. Verken loven eller forarbeidene gir noen eksplisitt løsning på dette spørsmålet. Popplyl. § 8 bokstavene a) til f) innebærer på en side en enkel måte for arbeidsgiver å etablere et rettslig grunnlag for kontrolltiltaket. På den annen side vil det rettslig sett være en fordel om det foreligger et samtykke, jf. uttalelsene i Ot.prp. nr. 92 (1998-99) på side 108:

"(...) Behandling av personopplysninger bør i størst mulig utstrekning baseres på samtykke fra den registrerte, selv om den også kan hjemles i de grunnlagene som oppstilles i bokstavene a-f. For det første vil dette styrke den registrertes muligheter til å råde over opplysninger om seg selv. For det annet vil man ved å basere behandlingen på samtykke unngå mulig tvil om de mer skjønnsmessige vilkårene i bokstavene a til f er oppfylt."

I Norsk Lovkommentar har Dag Wiese Schartum skrevet følgende om denne problemstillingen:

"Det er uavklart om en behandlingsansvarlig kan nøye seg med å konstatere at kravet til nødvendighet er tilfredsstilt og derfor la være å innhente samtykke fra de personer opplysningene gjelder. Kravene til nødvendighet i § 8 bokstavene a-f er slik formulert at nesten ethvert behandlingsformål kan legitimeres på denne måten. Loven kan neppe forstås slik at samtykkealternativet kan ignoreres fordi det er mulig å påberope seg et av nødvendighetsalternativene".[108]

Schartum synes videre å legge til grunn at de hjemmelsgrunnlag som følger av § 8 bokstavene a) til f) kun skal anvendes dersom arbeidsgiver ikke finner det praktisk eller økonomisk mulig å innhente samtykke – i alle fall gjelder dette bokstavene b) til f). Bokstav a) kan nemlig etter hans oppfatning i seg selv sies å omfatte et element av samtykke. Uttalelsen synes å ha grunnlag i et spørsmål om hvorvidt den behandlingsansvarlige kan "styre unna" innhenting av samtykke, og i stedet behandle personopplysninger med hjemmel i § 8 bokstavene a) til f). Schartum synes å hevde at bokstavene a) til f) er sekundære hjemmelsgrunnlag, på den måten at samtykke skal forsøkes innhentet i de tilfeller det er mulig. Dette kan ikke forankres i ordlyden, men har gode grunner for seg. Det kan imidlertid neppe oppstilles noe formelt krav om at samtykke skal forsøkes innhentet først. I Ot.prp. nr. 92 (1998-99) på side 108 står det kun at behandlingen *"bør"* baseres på samtykke. I en del tilfeller ville et krav om å først forsøke å innhente samtykke kunne undergrave formålet med kontrolltiltaket, da arbeidstaker gis anledning til å hale ut tiden, for på den måten å rydde av veien opplysninger som kan få negative konsekvenser for vedkommende. Nødvendighet er i

[108] Note 27 til § 8 i Norsk Lovkommentar.

tillegg oppstilt som *alternativt* hjemmelsgrunnlag til lov og samtykke. Til tross for at også lojalitetsplikten mellom arbeidsgiver og arbeidstaker kan tilsi at arbeidsgiveren bør forsøke å innhente samtykke først, er det ingen klare holdepunkter i primærrettskildene for å legge Schartums syn til grunn.[109] Dersom den behandlingsansvarlige har tilstrekkelig hjemmel i popplyl. § 8 bokstavene a) til f), er dette tilstrekkelig for å behandle opplysningene.

Særlige problemer reiser seg også i de tilfeller hvor samtykke er forsøkt innhentet, men hvor arbeidstaker har nektet å gi dette. Kan arbeidsgiver da likevel foreta kontrolltiltaket? Noe kategorisk svar kan neppe gis på dette spørsmålet. Dersom vilkårene i en av bokstavene i § 8 er oppfylt og arbeidsgiver har et saklig behov for å kontrollere sine ansattes e-post og logger, kan arbeidstakerne neppe gjøre tiltaket ulovlig ved å nekte samtykke. Arbeidsgiver bør i utgangspunktet ikke stilles dårligere rettslig sett fordi han har forsøkt å tilnærme seg problemene på en lojal måte ovenfor arbeidstakerne. På den annen side vil det lett tenkes at nødvendighetsnormen skjerpes noe i disse tilfellene, særlig i de tilfeller hvor *viktige* personvernhensyn kommer i strid med arbeidsgivers behov.[110]

3.6 Generelt om betydningen av arbeidsavtaler og instrukser

En relevant problemstilling i forbindelse med kontroll og overvåking i arbeidslivet, er hvilken rettslig betydning avtaleregulering av kontrolladgang har. Arbeidstakere blir ofte møtt med arbeidsavtaler og interne instrukser som fastsetter rammene for kontrolladgangen i den aktuelle bedriften. Ovenfor er arbeidsavtalens betydning drøftet

---

[109] Nina Melsom har påpekt at det kan være grunn til å reise spørsmål om ikke innhenting av samtykke er et bedre middel til å ivareta lovens formål enn å benytte hjemmelen i § 8 bokstav f). Uttalelsen gir ingen løsning på problemstillingen, men hennes poeng vil uansett kunne være et moment i vurderingen i forhold til begrepene *"nødvendighet"* og *"berettiget interesse"*, jf. § 8 bokstav f). Se Nina Melsom, "Ny lov om personopplysninger – noen arbeidsrettslige problemstillinger" på side 385.

[110] Se Norsk Lovkommentar, note 27 til popplyl. § 8 ved Dag Wiese Schartum, samt Ot.prp. nr. 92 (1998-99) på side 109.

i forhold til popplyl. § 8 bokstav a). Nedenfor vil det bli gjort rede for arbeidsavtalens og interne instruksers betydning for kontrolladgangen på et mer generelt plan.

En arbeidsavtale er basert på tilbud og aksept, slik vi finner disse mekanismene i kontraktsretten for øvrig. Ved å inngå en slik avtale påtar partene seg en rekke forpliktelser overfor hverandre, og undertegningen innebærer et samtykke til det som følger av avtalens bestemmelser. Et slikt samtykke kan følgelig også innebære en aksept av at arbeidsgiver kontrollerer innholdet i e-post og informasjon i loggene for øvrig. Det er ikke dermed sagt at kontrolltiltakene er tillatt etter personopplysningsloven. Først og fremst kommer begrensningene i lovens § 2 nr. 7 inn med fyll tyngde. Det vil si at samtykket skal være uttrykkelig, frivillig og informert. Ofte vil kravet til uttrykkelighet og informasjon være oppfylt i en slik situasjon. Når arbeidstaker derimot presenteres for denne typen vilkår i arbeidsavtalen, kan det være så som så med den reelle frivilligheten. Arbeidsavtalens bindende funksjon er avhengig av at samtlige avtalevilkår godtas av avtalepartene. Arbeidstaker kan således føle seg tvunget til å gå med på vilkår han egentlig ikke føler seg komfortabel med, i frykt for ikke å få jobben. Særlig gjelder dette i et presset arbeidsmarked, hvor alternativene kanskje er få. Det samme gjelder i forhold til arbeidstakere som i utgangspunktet kanskje ikke er fullt ut kvalifisert for en stilling av den aktuelle typen, men som ser karrieremessige fordeler ved å skrive under. Dette er en problemstilling som ikke er omhandlet i forarbeidene til personopplysningsloven, og det finnes heller ikke rettspraksis hvor graden av frivillighet har vært diskutert i denne forbindelse. Det må likevel etter min oppfatning kunne legges til grunn at kravet om frivillighet i § 2 nr. 7 normalt er oppfylt også i disse situasjonene, jf. også punkt 3.2.2. Inngåelsen av en arbeidsavtale må sies å være frivillig, til tross for at arbeidstaker kanskje reelt sett føler at han ikke har noe valg.[111] Velger man å akseptere de vilkårene som fremgår av avtalen, er dette en risiko man selv må bære.[112] Dette innebærer at arbeidstaker, ved å skrive under på arbeidsavtalen, kan samtykke i at arbeidsgiver skal kunne kontrollere også *privat* e-post på arbeidsplassen.

---

[111] Dette gjelder likevel ikke dersom arbeidsgiver truer vedkommende til å skrive under. Her vil det foreligge et klart tilfelle av tvang, og frivillighetskravet i popplyl. § 2 nr. 7 vil ikke være oppfylt.

[112] Det finnes trolig preseptorisk arbeidsrettslig lovgivning som oppstiller visse skranker for avtalefriheten, men dette skal ikke forfølges nærmere her.

Se nærmere om forholdet mellom privat og virksomhetsrelatert e-post i punkt 5.2 nedenfor.

Når det gjelder grunnkravene til behandlingen av personopplysninger, jf. popplyl. § 11, samt de ulovfestede kravene til saklighet og proporsjonalitet, er dette krav arbeidsgiver ikke kommer unna ved å innhente samtykke gjennom arbeidsavtalen (eller på andre måter). Dette følger både av det ulovfestede arbeidsrettslige regelverket og av personopplysningsloven.[113] Kravet til saklighet følger blant annet av popplyl. § 11 (1) bokstav b), jf. nedenfor. Denne bestemmelsen oppstiller *grunnkrav* til behandlingen av personopplysninger, og gjelder uavhengig av om behandlingen er basert på hjemmel i lov, på samtykke eller på nødvendighetsavveiningen etter § 8 bokstavene a) til f). Kravet om proporsjonalitet er derimot ikke regulert i § 11. Når kontrolladgangen er avtaleregulert og basert på samtykke, er det derfor lite som tyder på at *lovens* proporsjonalitetsbegrensning kommer inn. Det ulovfestede proporsjonalitetsprinsippet gjelder imidlertid side om side med personopplysningsloven, og vil komme inn som selvstendig begrensning i forhold til arbeidsavtalen gjennom popplyl. § 1 (2).

Et annet sentralt moment i forbindelse med den rettslige betydningen av arbeidsavtalen, er avtalens funksjon i forhold til arbeidsgivers informasjonsplikt. Både etter det ulovfestede og det lovfestede regelverket har arbeidsgiver en plikt til å varsle de ansatte om kontrolltiltak på arbeidsplassen. Tilsvarende plikter følger av Hovedavtalen mellom LO og NHO.[114] I og med at arbeidsavtalen, eventuelt interne instrukser e.l., inneholder bestemmelser om kontroll og overvåking, blir arbeidstaker varslet allerede på dette tidspunkt. Arbeidsavtalen og instruksene fungerer på denne måten som varslingsinstrumenter. Dersom arbeidsgiver holder seg innenfor de rammene som er *lovlig* skissert i avtalen, vil arbeidstakerne sjelden senere bli hørt med at informasjonsplikten ikke er overholdt. For den typen kontrolltiltak som er omfattet av personopplysningsloven, herunder kontroll av e-post og datalogger, er det imidlertid i

[113] Se også ARD 1937 side 114, ARD 1951 side 201, ARD 1958 side 189, ARD 1959 side 1 og ARD 1968 side 44.

[114] Se punkt 6.3.1.

tillegg en forutsetning at kravene i popplyl. §§ 19 og 20, jf. 23, er oppfylt. Se nærmere om dette i punkt 6.2.

I tillegg til den regulering av rettigheter og plikter som følger direkte av arbeidsavtalen, opererer arbeidsgiver ofte med interne instrukser på arbeidsplassen. Noen ganger er det henvist til slike instrukser i arbeidsavtalen, og instruksene anses da å være vedlegg til arbeidsavtalen. Andre ganger er instruksene gitt uavhengig av den opprinnelige arbeidsavtalen, men de kan like fullt være bindende. Forutsetningen er likevel at innholdet i instruksene er innenfor rammene av hva arbeidsgiver lovlig kan regulere i kraft av sin styringsrett. Arbeidsgiver kan i slike interne instrukser nedlegge forbud mot privat bruk av bedriftens IT-utstyr, eventuelt oppstille konkrete begrensninger i bruken. Slike forbud eller begrensninger vil i sin tur kunne ha betydning for arbeidsgivers rett til å kontrollere sine ansattes e-post o.l., jf. punkt 3.4.2 ovenfor. Arbeidstaker vil da ha en mindre berettiget forventning om diskresjon, da all e-post i utgangspunktet da skal være *virksomhetsrelatert,* jf. punkt 5.2 nedenfor. Tilsvarende gjelder ikke nødvendigvis for innsyn i loggene for øvrig. Loggene kan inneholde informasjon om arbeidstakernes effektivitet, hva de har gjort i arbeidstiden, når de har gjort det, hvem de har kommunisert elektronisk med, osv. Betenkelighetene med å tillate generelt innsyn er derfor etter min mening større.

> Slike forbud og begrensninger vil også kunne ha betydning for rettmessigheten av å lagre private dokumenter og lignende i bedriftens datasystem. Arbeidsgiver vil således kunne ha rett til å gå inn og lese, eventuelt slette, private dokumenter som befinner seg på såkalte "åpne brukerområder" på bedriftens server. Se også RG 1993 side 77. Datatilsynet har lagt et tilsvarende syn til grunn i sine retningslinjer: *"Datatilsynet tilrår at den det gjeld blir rådd til å fjerne private filer sjølv. Likevel kan den systemansvarlege slette slike filer dersom dei strir mot dei interne retningslinjene for drift og tryggleik. Føresetnaden er at dei tilsette kjenner retningslinjene og konsekvensar det kan få å ha private filer i informasjonssystemet".*[115]

I punkt 3.2.5 ble det redegjort for betydningen av tariffavtalene, hovedsaklig med tanke på kollektive samtykker til kontrolltiltak. Dersom domstolene i fremtiden skulle godta

---

[115] Se < http://www.datatilsynet.no/dtweb/art_831.html > (13.10.2003).

kollektivt samtykke innenfor personopplysningslovens virkeområde, vil lovens begrensninger, saklighetsprinsippet[116], proporsjonalitetsprinsippet[117] mv. komme inn som begrensning også i forhold til denne typen avtaler. En forutsetning for at LO og NHO på denne måten skal kunne tariffregulere kontrolladgangen, er også at informasjons- og drøftelsesplikten i Tilleggsavtale V til Hovedavtalen overholdes, jf. ARD 1978 side 110. I tillegg gjelder informasjonsplikten etter personopplysningsloven og det ulovfestede regelverket.

> For ordens skyld nevnes at Tilleggsavtale V i Hovedavtalen (2002-2005) synes å begrense kontrolladgangen i tråd med personopplysningsloven og det ulovfestede arbeidsrettslige regelverket. Se blant annet punkt 1 i Tilleggsavtale V, som lyder:
>
> *"Kontrolltiltak kan ha sitt grunnlag i teknologiske, økonomiske, sikkerhets- og helsemessige omstendigheter, samt andre sosiale og organisatoriske forhold i bedriften. Tiltak som innføres skal ikke gå ut over det omfang som er nødvendig og må være saklig begrunnet i den enkelte bedrifts virksomhet og behov".*[118]
>
> Når kontrolladgangen er regulert på denne måten, er betenkelighetene med å godta tariffregulering mindre. At kontrolladgangen er regulert i tariffavtalen, kan også tenkes å få betydning for nødvendighetsavveiningen etter § 8. For øvrig ville det kanskje vært ønskelig med en konkretisering av de begrensningene som gjelder, slik at tariffavtalene kunne fungere som et hjelpemiddel for arbeidsgivere og arbeidstakere, og at de da lettere kan sette seg inn i hva slags kontrolltiltak som er tillatt. Konkretiseringen kan for eksempel relatere seg til nødvendighetsbegrepet i popplyl. § 8, *"berettiget interesse"* i § 8 bokstav f), saklighetskriteriet mv.

---

[116] Se punkt 4.2. Se også ARD 1937 side 114, ARD 1951 side 201, ARD 1958 side 189, ARD 1959 side 1 og ARD 1968 side 44.

[117] Se punkt 4.3. Se også ARD 1978 side 110.

[118] Se også § 9-13 i Hovedavtalen.

4 Begrensningene i kontrolladgangen

4.1 Innledning

I kapittel 2 og 3 er det gjort rede for de rettslige grunnlagene for behandling av personopplysninger i arbeidslivet. Personopplysningsloven § 8 kan i seg selv sies å innebære en begrensning i arbeidsgivers styringsrett, da bestemmelsen oppstiller forholdsvis strenge rammer for behandlingsadgangen. Det finnes imidlertid en rekke andre lovfestede og ulovfestede begrensninger, herunder saklighetsprinsippet, proporsjonalitetsprinsippet og personopplysningslovens øvrige bestemmelser. Disse begrensningene vil bli behandlet i de påfølgende avsnittene. I tillegg vil det kort bli redegjort for i hvilken grad enkelte av arbeidsmiljølovens bestemmelser kan sies å innebære tilleggsbegrensninger i kontrolladgangen.[119]

4.2 Saklighetsprinsippet

4.2.1 Innledning

En av de mest sentrale begrensingene i styringsretten er det ulovfestede arbeidsrettslige *saklighetsprinsippet*. Prinsippet innebærer at ethvert kontrolltiltak skal være saklig begrunnet i virksomhetsrelaterte forhold, tiltaket må ikke praktiseres vilkårlig og det må ikke tas utenforliggende hensyn ved avgjørelsen om å sette kontrolltiltaket i verk. Videre må et kontrolltiltak være egnet til å oppnå formålet med tiltaket. Den informasjon arbeidsgiver vil tilegne seg i forbindelse med kontrolltiltaket må derfor korrespondere med formålet bak tiltaket. Tiltakenes lovlighet avhenger derfor i stor grad av arbeidsgivers begrunnelse for å sette dem i verk. De spørsmål som skal behandles i punkt 4.2 flg. er hva som er innholdet i det arbeidsrettslige saklighetsprinsippet, i hvilken grad et tilsvarende prinsipp er kommet til uttrykk i personopplysningsloven og hva som er likhetene og forskjellene mellom disse lovfestede og ulovfestede begrensningene i arbeidsgivers kontrolladgang.

---

[119] Det kan tenkes ytterligere begrensninger i kontrolladgangen, eksempelvis straffelovgivning, taushetspliktsbestemmelser mv. For mer informasjon, se NOU 1997: 19 på sidene 33-35.

4.2.2 Innholdet i det ulovfestede saklighetsprinsippet

I to dommer avsagt av Høyesterett, henholdsvis Rt. 2001 side 418 (Kårstø-dommen) og Rt. 2000 side 1602 (Nøkk-saken), ble det uttrykt at styringsretten måtte være begrenset av allmenne saklighetsnormer.[120]

> I Kårstø-dommen var spørsmålet om når arbeidstiden begynte og sluttet for to grupper av arbeidstakere ved Statoils anlegg på Kårstø. I denne forbindelse uttalte Høyesterett seg forholdsvis generelt om rekkevidden av arbeidsgivers styringsrett. I Nøkk-saken var spørsmålet hvorvidt Stavanger kommune i kraft av styringsretten kunne kreve at to utdannede skipsmaskinister på kommunens brannbåt skulle integreres i kommunenes hovedbrannstyrke. Ingen av avgjørelsene omhandlet kontrolltiltak på arbeidsplassen, men uttalelsene omkring styringsretten og saklighetsnormen vil kunne ha betydning utover de konkrete saksforholdene.

I Nøkk-saken uttalte Høyesterett følgende:

> *"Arbeidsgiver har i henhold til styringsretten rett til å organisere, lede og kontrollere og fordele arbeidet, men det må skje innenfor rammen av det arbeidsforhold som er inngått. Ved tolkningen og utfyllingen av arbeidsavtalene må det blant annet legges vekt på stillingsbetegnelse, omstendighetene rundt ansettelsen, sedvaner i bransjen, praksis i det aktuelle arbeidsforhold og hva som finnes rimelig i lys av samfunnsutviklingen".*

Høyesterett henviste i Kårstø-dommen til Nøkk-saken, og uttalte i forlengelsen av sitatet ovenfor:

> *"(...) Styringsretten begrenses imidlertid av mer allmenne saklighetsnormer. Utøvelse av arbeidsgivers styringsrett stiller visse krav til saksbehandlingen, det må foreligge et forsvarlig grunnlag for avgjørelsen, som ikke må være vilkårlig, eller basert på utenforliggende hensyn".*

Høyesterett henviser her til *allmenne saklighetsnormer*. Disse normene utgjør til sammen det som i denne avhandlingen blir omtalt som saklighetsprinsippet i

---

[120] Se også underutvalgets rapport på side 28. Tilsvarende uttalelser finnes i ARD 1961 side 90.

arbeidsretten. De begrensninger som følger av de alminnelige domstolers og Arbeidsrettens praksis omkring kontroll og overvåking i arbeidslivet, bygger på de samme hensyn som ligger bak alminnelige personvernrettslige prinsipper og regler om *vern av den personlige integritet,* forvaltningsrettslige prinsipper om forsvarlig saksbehandling (eks. den såkalte myndighetsmisbrukslæren) mv. Det er hevet over tvil at de ulovfestede *personvernrettslige* prinsippene også må kunne anvendes i forhold til kontroll og overvåking i arbeidslivet. Prinsippene hviler på et overordnet behov for beskyttelse av enkeltindivider mot blant annet uberettigede kontrolltiltak. Det er imidlertid vanskelig å angi eksakt hvilket innhold disse prinsippene har, og på denne bakgrunn redegjøre for eventuelle forskjeller fra det ulovfestede *arbeidsrettslige* saklighetsprinsippet. Når det nedenfor gjøres rede for *ulovfestede prinsipper* eller *ulovfestet rett*, er det det ulovfestede arbeidsrettslige regelverket det siktes til – med mindre noe annet eksplisitt fremgår.

> Saklighetsprinsippet og proporsjonalitetsprinsippet (se punkt 4.3) er i arbeidsrettslig teori og praksis gjerne omtalt som ulovfestede *arbeidsrettslige* prinsipper. Prinsippene vil imidlertid beskytte de samme interessene som enkelte av de personvernrettslige prinsippene i forhold til kontrolltiltak i arbeidslivet. Hvorvidt man da kaller prinsippene for rene arbeidsrettslige prinsipper, eller om man omtaler de som *personvernrettslige prinsipper på arbeidsrettens område*, har ikke og bør ikke ha noen rettslig betydning. Dette til tross for at saklighets- og proporsjonalitetsprinsippet også vil begrense arbeidsgivers styringsrett i forhold til andre situasjoner enn der hvor utøvelse av styringsretten har personvernmessige konsekvenser.

Saklighet er en rettslig standard, og den rettslige vurderingen av et kontrolltiltak må følgelig baseres på skjønnsmessige avveininger i det konkrete tilfelle. Den nærmere utformingen av saklighetskravet har funnet sted gjennom arbeidsrettslig rettspraksis. Det er utformet noen retningslinjer som lar seg overføre fra sak til sak, blant annet at ethvert kontrolltiltak skal være begrunnet i virksomhetsrelaterte forhold, at tiltaket skal være egnet til å fremme formålet med den aktuelle inngripen, og at tiltaket ikke må praktiseres vilkårlig mv., jf. ovenfor. Prinsippet skal således beskytte arbeidstakerne mot vilkårlige inngrep i deres personlige integritet. Noe særlig nærmere en presisering tror jeg ikke man kommer.

Til tross for at personopplysningsloven ikke er vedtatt direkte på bakgrunn av rettspraksis i Norge, finner man igjen utslag av tilsvarende regler og prinsipper i personopplysningsloven.[121] I de neste avsnittene skal det derfor gjøres rede for kravet til saklighet, slik dette fremkommer i personopplysningsloven, samt redegjøres for hvordan lovens bestemmelser skal fortolkes i forhold til og på bakgrunn av ulovfestet rett.

4.2.3 Krav om saklig begrunnet formål – popplyl. § 11 (1) bokstav b)

Personopplysningslovens § 11 gjennomfører direktivets artikkel 6, og oppstiller 5 kumulative vilkår – eller grunnkrav – til behandling av personopplysninger.[122] Personopplysningsloven regulerer ikke kontroll og overvåking direkte, men kontroll av e-post og logger vil ofte innebære behandling av personopplysninger, jf. punkt 2.2.1. Popplyl. § 11 innebærer at alle fem vilkårene må være oppfylt for at kontroll av e-post og logger skal være rettmessig. Mens popplyl. § 8 oppstiller vilkårene for adgangen til å *iverksette* kontrollen, oppstiller § 11 krav til selve *gjennomføringen* av kontrolltiltaket. I dette avsnittet er det i første omgang § 11 (1) bokstav b) som er av størst interesse.

Popplyl. § 11 (1) bokstav b) uttrykker i det vesentligste det samme som det som følger av rettspraksis vedrørende kontroll- og overvåkningstiltak i arbeidslivet.[123] Både lovens krav til saklighet og det ulovfestede arbeidsrettslige saklighetsprinsippet søker å ivareta sentrale personvernhensyn. Etter popplyl. § 11 (1) bokstav b) skal den behandlingsansvarlige sørge for at opplysninger som behandles:

> *"bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet".*

---

[121] Personopplysningslovens bestemmelser er imidlertid utslag av ulovfestede *personvernrettslige* regler og prinsipper, da loven ikke er utformet med særlig tanke på arbeidslivet.

[122] Popplyl. § 11 er en videreføring av kravet til behandling av opplysninger etter den tidligere personregisterloven § 6, og praksis omkring denne bestemmelsen vil være relevant i tolkningen av § 11 (1) bokstav b).

[123] Jf. underutvalgets rapport på side 46 og side 71.

Man ser at § 11 (1) bokstav b) i realiteten innebærer to krav til kontrolltiltakets formål. For det første skal formålet være *uttrykkelig angitt*, og for det annet skal formålet være *saklig begrunnet i forhold til den virksomhet den behandlingsansvarlige driver*. Det er den behandlingsansvarliges oppgave å angi formålet med kontrolltiltaket, og formålsangivelsen skal klart fremgå av meldingen eller konsesjonssøknaden til Datatilsynet, jf. §§ 31 og 32.

Kravet om at formålet skal være uttrykkelig angitt innebærer at formålsangivelsen ikke kan være for vid eller for vag.[124] Den behandlingsansvarlige må således presisere konkret hva han ønsker å oppnå med behandlingen, jf. for så vidt NOU 1997: 19 på side 137. Departementet uttalte i Ot.prp. nr. 92 (1998-99) på sidene 113-114 at uttrykkelighetskravet innebærer at *"den behandlingsansvarlige forut for behandlingen må fastsette et formål som er tilstrekkelig konkret og avgrenset til at det skaper åpenhet og klarhet om hva behandlingen skal tjene til. (...) Generelle og vage beskrivelser som "administrative oppgaver" eller "kommersiell bruk" vil ikke være tilstrekkelig presise"*. Det vil derfor ikke være tilstrekkelig å hevde at behandlingen er basert på et ønske om å overvåke arbeidstakeren; det kreves en presisering av hva slags type kontrolltiltak det er snakk om og hvorfor det settes i verk. Dette henger også sammen med at opplysningene ikke senere skal benyttes til formål som er *uforenlige* med de som opprinnelig var oppgitt, jf. § 11 (1) bokstav c). Man ser altså at den uttrykkelige formålsangivelsen i tillegg skal oppstille rammene for senere bruk av de opplysninger som fremkommer i og med kontrolltiltakene (se også personopplysningsforskriftens § 7-11 (3)). Formålsangivelsen vil videre danne grunnlaget for Datatilsynets vurdering av hvorvidt det opprinnelige angitte formålet er saklig begrunnet i virksomhetens forhold. Formålsangivelsen må være mer presis enn de formål som er kommet til uttrykk i popplyl. § 8, jf. Ot.prp. nr. 92 (1998-99) på side 114, og jo viktigere personvernhensyn som kan bli krenket, desto klarere må formålet være angitt, jf. NOU 1997: 19 på side 137.

[124] I teorien er det lagt til grunn at denne delen av bestemmelsen er utslag av det såkalte *"formålsbestemthetsprinsippet" eller "Purpose Spesification Principle"*.

I Kårstø-dommen, Rt. 2001 side 418, ble det uttalt at utøvelsen av styringsretten stilte krav til saksbehandlingen og at avgjørelsen om å sette i verk kontrolltiltaket måtte baseres på et forsvarlig grunnlag. Kravet til uttrykkelig formålsangivelse i popplyl. § 11 første ledd, bokstav b) ivaretar nettopp denne forutsetningen. Ved at arbeidsgiver pålegges å vurdere formålet med kontrolltiltaket nøye før han setter det i verk, vil han også konkret måtte vurdere om kontrolltiltaket er forsvarlig.

Formålsangivelsen har følgelig også betydning der arbeidstakeren samtykker i kontrolltiltaket. Dersom formålet er uklart angitt, vil det senere kunne stilles spørsmål om arbeidstakeren rent faktisk har samtykket i tiltaket i tråd med lovens samtykkekrav. Formålsangivelsen ivaretar på denne måten også viktige notoritetshensyn i forbindelse med kontrolltiltaket.

I kravet til saklighet ligger en formodning om at arbeidsgiver ikke fritt kan velge hvilke formål et kontrolltiltak skal ha. Behandlingen av personopplysningene skal være begrunnet i saklige, virksomhetsmessige *behov,* hvilket betyr at formålet skal ha naturlig sammenheng med den virksomhet arbeidsgiver normalt utøver. Man kan således ikke behandle personopplysninger med et hvilket som helst formål, selv om dette formålet er uttrykkelig angitt, jf. NOU 1997: 19 på side 137. På samme side i utredningen er det lagt til grunn at direktivets oppregning i art. 7 (se også popplyl. § 8 bokstavene a) til f)) kan gi en viss veiledning i vurderingen av behandlingens saklighet. Et eksempel i Kommentarutgaven kan bidra til en viss klargjøring; en lege kan ikke behandle økonomiske opplysninger om sine pasienter med det formål å foreta en kredittsjekk av dem. Eksemplet illustrerer et klart eksempel på overtramp, men er kanskje mindre egnet til å brukes som eksempel i grensetilfellene. Et eksempel som kanskje fungerer bedre som illustrasjon, er tilfeller hvor arbeidsgiver driver en virksomhet som krever strengt hemmelighold av virksomhetsrelaterte opplysninger. I disse tilfellene vil *behovet for hemmelighold* normalt kunne gjøre kontroll av de ansattes korrespondanse mv. rettmessig, da behovet er relatert til den spesielle form for virksomhet arbeidsgiver driver. Hadde formålet med kontrolltiltaket ikke vært å forhindre informasjonslekkasjer, men i stedet å finne grunner til å få vedkommende oppsagt eller avskjediget, ville kontrolltiltaket *ikke* vært saklig begrunnet i arbeidsgivers virksomhet.

I forlengelsen av det siste eksemplet kan det være interessant å vurdere de rettslige spørsmålene som oppstår der arbeidsgivers virksomhet endrer karakter i løpet av kontrollperioden. Hvis arbeidsgivers kontrolltiltak anses rettmessige fordi den aktuelle virksomheten gjør det påkrevd med strengt hemmelighold, vil kontrolltiltakene kanskje ikke kunne opprettholdes dersom virksomhetens art på et gitt tidspunkt ikke lenger gjør hemmelighold påkrevd. Kontrolltiltakenes begrunnelse vil da måtte vurderes på nytt i forhold til den nye virksomhetstypen og være saklig i forhold til denne. Dette følger ikke eksplisitt av lovens ordlyd, men er en konsekvens av at enhver behandling av personopplysninger skal være saklig begrunnet i virksomheten. Selv om en type kontrolltiltak er rettmessig på ett tidspunkt, er det derfor ikke gitt at den er det på et senere tidspunkt. Tilsvarende vurdering må kanskje foretas i forhold til *hjemmelsgrunnlaget* for behandlingen. Dersom arbeidstakeren har samtykket til kontrolltiltakene mens hemmelighold var essensielt for bedriften, vil nytt samtykke trolig måtte innhentes dersom forutsetningene for samtykket endrer seg. Og der arbeidsgiver hjemlet kontrolltiltakene i § 8 bokstavene a) til f), vil en ny nødvendighetsavveining måtte foretas i forhold til den endrede virksomheten. Man ser også her den nære sammenhengen mellom § 8 og § 11.

Et poeng som også bør nevnes, er at det på en arbeidsplass ikke alltid vil være arbeidsgiver som er behandlingsansvarlig. Det forekommer at kontrolltiltak settes i gang av en tredjeperson uten arbeidsgivers ønske og viten. Det kan for eksempel tenkes at denne tredjepersonen ønsker å sette enkelte arbeidstakere i dårlig lys ved å kontrollere deres effektivitet, kontrollere om de aktuelle arbeidstakerne har brutt IT-instruksene eller liknende. I disse tilfellene vil saklighetsnormen måtte vurderes i forhold til den som rent faktisk behandler opplysningene og i forhold til den virksomhet denne personen driver. Dersom tredjepersonen derimot behandlet personopplysningene *på vegne av* arbeidsgiver, er det naturlig å se på tredjepersonen som ”databehandler”, jf. popplyl. § 2 nr. 5. Ansvaret for kontrolltiltakets rettmessighet vil i disse tilfellene fortsatt ligge hos arbeidsgiver, da denne ikke kan fraskrive seg ansvaret ved å sette bort oppdraget til andre. I forhold til større bedrifter vil dette være en praktisk problemstilling, da det her ofte finnes egne IT-ansvarlige som foretar kontrolltiltakene

på arbeidsgivers vegne, eventuelt at administrasjonen av bedriftens IT-utstyr er satt bort til personer/firmaer utenfor bedriften.

I NOU 1997: 19 på side 137 (forslag til popplyl. § 7) uttaler utvalget at *lovlighet* burde presiseres som et selvstendig krav i forbindelse med behandlingens formål. Departementet mente at dette kravet var så selvsagt at det ikke var noen grunn til å presisere det i lovteksten, jf. Ot.prp. nr. 92 (1998-99) på side 114. Utover dette gir forarbeidene liten veiledning i forhold til popplyl. § 11 (1) bokstav b). Det er også sparsomt med arbeidsrettslig litteratur der saklighetsprinsippet er redegjort for i forbindelse med kontroll- og overvåkingstiltak i arbeidslivet. De begrensningene prinsippet innebærer, må således søkes belyst gjennom kartlegging av rettspraksis. Rettspraksis på området er imidlertid også sparsomt, særlig i forbindelse med e-post og datalogger. Dog finnes noen avgjørelser som gjelder andre former for kontroll og overvåkning på arbeidsplassen, eksempelvis TV-overvåkning, narkotika- og alkoholtesting o.l. De begrensningene i kontrolladgangen som følger av denne praksisen er relevante også for kontroll av ansattes e-post og datalogger, og således også i forhold til personopplysningslovens krav om saklighet. Avgjørelsene gir uttrykk for alminnelige begrensninger i arbeidsgivers styringsrett, og de rettssetningene som utledes av dem, kommer inn som vurderingsmomenter via lovens formålsbestemmelse, jf. popplyl. § 1 (2).

I ARD 1978 s. 110 hadde arbeidsgiver innført stikkprøvekontroll av arbeidstakernes privatbiler i det de skulle forlate arbeidsplassen. Arbeidsretten uttalte at et slikt kontrolltiltak foreskrev at det *saklig sett var behov for det*, tiltaket kunne *ikke være åpenbart grunnløst* eller *motivert av utenforliggende hensyn*, og tiltaket skulle *ikke praktiseres vilkårlig* – i den betydning at arbeidsgiver uten reell begrunnelse setter enkelte arbeidstakergrupper i en særstilling.[125] Tilsvarende ble lagt til grunn av Arbeidsretten i ARD 1959 side 1 og ARD 1968 side 44, der det videre ble presisert at

[125] Se også Tilleggsavtale V, punkt 2 i Hovedavtalen mellom LO/NHO 2002-2005, samt parallellen til den forvaltningsrettslige *myndighetsmisbrukslæren*, jf. eksempelvis Eckhoff/Smith, Forvaltningsrett på side 286-287 og 299 flg.

kontrolltiltakene måtte være ulovlige dersom arbeidsgiver har *satt seg utover ethvert skjønn*.

I tråd med Nøkk-saken, Rt. 2000 side 1602, er arbeidsgivers utøvelse av styringsretten begrenset innenfor rammene av arbeidsavtalen. Praksis på arbeidsplassen og sedvaner i bransjen mv. vil videre kunne tillegges vekt i tolkningen av denne avtalen. Dette må bety, at dersom arbeidstakerne har godtatt at arbeidsgiver fører en viss kontroll med deres aktiviteter på arbeidsplassen, vil dette kunne komme inn som et moment i tolkningen av arbeidsavtalen, noe som igjen vil ha betydning for vurderingen av tiltakets saklighet. Gitt at arbeidsgiver har gitt klart uttrykk for at e-post og datalogger vil kunne bli utsatt for kontroll. Har slike tiltak vært fast praksis på arbeidsplassen, vil selve saklighetsnormen kanskje lempes i forhold til situasjoner hvor man ikke har hatt en tilsvarende praksis. Høyesterett uttalte også at arbeidsavtalen vil måtte tolkes i lys av samfunnsutviklingen. I og med at drøftelsen omhandlet saklighetsnormen som begrensning i styringsretten, tolker jeg denne uttalelsen slik at saklighetsnormen er dynamisk, og at den således endres i takt med samfunnet for øvrig. Et kontrolltiltak som var ansett å være saklig motivert for 20 år siden, vil derfor ikke nødvendigvis være det i dag (og motsatt).[126]

4.2.4 Krav om tilstrekkelighet og relevans – popplyl. § 11 (1) bokstav d)

I popplyl. § 11 (1) bokstav d) er det inntatt en bestemmelse om at opplysninger som behandles skal være:

> *"(...) tilstrekkelige og relevante for formålet med behandlingen"*[127]

Kravet om *relevans* er atskilt fra det alminnelige kravet til saklig formål, jf. § 11 (1) bokstav b). Bestemmelsene henger imidlertid svært nøye sammen. Kravet til saklighet relateres i utgangspunktet til *begrunnelsen* for behandlingen av personopplysninger,

---

[126] Dette er følgelig noe man må ta høyde for når man benytter eldre rettspraksis i rettslig argumentasjon omkring kontrolltiltak på arbeidsplassen i nyere tid.

[127] I direktivet artikkel 6 nr. 1 bokstav c) står det at opplysningene *"skal være adekvate, relevante og ikke for omfattende i forhold til de formål de er innsamlet for og/eller senere behandles for"*.

mens kravet til relevans relaterer seg til *gjennomføringen* av behandlingen. Opplysningene skal altså være *relevante* i forhold til et formål som er *saklig* begrunnet i den behandlingsansvarliges virksomhet. Kravet til relevans følger også av de ulovfestede arbeidsrettslige reglene, men det synes ikke å ha utviklet seg noe eget relevansprinsipp i norsk rett. Opplysningenes tilknytning til formålet med kontrolltiltaket vil imidlertid være sentral i forhold til vurderingen av kontrolltiltakets saklighet, jf. kravet om at kontrolltiltaket skal være "egnet til" å oppnå formålet, jf. Rt. 1986 side 1250. Det arbeidsrettslige saklighetsprinsippet kan derfor også sies å omfatte et krav om relevans.

> I svensk rett synes det å være motsatt; man opererer ikke med noe eget saklighetsprinsipp, men i stedet et *relevansprinsipp*. I SOU 2002: 18 ("Integritetsutredningen") på side 68 annet avsnitt er relevansprinsippet beskrevet på følgende måte: *"Sävel i artikel 6 i direktivet som i § 9 PUL uttrycks relevansprincipen på så sätt att de personuppgifter som samlas in skall vara relevante i förhållande till ändamålen med behandlingen. Av kommissionens förklaring fremgår att detta innebär att uppgiftarna måste korrespondera med de mål man vill uppnå med behandlingen. Insamlingen av uppgiftarna får bara ske för särskilda, uttryckligt angivna och berättigade ändemål, viklet innebär att ändamålen med behandlingen av personuppgiftarna måste bestämmas av den personuppgiftsansvarige redan när uppgiftarna samlas inn. En alltför allmänt hållen ändamålsangivelse godtas inte utan avsikten är att andvändningen av personuppgifter skall defineras så precist som möjligt (...) Ändamålen för vilke personuppgifterna samlas in skall vidare vara bärettigade."* Man stiller altså krav om at formålet skal defineres klart og presist, at dette ikke skal være for vidt angitt, og at opplysningene som behandles skal være relevante i forhold til det formål de er samlet inn for. Det kan på denne bakgrunn virke som om det svenske relevansprinsippet omfatter både det som er inntatt i den norske popplyl. § 11 (1) bokstav b), og bokstav d), på samme måte som jeg mener det norske ulovfestede saklighetsprinsippet gjør det. Det ulovfestede saklighetsprinsippet omfatter således både krav til begrunnelsen og krav til gjennomføringen.

Relevansbegrepet er, som saklighetsbegrepet, ikke noe fast og entydig begrep. Innholdet i relevanskravet vil avhenge av den type opplysninger som behandles, måten opplysningene blir innhentet på og tidspunktet de blir samlet inn på.[128] Jo mer sensitive

[128] Jf. også NOU 2003: 21 på side 184 (punkt 13.5.3.1) hva gjelder kravet til relevans i utvalgets forslag til ny politiregisterlov.

opplysninger det er snakk om, og jo mer drastiske metoder man benytter for å innhente opplysningene – desto strengere vil en relevansvurdering være. I Ot.prp. nr. 92 (1998-99) på side 114 er det uttrykt at relevanskravet *"markerer en ytre grense for hvilke personopplysninger som kan trekkes inn i behandlingen",* og at behandlingen ikke må *"omfatte unødvendige personopplysninger"*.[129] I NOU 2003: 21 på side 184 (punkt 13.5.3.1) har utvalget, i forhold til forslag til ny politiregisterlov, uttalt at *"hensikten med relevanskravet er å forhindre at det behandles flere opplysninger enn det er behov for. Kan formålet oppnås ved at det registreres færre opplysninger eller mindre sensitive opplysninger, er politiet i henhold til relevanskravet forpliktet til å foreta begrensningen"*.

> NOU 2003: 21 utgjør ikke en del av personopplysningslovens forarbeider, men forslaget til ny politiregisterlov bygger til dels på personopplysningslovens (og direktivets) bestemmelser. Uttalelsene kan derfor bidra til å klargjøre begrepene i personopplysningsloven.

Man ser altså at det i relevanskravet foreligger en kobling mellom et krav om saklighet og et krav om proporsjonalitet. Kontrolltiltaket skal ikke gå ut over hva man ønsker å oppnå med behandlingen, og man skal ikke tilegne seg opplysninger utover det som er nødvendig i forhold til formålet. Det kan derfor tenkes at relevanskravet i personopplysningsloven til dels også er omfattet av det ulovfestede arbeidsrettslige proporsjonalitetsprinsippet. Se punkt 4.3 flg. nedenfor.

I tillegg til et krav om relevans, ligger det i § 11 (1) bokstav d) også et krav om at opplysningene skal være *tilstrekkelige* for formålet med behandlingen. Dette innebærer at opplysningene skal være egnet til å oppnå behandlingsformålet, men også at de skal være mest mulig fullstendige *"i forhold til det de skal representere"*.[130] Opplysningene må altså være dekkende i forhold til formålsangivelsen, for på denne måten å representere et "sannere" og fyldigere bilde av den registrerte.[131] Det er ikke noe krav

---

[129] Jf. direktivet artikkel 6 bokstav c) (*"ikke for omfattende"*).

[130] Jf. Kommentarutgaven på side 122.

[131] Jf. også NOU 2003: 21 på side 187 (punkt 13.5.4), hvor utvalget uttaler følgende:
"Tilstrekkelighetskravet innebærer at den registrerte har krav på at opplysningene er så fullstendige, det

om absolutt fullstendighet, men et krav om at opplysningene skal være *tilstrekkelig* fullstendige.[132] I forarbeidene til personopplysningsloven er dette uttalt på følgende måte: *"I kravet om at personopplysningene må være tilstrekkelige, ligger at opplysningsgrunnlaget må være så fullstendig som behandlingsformålet krever"*.[133] Når arbeidsgiver samler inn opplysninger om sine ansatte, må han derfor undersøke nøye at opplysningene er knyttet til den (de) aktuelle arbeidstaker(ne). Hvis arbeidsgiver kontrollerer loggopplysningene tilknyttet en av bedriftens datamaskiner, og deretter knytter opplysningene opp mot arbeidstaker A, må han forsikre seg om at opplysningene har den tilstrekkelige tilknytning til nettopp denne personen. Det kan for eksempel tenkes at datamaskinen benyttes av flere arbeidstakere, og at det derfor ikke er gitt at opplysningene omhandler As aktiviteter. Dersom arbeidsgiver eksempelvis finner spor av barnepornografi på serveren, plikter han å foreta grundige undersøkelser før opplysningene legges inn i en bestemt ansatts personalmappe e.l. Det kan eksempelvis tenkes at vedkommende arbeidstaker har mottatt barnepornografiske bilder pr. e-post, og at han derfor ikke har skyld i at bildene har blitt registrert på arbeidsgivers server.[134] Arbeidsgiver plikter da å foreta ytterligere undersøkelser for å avklare hvorvidt disse bildene kan knyttes til den aktuelle arbeidstakeren.

4.2.5 Forholdet mellom saklighetsprinsippet og popplyl. § 11 (1) b) og d)

Det foreligger foreløpig ingen rettsavgjørelser hvor personopplysningslovens saklighets- og relevanskrav er stilt opp mot det ulovfestede prinsippet. Det er mye som tyder på at kravene til behandlingen av personopplysninger etter loven og etter ulovfestet rett samsvarer. Se også underutvalgets rapport på side 71, hvor underutvalget uttaler at *" (...) personopplysningsloven og de arbeidsrettslige reglene bør tolkes i lys av hverandre. Saklighetskravet etter personopplysningsloven § 11 kan antakelig i vidt*

---

vil si utfyllende og detaljerte, at det hindrer at opplysningene gir et misvisende eller uriktig bilde av en person eller en situasjon (...)".

[132] Jf. også NOU 2003: 21 på side 187, annen spalte.

[133] Jf. Ot.prp. nr. 92 (1998-99) på side 114.

[134] Det kan da kanskje reises spørsmål om vedkommende arbeidstaker plikter å melde fra om hendelsen, slik at arbeidsgiver kan håndtere situasjonen på best mulig måte. Denne problemstillingen skal imidlertid ikke forfølges her.

omfang fortolkes som det arbeidsrettslige saklighetskravet (…)". Tilsvarende bør kravet til relevans i § 11 (1) bokstav d) etter min oppfatning tolkes i lys av de ulovfestede prinsippene, jf. ovenfor.

Etter personopplysningsloven vil saklighets- og relevansbegrensningen alltid komme inn som en begrensning i forhold til § 8, da samtlige vilkår i § 11 må være oppfylt i tillegg til de vilkår som følger av § 8. Kravene gjør det mulig å underkjenne et kontrolltiltak som ellers synes å være lovlig etter § 8. På denne måten representerer kravene eksplisitte begrensninger i de rettslige grunnlagene for behandling av personopplysninger. Innenfor arbeidsretten er saklighetsprinsippet utformet som en noe mer upresis begrensning i arbeidsgivers styringsrett.

Om forholdet mellom det ulovfestede og det lovfestede saklighetskravet, har de danske juristene Blume og Kristiansen lagt til grunn at det i dansk rett må skilles mellom negative og positive vurderinger av behandlingssituasjonene:

> *"Som udgangspunkt forekommer det nærliggende at antage, at den databeskyttelsesretlige saglighetsvurdering vil falde sammen med den arbejdsretlige, når det er tale om en negativ vurdering af en behandlingssituasjon. Så fremt en behandling ikke er saglig arbejdsretlig set, vil den ej heller være saglig databeskyttelsesretlig set (…). Det må betragtes som noget mer usikkert, om der er et tilsvarende sammenfald ved en positiv vurdering af en behandlingssituasjon. Det forekommer langt fra givet, at den arbejdsretligt saglige behandling i alle tilfælde vil være databeskyttelsesretlig sagligt. Det skyldes, at det er forskellige hensyn, der begrunder de to saglighedsprincipper, og databeskyttelsesrettens mer konsekvente fokus på at sikre saglig databehandling på ethvert område (…)".*[135]

Med dette legger forfatterne altså vekt på utgangspunktet for vurderingen. Der et kontrolltiltak er *usaklig* etter ulovfestede arbeidsrettslige regler, vil det høyst sannsynlig også være usaklig etter den danske personopplysningsloven. Det er ikke dermed gitt at kontrolltiltak som er *saklige* etter de arbeidsrettslige reglene også er saklige i forhold til personopplysningslovens regler. Med dette antyder de således at saklighetsnormen er noe strengere i personopplysningsloven. Hvorvidt dette utgangspunkt kan legges til

[135] Peter Blume og Jens Kristiansen, "Databeskyttelse på arbejdsmarkedet" på side 42.

grunn etter norsk rett også, er usikkert. Det ble under utformingen av direktivet og de nordiske personopplysningslovene lagt vekt på at personvernet skulle styrkes i forbindelse med behandling av personopplysninger. Se i denne sammenheng Ot.prp. nr. 92 (1998-99) på side 8, hvor det uttales at siktemålet med den nye loven har vært å styrke rettighetene til den som personopplysningene gjelder. Et slikt generelt siktemål gir imidlertid ikke grunnlag for å konkludere med at saklighetsnormen er skjerpet i og med vedtakelsen av personopplysningsloven. Oppfatningen synes tvert imot å være at det ulovfestede saklighetsprinsipp er sammenfallende med saklighetskravet i personopplysningsloven. Lovens regler og det ulovfestede prinsippet synes jo også å beskytte de samme interessene. Likevel er det på det rene at loven skjerper kravene til saksbehandling, eksempelvis gjennom reglene om melde- og konsesjonsplikt, retting, innsyn mv.

En forskjell mellom det ulovfestede prinsippet og lovens saklighetskrav, er imidlertid kravets utforming. Mens det arbeidsrettslige prinsippet krever at kontrolltiltaket skal være saklig motivert, basert på forsvarlige avveininger, ikke praktiseres vilkårlig mv., krever popplyl. § 11 (1) bokstav b) at kontrolltiltaket skal være basert på *formål* som er *saklig begrunnet* i den behandlingsansvarliges virksomhet. Noen stor realitetsforskjell innebærer dette likevel ikke. Et krav om saklig motivasjon og saklig behov for kontrolltiltaket vil alltid måtte vurderes i forhold til den aktuelle virksomheten og de spesielle forhold som gjør seg gjeldende der. Kravet om at kontrolltiltaket ikke må være vilkårlig eller basert på utenforliggende hensyn vil også kunne innfortolkes i lovens saklighetsnorm. Videre er det etter begge regelsett et krav om at *begrunnelsen* for kontrolltiltaket skal være saklig. Til tross for disse likhetene, er jeg som nevnt av den oppfatning at det ulovfestede prinsippet omfatter både et krav om saklighet og om relevans.

4.3 Proporsjonalitetsprinsippet

4.3.1 Innledning

Den neste begrensningen i styringsretten som skal behandles, er kravet om proporsjonalitet. I arbeidsretten har dette kravet utviklet seg til et rettslig prinsipp; *proporsjonalitetsprinsippet*. Begrepet "proporsjonalitet" betyr det samme som "forholdsmessighet", og man kunne derfor like gjerne omtalt prinsippet som et *forholdsmessighetsprinsipp*. Prinsippet er utformet på bakgrunn av et ønske om å begrense skadevirkningene av behandling av personopplysninger, og på denne måten beskytte enkeltindividenes personlige integritet.

Prinsippet består i hovedsak av to elementer (i forhold til denne avhandlingens emne). *For det første* oppstilles et krav om forholdsmessighet mellom *de interesser* arbeidsgiver søker å ivareta med kontrolltiltaket, og den krenkelsen tiltaket utgjør for arbeidstaker. Dette er et krav som relaterer seg til adgangen til å iverksette tiltak av den aktuelle typen. Prinsippet ligger på denne måten nært opp til saklighetsprinsippet, men er ikke nødvendigvis sammenfallende med dette. Mens saklighetsprinsippet oppstiller krav til begrunnelsen for kontrolltiltaket og dets evne til å oppnå det ønskede formål, oppstiller proporsjonalitetsprinsippet et krav om forholdsmessighet mellom de interesser og hensyn som taler for og i mot kontrolltiltaket. *For det annet* oppstilles en begrensning i forhold til *omfanget, utformingen* og *praktiseringen* av det konkrete kontrolltiltaket. Det må være forholdsmessighet mellom *tiltaket som sådan* og den krenkelsen det innebærer for arbeidstakeren. Tiltaket må ikke gå lenger enn det som kreves for å oppnå formålet, og prinsippet ligger derfor også nært opp til kravene om nødvendighet og relevans, jf. også punktene 3.4.1, 4.2.4 og 4.3.2. De to elementene glir over i hverandre, og vil sjelden måtte drøftes hver for seg. Spørsmålet om hvilke begrensninger proporsjonalitetsprinsippet oppstiller i den konkrete sak, vil måtte løses på bakgrunn av en sammensatt og skjønnsmessig vurdering. De to nevnte elementene vil imidlertid være av sentral betydning i denne vurderingen.

Når arbeidsgiver vurderer hvorvidt han skal kontrollere/overvåke sine ansattes aktiviteter, må han i hvert enkelt tilfelle vurdere hvor inngripende tiltaket kan fremstå

for den enkelte.[136] Kontrolltiltaket *som sådan* må være nødvendig for å gjennomføre formålet med det, og arbeidsgiver må på denne bakgrunn anvende det tiltaket som er minst inngripende overfor arbeidstakerne.[137] Prinsippet oppstiller således indirekte et krav om forholdsmessighet mellom mål og middel.

Proporsjonalitetsprinsippet oppstiller videre et krav om at det må foretas en vurdering av forholdet mellom behovet for kontroll og det rettsgrunnlaget kontrolltiltaket hviler på. Jo mer inngripende tiltaket er for den som utsettes for det, desto større krav stilles til det rettslige grunnlaget kontrolltiltaket baseres på.

4.3.2 Personopplysningslovens krav om proporsjonalitet

Det neste spørsmålet som skal behandles, er i hvilken grad personopplysningsloven inneholder regler som helt eller delvis tilsvarer det arbeidsrettslige proporsjonalitetsprinsippet. Etter personopplysningslovens § 8 er det mulig å behandle personopplysninger dersom dette er *nødvendig* etter nærmere bestemte kriterier, jf. § 8 bokstavene a) til f).

I Ot.prp. nr. 92 (1998-99) er begrepet *nødvendighet* som nevnt ikke drøftet særlig inngående. Det vil derfor være behov for å drøfte begrepet i lys av de arbeidsrettslige prinsippene og rettspraksis omkring personopplysningsloven. Til tross for at den rettskildemessige vekten av underrettspraksis er diskutabel, har jeg valgt å bruke en tingrettsdom som eksempel. I Oslo tingretts dom av 24.04.2002 (Oslo Sporveier) la retten til grunn at arbeidsgiver med hjemmel i popplyl. § 8 bokstav f) hadde adgang til å åpne bilder som arbeidstakeren hadde lastet ned på arbeidsgivers datamaskin. Domstolen hevdet at hensynet til arbeidstakerens personvern ikke oversteg hensynet til arbeidsgivers interesser. Arbeidsgiver hadde forut for nedlastingen gjort det klart at nedlasting av porno var forbudt på arbeidsplassen. Arbeidsgiver hadde engasjert IT-ansvarlig ved bedriften for å hjelpe en av de ansatte som hadde mistet en del e-post og

[136] Jf. underutvalgets rapport på side 28. Se også RG 2002 side 162.

[137] Se Rt. 1986 side 1250.

datafiler, og det ble gjennomført feilsøk på en av serverne i denne sammenheng. Under søkene ble det avdekket en rekke mistenkelige filer, noe som medførte at de aktuelle bildene ble åpnet. Innholdet var grovt pornografisk, noe som førte til ytterligere undersøkelser. Da bildene etter hvert ble knyttet til den aktuelle arbeidstakeren, ble vedkommende avskjediget. I avskjedssaken ble det lagt stor vekt på at oppdagelsen ble gjort som ledd i administrativ kontroll med systemet, og at kontrolltiltakene i utgangspunktet ikke hadde blitt satt i gang overfor en bestemt ansatt. Videre ble det lagt vekt på at nedlastingen var straffbar etter straffeloven § 204. Arbeidstakeren hadde anført flere dommer omkring ulovlig fjernsynsovervåkning som grunnlag for avskjæringen av bevisene, noe domstolen ikke fant relevant i denne saken. Ulovlig fjernsynsovervåkning måtte anses som mye mer inngripende overfor arbeidstakerne enn de tilfeller hvor arbeidsgiver mer eller mindre tilfeldig avdekker bilder som en ansatt selv hadde lastet ned fra internett.[138]

Det fremgår ikke klart i denne dommen hvor proporsjonalitetskravet kommer inn. Følger det av selve termen "nødvendig" innledningsvis i § 8, eller følger det av *"(...) kan ivareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen"*, jf. § 8 bokstav f)?[139] I punkt 3.4.1 er det lagt til grunn at det i selve nødvendighetskravet ligger en proporsjonalitetsbegrensning, til tross for at begrepene "nødvendighet" og "proporsjonalitet" ikke nødvendigvis er *helt* sammenfallende rettslig sett. Det er vanskelig å se at et kontrolltiltak er nødvendig etter § 8, hvis det ikke samtidig er proporsjonalt med formålet bak tiltaket. På den annen side følger det direkte av ordlyden i bokstav f) at man skal foreta en avveining mellom de motstridende interesser; for at kontrolltiltaket skal være rettmessig, må det være av en sånn art og basert på et slikt formål, at hensynet til arbeidstakerens personvern må vike. Mye tyder derfor på at proporsjonalitetsbegrensningen er kommet til uttrykk begge steder.

---

[138] Tilsvarende synspunkter er lagt til grunn også i Raufoss-dommen, Rt. 2001 side 1589.

[139] Proporsjonalitetsprinsippet er også kommet til uttrykk i lovens §§ 34 og 35, som gjelder Datatilsynets vurdering av hvorvidt konsesjon etter § 33 skal gis, samt hvorvidt det skal oppstilles vilkår for konsesjonen.

Avveiningen i forhold til kravet om proporsjonalitet er meget vanskelig – særlig med tanke på de manglende føringene i forarbeidene. Justisdepartementet har imidlertid uttalt at personvernhensyn må veie tungt i vurderingen av behandlingens rettmessighet etter § 8 bokstav f); særlig der personverninteresser veies opp mot arbeidsgivers kommersielle interesser (bl.a. økonomiske hensyn), jf. Ot.prp. nr. 92 (1998-99) på side 109. De lege ferenda bør tilsvarende kunne legges til grunn i forhold til vurderingen av hvorvidt et kontrolltiltak er nødvendig, og således også proporsjonalt.

I Raufoss-dommen, Rt. 2001 side 1589, foretok Høyesterett også en vurdering av forholdet mellom arbeidsgivers interesser og hensynet til arbeidstakerens personvern – denne gang på bakgrunn av personregisterloven og de ulovfestede personvernreglene (saksforholdet gikk tilbake til 1999 og personopplysningsloven var ennå ikke vedtatt). Arbeidsgiver hadde hatt store problemer med kapasiteten på sin internettlinje, og noe av bakgrunnen for dette var at en driftskonsulent ved bedriftens IT-avdeling hadde lastet ned store mengder musikkfiler (mp3) via arbeidsgivers internettlinje. Arbeidsgiver igangsatte kontroll av brannmurloggene på serveren, og oppdaget på denne måten musikkfilene. Ved hjelp av en annen ansatt, låste de seg inn på vedkommendes kontor og oppdaget at driftskonsulentens 2 datamaskiner var i full gang med nedlastning av musikk. De tok deretter utskrift fra loggene på den ene datamaskinen. Driftskonsulenten ble på bakgrunn av funnene oppsagt fra sin stilling. I vurderingen av hvorvidt den tidligere personregisterlovens bestemmelser var overtrådt, viste Høyesterett til personregisterlovens hovedforskrift § 2-20 (2) (nå videreført i personopplysningsforskriftens § 7-11), hvor det står at *"(...) registeret kan bare brukes til administrasjon av systemet, og til å avdekke/oppklare brudd på sikkerheten i edb-systemet"*. Høyesterett fant at forskriftsbestemmelsen ikke var til hinder for den kontroll arbeidsgiver her hadde foretatt, da tiltaket ble satt i verk for å avdekke årsakene til kapasitetsproblemene. Tiltaket måtte således være omfattet av begrepet *"administrasjon av systemet"*, og måtte derfor godtas. Hensynet til arbeidstakerens personvern veide i denne saken ikke tyngre enn arbeidsgivers behov for å avklare kapasitets- og sikkerhetsmessige problemer i datasystemet.

Avgjørelsen inntatt i Rt. 1991 side 616 (Gatekjøkken-kjennelsen) bygger på generelle personvernhensyn. Den omhandler videoopptak av arbeidstakere (bevisavskjæring i

straffeprosessen), men har betydning utenfor dette saksforholdet hva gjelder vern av arbeidstakernes personlige integritet.[140] Arbeidsgiver hadde uten å varsle de ansatte videoovervåket arbeidsplassen. Høyesterett fant at ingen eksplisitte lovbestemmelser rammet forholdet, men at videoopptakene likevel måtte avskjæres som bevis fordi de innebar et *for* alvorlig inngrep i de ansattes personlige integritet. Retten behandlet ikke proporsjonalitetsprinsippet eksplisitt. *Begrunnelsen for* bevisavskjæringen ble imidlertid hjemlet i alminnelige prinsipper om vern av den personlige integritet. Som nevnt tidligere, er det vanskelig å skille mellom *personvernrettslige* prinsipper om vern av den personlige integritet og de ulovfestede *arbeidsrettslige* prinsippene. Som i mye av praksisen på området for øvrig, resonnerer retten seg frem ved å se på inngrepets alvorlighetsgrad i forhold til arbeidstakernes behov for vern. Proporsjonalitetsprinsippet vil være av sentral betydning for en slik vurdering.

Kjennelsen inntatt i RG 2002 side 162 ble nevnt i punkt 3.4.3. I denne saken kom lagmannsretten til at hemmelig videoovervåking i visse tilfeller må godtas der arbeidsgiver har en konkret mistanke om straffbare forhold, og uttalte at man må foreta en proporsjonalitetsvurdering av inngrepets karakter og alvorlighet, herunder overvåkingens innretning og avgrensning i tid og rom. Lagmannsretten kom til at videoopptakene i dette tilfellet representerte et inngrep i personvernet som måtte tåles i et rettssamfunn, og at de derfor ikke kunne avskjæres som bevis.

Et krav om proporsjonalitet vil – i tillegg til å begrense adgangen til innsamling av personopplysninger – også kunne ha betydning for bruken av allerede innsamlet informasjon. Personopplysningslovens § 11 (1) bokstav c) oppstiller et krav om at innsamlede opplysninger ikke senere skal kunne behandles med formål som er uforenlige med det opprinnelig angitte formålet, med mindre den registrerte har samtykket til dette. Bestemmelsen er utslag av det såkalte ”finalitetsprinsippet”, jf. punkt 4.4 nedenfor.[141] Bokstav c) overlapper på sett og vis proporsjonalitetsprinsippet. I et krav om at kontrolltiltaket ikke skal være for inngripende overfor arbeidstakeren,

---

[140] Jf. Jakhelln, i ”Fjernarbeid” side 151.

[141] Se Ot.prp. nr. 92 (1998-99) på side 113. Finalitetsprinsippet er ikke er arbeidsrettslig prinsipp, men et internasjonalt *personvernrettslig* prinsipp.

ligger det også etter min mening et krav om at innhentede opplysninger ikke senere skal benyttes til andre formål enn det de ble innhentet for. I motsatt fall ville kontrolltiltaket lett bli ansett uforholdsmessig inngripende – uavhengig om innsamlingen av opplysningene opprinnelig var i samsvar med popplyl. § 8. Det er imidlertid viktig å være oppmerksom på at det da vil være snakk om to forskjellige behandlingsprosesser, som begge vil måtte ha selvstendig rettslig hjemmel.

Det er arbeidsgiver selv som må vurdere hvorvidt hans interesser må gå foran arbeidstakernes, og i forhold til kontroll av e-post og logger vil dette være tiltak som ofte settes i gang uten arbeidstakernes viten. Da dette i mange tilfeller kan være inngripende ovenfor arbeidstakerne, er det viktig at Datatilsynet forsøker å veilede arbeidsgiverne før de begår lovbrudd i så henseende. Veiledningen vil imidlertid være basert på usikre retningslinjer i forarbeider og praksis, og inntil domstolene har utformet nærmere retningslinjer omkring popplyl. § 8, og kanskje særlig bokstav f), vil det ulovfestede proporsjonalitetsprinsippet måtte fungere som en viktig tolkningsfaktor i forhold til personopplysningslovens bestemmelser. Personopplysningslovens formålsbestemmelse fastsetter at loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet (…), jf. § 1 (2). Det alminnelige, ulovfestede proporsjonalitetsprinsippet vil derfor komme inn som tolkningsfaktor i forhold til popplyl. § 8 via denne bestemmelsen. Prinsippet vil på denne bakgrunn komme inn som en konkret begrensning i kontrolladgangen på arbeidsplassen – uavhengig av om proporsjonalitetsbegrensningen i realiteten er ment å være omfattet av begrepet *nødvendig*. Dette innebærer også at begrensningen ikke bare gjelder i forhold til § 8 bokstavene a) til f), men også i forhold til kontrolltiltak som hjemles i samtykke eller lov/forskrift. På samme måte vil saklighetsprinsippet komme inn som tolkningsfaktor via lovens formålsbestemmelse, jf. ovenfor.

4.4 Finalitetsprinsippet – popplyl. § 11 (1) bokstav c)

I forbindelse med drøftelsen av proporsjonalitetsprinsippet og popplyl. § 11 (1) bokstav b), ble § 11 (1) bokstav c) kort nevnt. Bestemmelsen fortjener imidlertid en noe mer

inngående redegjørelse. Bokstav c) fastslår at innsamlede personopplysninger *"ikke* [skal] *brukes senere til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker"*. Bestemmelsen er som nevnt utslag av det personvernrettslige *finalitetsprinsippet*, og innebærer en viktig begrensning i adgangen til å kontrollere arbeidstakernes e-post og logger.[142]

Popplyl. § 11 (1) bokstav c) er eksempelvis relevant der arbeidsgiver har logget opplysninger om arbeidstakerens aktiviteter på internett, og senere ønsker å kontrollere innholdet i loggene, dvs. kontrollere de innsamlede opplysningene (tekst, bilder, lyd mv.). Når arbeidsgiver som behandlingsansvarlig ønsker å benytte allerede innsamlede opplysninger til andre formål enn det som var oppgitt i den opprinnelige formålsangivelsen, er det et vilkår at også den nye behandlingen har rettslig hjemmel, jf. popplyl. § 11 (1) bokstav a), jf. § 8. Enhver behandling av personopplysninger må vurderes i forhold til popplyl. § 8, og således ha *selvstendig hjemmel*, jf. Ot.prp. nr. 92 (1998-99) på side 112-113. At opplysningene allerede er samlet inn har ingen betydning for vurderingen av om vilkårene i § 8 er oppfylt. Det er således ikke noe argument for å tillate videre behandling at opplysningene allerede er i arbeidsgivers besittelse.[143]

Dersom allerede innsamlede personopplysninger skal brukes ved senere anledninger, er det en forutsetning at den nye behandlingen ikke er *uforenlig* med det opprinnelig angitte formålet bak innsamlingen. Departementet har kalt dette *"kravet om forenlighet"*, jf. Ot.prp. nr. 92 (1998-99) på side 113. Dersom den behandlingsansvarlige ønsker å benytte personopplysninger til formål som ikke er forenlig med den opprinnelige formålsangivelsen, må opplysningene samles inn igjen på nytt før en ny behandling skal kunne settes i verk. Dette gjelder uavhengig av om

---

[142] Utslag av dette prinsippet finner man også igjen i direktivet, jf. art. 6 nr. 1 bokstav b). Se også SOU 2002: 18 på side 69 for svensk retts vedkommende.

[143] Bestemmelsen må sees i sammenheng med § 11 bokstav e), som stiller krav til lagringen av opplysningene (samt at opplysningene skal være korrekte og oppdaterte). Av hensyn til oppgavens størrelsesmessige rammer har jeg valgt å ikke behandle denne bestemmelsen.

også den nye behandlingen har selvstendig rettslig hjemmel. Unntatt er situasjoner hvor den registrerte samtykker i den nye behandlingen.[144]

Hva ligger så i begrepet "uforenlig"?[145] Departementet ønsket ikke å utdype dette i loven, da spørsmålet måtte vurderes konkret og individuelt. Forarbeidene ramser likevel opp flere momenter som vil være sentrale i en slik vurdering, så som *"om bruk av opplysningene innebærer ulemper for den registrerte, om bruken skiller seg sterkt fra den som lå til grunn for innsamlingen, eller om bruken stiller strengere krav til datakvalitet enn det opprinnelige innsamlingsformålet"*, jf. Ot.prp. nr. 92 (1998-99) på side 113.[146]

> Uttalelsene tyder på at det er en viss sammenheng mellom popplyl. § 11 (1) bokstav c) og proporsjonalitetsprinsippet, da vurderingen også etter bokstav c) til dels vil bestå av en avveining mellom fordelene for den behandlingsansvarlige og ulempene for den registrerte. I NOU 1997: 19 på side 138 er det uttalt at fordelene med den nye behandlingen må være *vesentlig større* enn ulempene. Utvalget la således opp til at det skulle foretas en interesseavveining, hvor det krevdes kvalifisert interesseovervekt i favør av ny behandling av allerede innsamlede opplysninger.

Behandlingen vil normalt ikke være uforenlig med det opprinnelige formålet der det nye formålet har en klar og naturlig sammenheng med den behandlingsansvarliges virksomhet. Forarbeidene nevner som eksempel en bank som samler inn lånesøknadsopplysninger og senere bruker disse opplysningene til å tilby kundene finanstjenester. Eksemplet er imidlertid lite egnet som eksempel i forhold til kontrolltiltak i arbeidslivet.

Interessant er det imidlertid at nettopp bruk av innsamlede opplysninger til kontrollformål er nevnt som eksempel på uforenlig bruk i forarbeidene, jf. Ot.prp. nr. 92 (1998-99) på side 113. Det er understreket at dette eksemplet særlig relateres til

---

[144] Departementet fant det uhensiktsmessig å kreve ny innsamling der den registrerte allerede hadde samtykket, jf. Ot.prp. nr. 92 (1998-99) på side 113.

[145] Se også personverndirektivets art. 6 nr. 1 bokstav b).

[146] Sml. utvalgets forslag til popplyl. § 8 nr. 3 i NOU 1997: 19.

behandlingsansvarlige som ikke har kontrolltiltak som en naturlig del av virksomheten, og hvor ubehaget for den registrerte vil bli stort i forhold til fordelene for den behandlingsansvarlige. Uttalelsen tyder på at innsamling av opplysninger i bedriftens datasystem (logging) med informasjonssikkerhetsmessige formål, ikke senere kan brukes til å kontrollere de ansattes aktiviteter.[147] Denne form for kontrolltiltak vil i utgangspunktet være uforenlig med det opprinnelige formålet bak innsamlingen, og bestemmelsen i bokstav c) har som følger at opplysningene må samles inn på nytt før de eventuelt benyttes til kontrollformål. Da er det en forutsetning at kontrolltiltaket har selvstendig rettslig hjemmel, jf. § 11 (1) bokstav a), jf. § 8.

> I NOU 1997: 19 på side 138 er det tatt forbehold for de tilfeller hvor ny innsamling ikke lenger er mulig. Utvalget la her til grunn at slike tilfeller etter omstendighetene kunne tale for å tillate ny behandling med endret formål. Et eksempel kan her være på sin plass. Gitt at loggopplysninger blir samlet inn som ledd i alminnelig administrasjon av datasystemet, eventuelt for å oppklare sikkerhetsbrudd i dette. Dersom det oppdages datafiler med barnepornografisk innhold, kan det tenkes at arbeidsgiver, eventuelt politiet, ønsker å finne ut hvem som har lastet ned disse filene. Det blir således tatt en sikkerhetskopi av loggfilene, mens de opprinnelige filene blir liggende i de opprinnelige aktivitetsloggene. Dersom den skyldige senere sletter sine spor fra serveren, vil ytterligere behandling av arbeidsgivers sikkerhetskopi kanskje være eneste mulighet til å oppklare forholdet. Verken arbeidsgiver eller politiet vil da ha noen mulighet til å samle loggopplysningene inn på nytt. Videre behandling av loggopplysningene vil da ha et annet formål enn den opprinnelige innsamlingen. I tråd med utvalgets uttalelser vil situasjonen imidlertid kunne tilsi at videre behandlingen av opplysningene tillates av hensyn til etterforskningen. En annen sak er at også sikkerhetskopieringen av filene innebærer behandling med et annet formål enn det opprinnelige. Utvalgets kommentarer ble imidlertid ikke videreført i Ot.prp. nr. 92 (1998-99), og det er derfor usikkert hvilken betydning de vil få i forhold til popplyl. § 11 (1) bokstav c).

I tillegg til de eksplisitte begrensningene i bokstav c), er det viktig å ikke glemme at vilkårene i popplyl. § 11 er kumulative. Dette innebærer at saklighet, relevans mv. må vurderes konkret også i forhold til den nye behandlingen.[148]

---

[147] Se parallellen til personopplysningsforskriftens § 7-11 (3).

[148] For ordens skyld nevnes at § 11 (2) fastslår at senere behandling av personopplysninger for historiske, statistiske eller vitenskapelige formål ikke anses uforenlig etter bokstav c) dersom samfunnets interesse i

4.5 Arbeidsmiljøloven som begrensning i kontrolladgangen

Arbeidsmiljøloven (aml.) inneholder enkelte bestemmelser som kan tenkes å innebære begrensninger i kontrolladgangen, jf. henholdsvis § 7 nr. 1, § 12 nr. 1 og § 12 nr. 2 (4). Nedslagsfeltet for bestemmelsene er ikke helt avklart i rettspraksis, i alle fall ikke i forhold til temaet for denne avhandlingen.

Aml. § 12 nr. 1 fastslår at *"Teknologi, arbeidsorganisasjon, utførelse av arbeidet, arbeidstidsordninger og lønnssystemer skal legges opp slik at arbeidstakeren ikke utsettes for uheldige fysiske eller psykiske belastninger (...)".* Videre er det i siste punkt presisert at arbeidstakerne ikke skal *"utsettes for trakassering eller annen utilbørlig opptreden"*. Bestemmelsen oppstiller generelle krav til arbeidsmiljøet og arbeidsgivers tilrettelegging av arbeidet, men kan lett tenkes å omfatte kontrolltiltak i arbeidslivet, jf. for så vidt Ot.prp. nr. 50 (1993-94) på side 66. Henning Jakhelln hevder at bestemmelsen omfatter enhver form for kontrolltiltak på arbeidsplassen.[149]

> I en noenlunde tilsvarende bestemmelse i arbeidervernloven av 1956, var fokuset i hovedsak rettet mot arbeidernes fysiske helse. Psykiske virkninger av arbeidet var omfattet av den generelle bestemmelsen, men dette fulgte ikke av ordlyden. I dagens arbeidsmiljølov er det tatt større høyde for psykiske virkninger av arbeidet, noe som klart fremgår av ordlyden i § 12 nr. 1.

At kontroll og overvåking omfattes av den generelle *ordlyden* i § 12 nr. 1 må være rimelig klart. Problemet er imidlertid at bestemmelsen vanskelig kan innebære noen *konkret* begrensning i arbeidsgivers kontrolladgang. Den oppstiller flere vage og generelle krav, uten at det er mulig å utlede noen konkrete rettigheter eller plikter av den. Bestemmelsen kan imidlertid tenkes å komme inn som en tolkningsfaktor ved anvendelsen av lovverket for øvrig. I vurderingen av hvorvidt et kontrolltiltak er

---

at behandlingen finner sted klart overstiger ulempene for den enkelte, jf. også NOU 1997: 19 på side 138-139. Bestemmelsen er ikke sentral for denne oppgaven, og vil derfor ikke blir drøftet nærmere.

[149] Jf. Jakhelln, "Fjernarbeid" på side 148.

proporsjonalt, vil tiltakets innvirkning på den ansattes psykiske helse være et relevant moment. Et kontrolltiltak som fremstår som *utilbørlig opptreden* fra arbeidsgivers side vil også lett kunne settes til side som lovstridig. Situasjonen er imidlertid den at det i vurderingsnormene i personopplysningsloven, eks. *"nødvendig"* i § 8, allerede er tilrettelagt for at slike momenter vil kunne spille inn i vurderingen av tiltakets rettmessighet. Behovet for å påberope seg aml. § 12 nr.1 er derfor kanskje ikke særlig stort.

Aml. § 12 nr. 1 (samt § 12 nr. 3 og § 19) ble påberopt i Rt. 1991 side 616 ("Gatekjøkken-kjennelsen"). Saken gjaldt videoovervåking på arbeidsplassen, og hvor Høyesterett uttalte følgende:

> *"Arbeidsmiljøloven inneholder ikke noen bestemmelse som uttrykkelig retter seg mot videoovervåkning eller videoopptak på arbeidsplassen. De bestemmelser som kan tenkes å få anvendelse på forholdet, er holdt i meget generelle vendinger. Paragraf 12 nr 1 første ledd bestemmer blant annet at arbeidsorganisasjonen skal legges opp slik at arbeidstakerne ikke utsettes for uheldige psykiske belastninger (...).*
>
> *Direktoratet for arbeidstilsynet har i en generell veiledning om arbeidsmiljøloven § 12, bestillingsnr 327, uttalt at fjernsynsovervåkning av ansatte reguleres av arbeidsmiljøloven § 12. Det samme har direktoratet lagt til grunn i en konkret sak. (...).*
>
> *Selv om de nevnte bestemmelser er vage, kan det nok være atskillig som taler for at de bør gis anvendelse. Bestemmelsene må tolkes i lys av loven bærende prinsipper, jf særlig formålsbestemmelsen i § 1 og det generelle krav til arbeidsmiljøet i § 7 nr 1. Hemmelig overvåkning av ansatte fremtrer som et alvorlig inngrep i arbeidsmiljøet".*

Uttalelsene retter seg ikke mot e-post og logger, men mot hemmelig fjernsynsovervåking på arbeidsplassen. Til tross for de faktiske forskjellene i disse kontrolltiltakene, taler reelle hensyn for at bestemmelsen også kan omfatte kontroll av e-post og logger. Høyesterett konkluderte imidlertid ikke på spørsmålet om § 12 nr. 1 kan påberopes direkte i forbindelse med kontroll og overvåking i arbeidslivet, og problemstillingen er derfor foreløpig uavklart de lege lata. De lege ferenda er det imidlertid ikke noe som tilsier at bestemmelsen ikke bør kunne påberopes, enten som en selvstendig skranke for kontrolltiltak som ikke omfattes av personopplysningsloven,

eller som en tilleggsskranke der tiltakene omfattes. Kontroll av e-post og datalogger er kontrolltiltak som kan utsette de ansatte for uheldige psykiske belastninger, noe arbeidsgiver er forpliktet til å forhindre i henhold til aml. § 12 nr. 1.

En annen mulig begrensning i styringsretten følger av aml. § 12 nr. 2 (4), som fastslår at *arbeidet må tilrettelegges på en slik måte at den ansattes verdighet ikke krenkes.* Denne bestemmelsen er også helt generell, og gjelder utformingen av arbeidet. Den ble tilføyd ved endringslov av 6. januar 1995, og i forarbeidene er kontrolltiltak ikke særskilt nevnt i denne forbindelse. I Innst. O. nr. 2 (1994-95) på side 18 ble kjønnsdiskriminerende påkledning på arbeidsplassen, herunder toppløs servering, nevnt som eksempel på bestemmelsens nedslagsfelt.[150] Sett hen til lovens formål og til ordlyden i bestemmelsen, kan det imidlertid tenkes at også denne kan påberopes i forbindelse med kontroll av e-post og logger. Som Jakhelln uttalte:

> *"Bestemmelsen er imidlertid utformet helt generelt, og må derfor antas å ha en vesentlig videre rekkevidde enn de spesielle forhold som knytter seg til de ansattes påkledning mv."* [151]

Høyesterett uttalte i Rt. 1991 side 616 at atskillige hensyn talte for å la § 12 nr. 1 komme direkte til anvendelse i forbindelse med kontrolltiltak. Det samme vil antakelig også gjelde § 12 nr. 2 (4) – bestemmelsen var imidlertid ikke inntatt i loven da Høyesterett avsa kjennelsen. Situasjonen er likevel etter min mening den samme som for § 12 nr. 1. Bestemmelsen er vag og skjønnsmessig, og bærer lite preg av å gi partene konkrete rettigheter og plikter. Alternativet til å se bestemmelsen som en selvstendig begrensning i kontrolladgangen er da også her å la den få betydning for fortolkningen av personopplysningslovens bestemmelser. [152]

Høyesterett nevnte i Rt. 1991 side 616 også aml. § 7 nr. 1. Denne bestemmelsen oppstiller krav om at arbeidsmiljøet skal være fullt forsvarlig ut fra både en enkeltvis og samlet vurdering av faktorer i arbeidsmiljøet som kan ha innvirkning på arbeidstakernes

---

[150] Jf. Jakhelln, "Fjernarbeid" på side 150. Se også Friberg m.fl. på side 128.

[151] Se Jakhelln, "Fjernarbeid" på side 150 (note 204).

fysiske og psykiske helse og velferd. For behandling av personopplysninger i arbeidslivet vil også denne bestemmelsen kunne komme inn som en begrensning, om enn med samme begrensede slagkraft som § 12 nr. 1 og nr. 2 (4).

Det bør kunne legges til grunn at bestemmelsene i arbeidsmiljøloven ikke innebærer begrensninger i adgangen til å kontrollere e-post og logger *utover* hva som følger av personopplysningslovens bestemmelser og rettspraksis. For kontrolltiltak som ikke omfattes av personopplysningsloven, kan bestemmelsene likevel fungere som selvstendige skranker for arbeidsgiver. Det kan også tenkes at arbeidsgivers kontrolltiltak bare delvis er omfattet av personopplysningsloven, eksempelvis der han både kontrollerer arbeidstakernes vanlige brevpost og deres e-post. Brevbruddet vil da kunne være i strid med aml. §§ 7 nr. 1, 12 nr. 1 og 12 nr. 2 (4), mens kontrollen av e-post i tillegg vil være regulert av personopplysningsloven.[153]

---

[152] Se NOU 1997: 19, punkt 6.1.8 – aml. § 12 er her drøftet i forbindelse med plassering av overvåkingsutstyr.

[153] Brevbrudd er også straffbart etter straffeloven § 145 (1). I underutvalgets rapport på side 57 er det lagt til grunn at arbeidsgiver etter omstendighetene kan straffes etter straffeloven § 145 (2) dersom han uberettiget leser sine ansattes e-post (”e-postbrudd”).

5 Nærmere om kontroll av datalogger og e-post

5.1 Kontroll av datalogger

5.1.1 Innledning

"Logging" er i korthet en *felles* betegnelse på automatisk innsamling/registrering av opplysninger i et datasystem, hvor opplysningene lagres i såkalte logger/datalogger. Dersom opplysningene som samles inn og registreres er personopplysninger i lovens forstand, krever også loggingen selvstendig rettslig grunnlag i henhold til popplyl. § 8. Nedenfor vil drøftelsen i hovedsak bli sentrert rundt kontroll av *innholdet* i loggene; med andre ord den *etterfølgende* behandlingen av personopplysningene.

> Arbeidsgiver vil normalt ha en forholdsvis vid rettslig adgang til å samle inn ("logge") opplysninger i sitt datasystem. Dette på bakgrunn av at arbeidsgiver normalt selv (eventuelt ved hjelp av andre personer/selskaper) forestår administrasjon av systemet, og han må derfor av tekniske og sikkerhetsmessige hensyn kunne registrere opplysninger om de aktiviteter som foregår i systemet. Dersom innsamlingen/registreringen har slike formål, vil behandlingen normalt være rettmessig i forhold til popplyl. § 8 bokstav f), eventuelt bokstav a). De øvrige grunnvilkårene for behandlingen vil normalt også være oppfylt, jf. eksempelvis vilkårene i popplyl. § 11. Dersom arbeidsgiver derimot innstiller loggfunksjonene i den hensikt å kontrollere og overvåke sine ansatte, blir forholdet et annet. Personopplysningsforskriften § 7-11, som det vil bli redegjort for nedenfor, kan gi viktig veiledning for adgangen til å logge opplysninger. Dette til tross for at denne bestemmelsen ikke gir noe rettslig grunnlag for behandlingen. Forskriften § 7-11 (3) oppstiller i tillegg et konkret forbud mot etterfølgende behandling av personopplysninger i kontrolløyemed. Denne bestemmelsen kan etter min mening gi veiledning også i forhold til den rettslige adgangen til å foreta selve innsamlingen/registreringen av opplysningene. Her vil man imidlertid kunne møte vanskelige bevisspørsmål. Siden arbeidsgiver normalt vil ha behov for å samle inn opplysningene i tilfeller som nevnt i forskriften § 7-11, vil man vanskelig kunne bevise at de samme opplysningene opprinnelig ble samlet inn med kontrollformål.

Det finnes en rekke forskjellige typer logger. Datamaskinens alminnelige aktiviteter logges ett sted på serveren, internettaktiviteter logges et annet, e-post logges et tredje sted osv. Betegnelsen tar således ikke høyde for at det foreligger store forskjeller i måten opplysningene samles inn på, eller at det finnes en rekke forskjellige typer

logger. Et viktig poeng som sjelden blir fremhevet i verken teori eller rettspraksis, er at man derfor ikke alltid kan operere med grovmaskede rubriseringer av de tekniske løsningene i et datasystem, jf. "adgangen til å *logge* opplysninger" eller "adgangen til å kontrollere *datalogger*" osv.

I forhold til de rettslige grunnlagene for behandlingen av personopplysninger, vil det kunne være nødvendig å skille mellom de ulike typetilfellene. Lovens krav til et samtykke innebærer at arbeidstakeren må være inneforstått med hvilke typer opplysninger om han som skal behandles. Hvis det da foreligger et samtykke til at arbeidsgiver kan kontrollere "loggene", er dette ikke nødvendigvis tilstrekkelig. Har arbeidstakeren da samtykket til innsyn i e-postloggene, brannmurloggene, Temporary Files-loggene eller File Transfer Protocol (FTP)-loggene?[154] Opplysningstypen kan variere sterkt fra loggtype til loggtype, og jeg tror ikke en slik generalisering er tilstrekkelig i forhold til samtykkekravet. Informasjonskravet i popplyl. § 2 nr. 7 gjør det nødvendig med ytterligere spesifiseringer. Har arbeidstakeren kun samtykket til innsyn i brannmurloggene, kan arbeidsgiver heller ikke kontrollere innholdet i andre typer logger med hjemmel i dette samtykket. Noe av den samme problematikken kan oppstå i forbindelse med popplyl. § 8 bokstav f). Arbeidsgiver kan for eksempel ha en berettiget interesse i å kontrollere én type logg, mens innsyn i logger som måler effektivitet på arbeidsplassen kan gå langt utover hva arbeidsgiver har rettslig dekning for å gjøre. Tilsvarende i forhold til e-post loggene; innsynsretten kan strekke seg til innsyn i såkalt *trafikkdata*, mens den ikke omfatter kontroll av innholdet i e-posten (tekst, bilde, lyd mv.). [155]

5.1.2 Personopplysningsforskriften § 7-11

Etter § 7-11 i forskrift til personopplysningsloven av 15.12.2000 (personopplysningsforskriften), gjøres unntak fra meldeplikten i

---

[154] Disse er kun eksempler på loggtyper.

[155] Trafikkdata er data som foreteller hvem som har sendt e-post, hvem som har mottatt den, når dette har skjedd osv. Dataene forteller ikke noe om det nærmere innholdet i e-posten. Termen brukes også om data som forteller hvilke nettsteder man har vært inne på, når dette er gjort og hvem som har vært inne på de aktuelle sidene (identifikasjonen skjer ved å kontrollere de såkalte IP-numrene).

personopplysningsloven § 31 (1) ved *"behandling av personopplysninger som følge av registrering av aktiviteter (hendelser) i et edb-system, samt behandling av personopplysninger om disposisjoner til ressurser i systemet"*. Bestemmelsen retter seg mot logging av opplysninger i datasystemet. Etter annet ledd kommer unntaksregelen kun til anvendelse dersom behandlingen har som formål *"å administrere systemet"*, jf. bokstav a), eller *"å avdekke/oppklare brudd på sikkerheten i edb-systemet"*, jf. bokstav b). Forskriftsbestemmelsen åpner altså for at arbeidsgiver kan logge visse opplysninger uten å melde fra til Datatilsynet, dersom formålet er å administrere datasystemet eller ivareta informasjonssikkerheten i dette. Tredje ledd er ny i og med personopplysnings-forskriften, og oppstiller forbud mot senere behandling av loggopplysninger i kontrolløyemed. Tredje ledd gjelder for så vidt uavhengig av meldepliktreglene, og oppstiller derfor en begrensning som åpenbart vil få betydning for kontrolladgangen.[156]

Dommen inntatt i Rt. 2001 side 1589 (Raufoss-dommen) og Oslo tingretts dom av 24.04.2002 (Oslo Sporveier) omhandlet begge behandling av personopplysninger i datalogger på arbeidsplassen. Behandlingen var i disse sakene ikke foretatt for å kontrollere/overvåke de ansatte; opplysningene ble funnet ved en tilfeldighet mens arbeidsgiver utførte *administrative kontrolltiltak*, dvs. tiltak for å avdekke feil i datasystemet. Dommene bærer bud om at personopplysninger kan behandles i kontrolløyemed under visse forutsetninger, nemlig dersom opplysningene i utgangspunktet oppdages under slike forhold som beskrevet i forskriften § 7-11 (2) bokstav a) eller b).[157]

---

[156] Se Datatilsynets retningslinjer vedrørende loggene: *"Logging inneber ei handsaming av personopplysningar som er meldepliktig etter personopplysningslova. Logginga er likevel friteken frå meldeplikt når opplysningane berre skal brukast til administrasjon av datasystemet eller oppdaging og oppklaring av brot på tryggleiken. (Sjå forskrifta § 7-11). Verksemda kan ikkje dekkje seg bak denne regelen dersom formålet med bruken er å overvake dei tilsette. Det vil seie at ein til dømes ikkje kan kartleggje kor mye tid dei tilsette bruker på nettet eller kva sider dei ser på (...)"* <http://www.datatilsynet.no/dtweb/attachment/895/loggar.html> (13.10.2003).

[157] Raufoss-dommen ble avsagt før personopplysningsloven var trådt i kraft, og personregisterloven og dens Hovedforskrift § 2-20 dannet derfor det rettslige utgangspunkt for vurderingen. Bestemmelsen er imidlertid i det vesentlige videreført i personopplysningsforskriften § 7-11.

> I Datatilsynets retningslinjer er "administrasjon av datasystemet" beskrevet på følgende måte: *"Administrasjon av systemet er å sørgje for at dei ressursane som finst i datasystemet til ei kvar tid kan verte nytta optimalt til det beste for verksemda. Ein del av administrasjonen kan til dømes vere å sørgje for at tilsette ikkje lastar ned og lagrar store mengder data for private formål i bedrifta sine nettverk."* [158]

I en kjennelse fra Gulating lagmannsrett av 19. februar 2003, gikk retten også inn på den nevnte forskriftsbestemmelsen.[159] En arbeidstaker ble avskjediget fra sin stilling i Phillips Petroleum Company Norway AS ("arbeidsgiver"), på bakgrunn av at han hadde foretatt søk etter og nedlasting av pornografisk materiale på internett. Arbeidsgiver hadde kontrollert loggene på bedriftens server, og forsøkte deretter å føre opplysninger om forholdet som bevis i avskjedssaken. Som ledd i vurderingen av bevisavskjæringsspørsmålet, gikk lagmannsretten inn på spørsmålet om hvorvidt opplysningene var innhentet i strid med personopplysningsloven. Lagmannsretten fant det problematisk å avgjøre hvordan popplyl. § 8 skulle fortolkes i denne saken, og uttalte noe overraskende at den ikke fant tilstrekkelige holdepunkter for at det bevismaterialet som det her var snakk om, var omfattet av personopplysningsloven. På dette tidspunktet hadde Høyesterett allerede uttalt at loggopplysninger er personopplysninger i lovens forstand, så fremt disse kan knyttes til enkeltpersoner, jf. Rt. 2001 side 1589 (Raufoss). Det er derfor noe betenkelig at lagmannsretten ikke la samme oppfatning til grunn under henvisning til Raufoss-dommen, da denne også hadde vært fremme ved flere anledninger under hovedforhandlingen. Uten å konkludere på spørsmålet om hvorvidt loven kom til anvendelse, slo imidlertid retten fast at arbeidsgivers kontrolltiltak ikke var i strid med personopplysningsforskriften § 7-11 – under henvisning til nettopp Raufoss-dommen. Bevisene ble derfor tillatt ført i avskjedssaken.

Innholdet i personopplysningsforskriften § 7-11 (2) bokstav b) har ennå ikke vært gjenstand for domstolsbehandling. Min oppfatning er at bestemmelsen gjør unntak fra meldeplikten der formålet eksempelvis er å avdekke eventuelle virus- eller hacker-angrep, da den gjelder behandling som har til formål å avdekke/oppklare

---

[158] Se < http://www.datatilsynet.no/dtweb/attachment/831/loggar.html > (13.10.2003).

[159] LG-2003-00090.

sikkerhetsmessige brudd på datasystemet. Denne typen sikkerhetsrisikoer vil i hvert fall kunne sies å være omfattet etter en rent språklig fortolkning av bestemmelsen. Videre vil jeg anta at den hjemler unntak fra meldeplikten i tilfeller hvor formålet med behandlingen er å avdekke hvorvidt arbeidstakerne eksempelvis har blottlagt informasjon i datasystemet for uvedkommende tredjemenn mv. I Gulating lagmannsretts kjennelse var det også anført at nedlastingen og søkene hadde vært forbundet med en viss risiko for virusangrep på bedriftens server. Lagmannsretten kunne ikke se bort fra at nedlastingen hadde påført arbeidsgiver en viss sikkerhetsrisiko, og underbygget sin konklusjon med dette. Retten rubriserte imidlertid ikke dette momentet inn under forskriften § 7-11 (2) bokstav b), noe som kunne ha vært en naturlig løsning – i hvert fall dersom kontrolltiltakene til dels hadde hatt som formål å avdekke om nedlastingen/søkene hadde påført arbeidsgiver en risiko for brudd på informasjonssikkerheten.[160] Sikkerhetsrisikoen var kort nevnt også i Raufoss-dommen, men retten tok heller ikke her direkte stilling til spørsmålet.

> Datatilsynet har etter det jeg kjenner til ikke forsøkt å redegjøre for hva slags informasjonssikkerhetsmessige tiltak som omfattes av forskriften § 7-11 (2) bokstav b). Tilsynet har imidlertid kommentert hva som formelt sett kreves før den behandlingsansvarlige kan påberope seg unntaket fra meldeplikten:
>
> *"Personopplysingslova § 13 og forskrifta sitt kapittel 2 stiller krav til informasjonstryggleik for verksemder som handsamar personopplysingar. For at fritaka i forskrifta skal kunne brukast, må verksemda ha tilpassa seg desse krava".* [161]

Det at forskriftsbestemmelsen gjør unntak fra meldeplikten ved logging som ledd i administrasjon av systemet eller logging for å avdekke sikkerhetsbrudd, åpner for misbruk fra arbeidsgivers side. Arbeidsgiver kan lett kamuflere kontrolltiltak ved å henvise til at opplysningene ble samlet inn på bakgrunn av formål som nevnt i annet ledd bokstav a) eller b). Denne misbruksproblematikken reiser vanskelige

---

[160] Det er det er noe usikkert hvorvidt bestemmelsen retter seg mot både eksterne (typisk "hacking") og interne sikkerhetsbrudd, eller om den kun retter seg mot den ene typen. Ser man Raufoss-dommen og lagmannsrettskjennelsen i sammenheng, synes det som om domstolene har lagt til grunn at både eksterne og interne sikkerhetsmessige risiki er relevante i forhold til § 7-11.

[161] Se < http://www.datatilsynet.no/dtweb/attachment/831/loggar.html > (13.10.2003).

bevisspørsmål. For å benytte eksemplet fra Raufoss-dommen; hva skal til for å si at man har problemer med kapasiteten på internettlinjen? Hastigheten på nettforbindelsen kan variere fra sekund til sekund. Etter min oppfatning bør det derfor kreves at arbeidsgiver dokumenterer hastigheter som ligger langt lavere enn normalt for at kontroll av loggene rettmessig skal kunne karakteriseres som administrativ kontroll, jf. bokstav a). På den annen side vil det være komplisert å skulle dokumentere at arbeidsgiver rent faktisk *ikke* har ansett kapasitetsproblemene som så overhengende at han følte behov for administrasjon i form av kontroll av systemet.

5.1.3 Kan kontrolltiltak hjemles i personopplysningsforskriften § 7-11?

Ovenfor er det gjort rede for personopplysningsforskriften § 7-11 og dens unntak fra meldepliktreglene i personopplysningsloven. Etter å ha analysert rettspraksis på området synes det imidlertid som om domstolene har tillagt bestemmelsen en videre betydning enn det ordlyden gir grunnlag for. Forskriften § 7-11 sier ikke at logging er tillatt når den utføres i forbindelse med administrasjon og/eller sikkerhetsrutiner. Den sier heller ikke at innholdet i loggene senere kan kontrolleres dersom opplysningene var samlet inn på bakgrunn av disse formålene.[162] Bestemmelsen åpner etter ordlyden kun for *unntak fra meldeplikten* i personopplysningsloven i visse tilfeller, samt at den oppstiller et eksplisitt forbud mot senere bruk av innsamlede opplysninger i kontrolløyemed. Hvorvidt en behandling har rettslig hjemmel, og hvorvidt en behandling er meldepliktig, er to vidt forskjellige spørsmål. Høyesterett synes imidlertid å ha tolket forskriftsbestemmelsen slik at behandlingen er rettmessig der den har som formål å administrere systemet, jf. Raufoss-dommen.[163] Tilsvarende ble lagt til grunn av Gulating lagmannsrett i kjennelsen av 19. februar 2003. Jeg stiller meg noe uforstående til at Hovedforskriften § 2-20 og personopplysningsforskriften § 7-11 nærmest fremstår som selvstendige hjemmelsgrunnlag i forhold til kontroll av datalogger. Hjemmelen for behandling av personopplysninger må i utgangspunktet søkes i samtykke, lovhjemmel eller popplyl. § 8 bokstavene a) til f), og ikke i en forskriftsbestemmelse som gjør

---

[162] Dette vil trolig også være behandling som er *uforenlig* med det opprinnelige formålet bak innsamlingen, og derfor også i strid med popplyl. § 11 (1) bokstav c).

[163] I Raufoss-dommen var det henvist til personregisterlovens hovedforskrift § 2-20 (2) – nå videreført i personopplysningsforskriftens § 7-11 (2).

unntak fra meldeplikten. Det fremgår imidlertid ikke klart av de nevnte avgjørelsene at det er via popplyl. § 8 domstolene har resonnert. Domstolene synes å ha "hoppet over" den rettslige vurderingen etter popplyl. § 8, og forutsatte at forskriften hjemlet de aktuelle behandlingene. Høyesterett uttalte i Raufoss-dommen at de *"ikke kan se at hovedforskriftens § 2-20 annet ledd utgjør noe hinder (...)"*. At forskriftsbestemmelsen ikke utgjorde noe *hinder* for kontrolltiltaket er vel korrekt. Noe helt annet er imidlertid å slutte *fra denne bestemmelsen* at kontrolltiltaket er tillatt.[164]

Til tross for min skepsis til domstolenes rettskildebruk i de to nevnte avgjørelsene, er jeg likevel enig i at forskriften § 7-11 kan gi viktig veiledning i forhold til vurderingen av kontrolltiltakenes rettmessighet. Dersom behandlingen av personopplysninger skjer innenfor rammene av § 7-11, vil dette måtte telle med i avveiningen etter personopplysningsloven § 8, jf. § 11. Informasjonssikkerhet og behov for administrasjon av datasystemene vil derfor kunne utgjøre tungtveiende interesser i forhold til nødvendighetsavveiningen etter § 8, samt i forhold til de lovfestede og ulovfestede kravene til saklighet og proporsjonalitet.

5.2 Kontroll av e-post

5.2.1 Skillet mellom privat og virksomhetsrelatert e-post

Adgangen til å kontrollere e-post i arbeidslivet har i teori og rettspraksis blitt knyttet opp mot skillet mellom *privat* og *virksomhetsrelatert* e-post. Sondringen har ingen konkrete holdepunkter i personopplysningsloven, men er likevel relevant i forhold til vurderingen av hvorvidt et kontrolltiltak er nødvendig eller ikke og hvorvidt arbeidsgiver har en *berettiget interesse* etter popplyl. § 8 bokstav f). For å kartlegge rettsstillingen i Norge på dette punktet, er man henvist til å analysere den begrensede rettspraksisen på området.[165]

---

[164] Etter hovedforskriftens § 2-20 hadde man ingen bestemmelse som tilsvarte personopplysningsforskriftens § 7-11 (3).

[165] I den finske "lag om integritetsskydd i arbetslivet" er spørsmålet særregulert, jf. § 9, hvor det er nedlagt forbud mot at arbeidsgiver går inn på private e-post-meldinger.

> For ordens skyld vil jeg gjengi Datatilsynets retningslinjer omkring kontroll av e-post på arbeidsplassen: *"Det er viktig å skille mellom privat og virksomhetsrelatert e-post. Arbeidsgiveren din har ikke adgang til å lese e-post du mottar som privatperson uten at du har samtykket. Dette gjelder selv om arbeidsgiveren må sies å være "eier" av datasystemet. Arbeidsgiveren har imidlertid rett til innsyn i virksomhetsrelatert e-post. Arbeidsgiverens interesse i å lese disse meldingene overstiger hensynet til ditt personvern"*. Retningslinjene ble publisert på Datatilsynets nettsider 23.05.2001, "Arbeidsgivers innsyn i de ansattes e-post – spørsmål og svar".[166]

Dommen inntatt i RG 1993 side 77 ("Memorex-dommen") omhandlet en systemkonsulent ("arbeidstakeren") som hadde blitt oppsagt fra sin stilling. [167] Arbeidstakeren ble i oppsigelsestiden oppmerksom på at administrerende direktør ("arbeidsgiver") hadde gått inn på hans private brukerområde i bedriftens databaserte postsystem. Arbeidsgiver hadde i forbindelse med kontrolltiltaket oppdaget forhold som medførte at arbeidstakeren ble avskjediget. I avskjedssaken fremkom spørsmålet om arbeidsgivers handling var i strid med de ulovfestede reglene om vern av den personlige integritet. Retten la til grunn at bedriftsledelsen måtte ha tilgang til *åpne brukerområder*, da de kunne ha behov for å hente ut bedriftsinformasjon som lå der. Det arbeidsgiver hadde gjort i dette tilfelle, var imidlertid å skaffe seg tilgang til et brukerområde som i retningslinjene for bruk av datasystemet var merket med "privat". Retten fant at dette kunne være lov dersom de ansatte på forhånd var blitt varslet om at arbeidsgiver hadde adgang til dette – noe som ikke var tilfelle i denne saken. Retten uttalte således:

> *"Etter rettens oppfatning må det forhold at ledelsen uten den ansattes viten går inn på de ansattes "private" område på dataanlegget, anses som et inngrep i den personlige integritet. Retten ser det slik at det er en viktig side ved det ulovfestede personvern at en ansatt skal kjenne til hvilke opplysninger og dokumenter arbeidsgiver har tilgang til (...)".*

I Rt. 2002 side 1500 la Høyesteretts kjæremålsutvalg til grunn tilsvarende synspunkter som de som ble skissert i underrettsdommen. Denne kjennelsen er avsagt på et tidspunkt

---

[166] Se < http://www.datatilsynet.no/dtweb/attachment/823/epost.html > (13.10.2003).

[167] Asker og Bærum herredsretts dom av 30. april 1992.

hvor bruken av e-post har utviklet seg enormt i forhold til situasjonen i 1992, og hvor skillet mellom privat og virksomhetsrelatert e-post har blitt mer fremtredende enn den gang. Et av hovedspørsmålene var om e-post som var sendt til og fra arbeidstakers e-post adresse hos arbeidsgiver, uten samtykke kunne fremlegges som bevis i en avskjedssak. Arbeidstakeren hadde blitt oppsagt fra sin stilling i bedriften pga rasjonaliseringstiltak. Vedkommende hadde fått tillatelse til å drive aktiv jobbsøking i oppsigelsestiden, men tillatelsen ble etter hvert trukket tilbake. Arbeidsgiver hadde senere kontrollert e-post- loggene, hvor det ble oppdaget en rekke e-postmeldinger fra arbeidstakeren til et konkurrerende firma i Sverige. Bakgrunnen var at det under rutinemessig backup/sikkerhetskopiering av filer på datasystemet ble oppdaget e-post fra arbeidstakeren til det svenske selskapet. Det ble deretter utført en rekke avgrensede søk på bedriftens server, hvor flere e-postmeldinger ble funnet. E-posten viste at arbeidstakeren angivelig hadde inngått ny arbeidsavtale med det svenske selskapet, samtidig som han hadde forsøkt å trekke sine forretningsforbindelser inn i samarbeid med dette selskapet. Herredsretten nektet e-post meldingene fremlagt som bevis i oppsigelsessaken. Kjennelsen ble påkjært til Borgarting lagmannsrett, som kom til motsatt resultat.[168] Saken gjaldt i realiteten et bevisavskjæringsspørsmål, men vurderingen av hvorvidt personopplysningslovens regler var brutt ville ha betydning for dette spørsmålet – til tross for at det ikke er gitt at slike bevis vil bli avskåret selv om de er innhentet på lovstridig måte. Arbeidstakeren hevdet at e-posten var av privat karakter, da innholdet relaterte seg til hans jobbsøking. Lagmannsretten var ikke enig i dette, da meldingene også omhandlet det svenske selskapets etableringsplaner i Norge. I denne sammenheng uttalte lagmannsretten:

> *"(...) A synes å ha gjort et vesentlig poeng av at meldingene må anses som private fordi de angår hans egne aktiviteter og planer i forbindelse med den jobbsøkingsprosess han var inne i, og at han i denne sammenheng ikke handlet for X. Lagmannsretten stiller seg tvilende til om dette er noe egnet kriterium i den spesielle situasjon som her foreligger. Så vidt skjønnes er det ikke omstridt at meldingene, eventuelt med unntak for bilag 7, gjelder forberedelse til eller har nær sammenheng med mulig ansettelse av A i Z AB, et firma som tar sikte på å bygge opp virksomhet i Norge som vil komme i et direkte konkurranseforhold med X. Planer om slik etablering vil klarligvis være av stor interesse for X og slik sett ha*

[168] Borgarting Lagmannsretts kjennelse av 24.09.2002 (LB-2002-02299).

direkte betydning for Xs virksomhet. Når til og med en av Xs egne ansatte er en drivende kraft i dette arbeid, er det - fra X sitt ståsted - nærliggende å oppfatte de omtalte aktiviteter som virksomhetsrelaterte. Lagmannsretten viser for øvrig til opplysningene om hvordan A har angitt avsender på meldingene, og nøyer seg med å konstatere at meldingene med minst like stor rett kan hevdes å være virksomhetsrelaterte som private".

Kjennelsen ble påkjært til Høyesteretts kjæremålsutvalg, men ble opprettholdt. Kjæremålsutvalget kunne ikke se at lagmannsretten hadde feiltolket personopplysningsloven, da sondringen mellom virksomhetsrelatert og privat e-post var relevant i forhold til vurderingen av arbeidsgivers *berettigede interesse*, jf. § 8 bokstav f). Kjæremålsutvalget viste i denne sammenheng til Datatilsynets retningslinjer, jf. ovenfor. Deler av retningslinjene ble gjengitt ordrett i kjennelsen, noe som i seg selv er litt kuriøst.

Lagmannsrettens og kjæremålsutvalgets sondring mellom privat og virksomhetsrelatert e-post, samt betydningen av sondringen i forhold til hjemmelsgrunnlaget i personopplysningsloven, synes å være uttrykk for gjeldende rett. At e-post med slikt innhold kunne karakteriseres som virksomhetsrelatert i sin helhet, synes jeg imidlertid fremstår som noe urimelig. Arbeidstakeren hadde drevet aktiv jobbsøking mv. – vel å merke i strid med hva som var tillatt partene i mellom – og til tross for at arbeidsgiver kunne ha stor interesse i innsyn i disse forhold, synes jeg begrepet "virksomhetsrelatert" ble strukket vel langt i denne saken.

Som det vil bli redegjort for i kapittel 6, har arbeidsgivers informasjonsplikt stor betydning for adgangen til å kontrollere arbeidstakernes e-post. Privat e-post kan aldri kontrolleres uten samtykke fra vedkommende arbeidstaker, jf. Rt. 2002 side 1500. Er det er snakk om virksomhetsrelatert e-post, kan det tenkes å være en forutsetning at arbeidstakerne har blitt informert av arbeidsgiver om at denne typen e-post vil kunne bli kontrollert.

Til tross for at man nå har et relevant rettslig skille mellom privat og virksomhetsrelatert e-post, er det likevel ikke alltid så lett å avgjøre hva som er privat og hva som er

virksomhetsrelatert. I SOU 2002: 18 på side 101 flg. har det svenske utvalget kort drøftet begrepet "privat", og uttalte i denne sammenheng:

> *"Här avses uppgifter som är privata i den meningen att de är hänförliga till arbetstagaren som privatperson i motsats til sådana uppgifter som är hänförliga till arbetet eller annars till arbetstagarens egenskap av just arbetstagare (...)".*

Uttalelsen gir kanskje ikke mye veiledning, men tar likevel fatt i det mest sentrale momentet – nemlig hvorvidt opplysningene er fremkommet i regi av arbeidstakeren som privatperson eller i regi av arbeidstakeren som nettopp arbeidstaker. E-post med rent personlig innhold (eksempelvis meldinger til venner og bekjente) bør normalt ikke by på særlige problemer. Det samme gjelder e-post som åpenbart relateres til bedriftens virksomhet (eksempelvis jobbrelatert korrespondanse med kunder/klienter, samarbeidspartene e.l.). Situasjonen er imidlertid mer komplisert når det gjelder e-post som kommer i en slags mellomstilling, noe Rt. 2002 side 1500 etter min mening bærer bud om.

Domstolenes sondring mellom privat og virksomhetsrelatert e-post kan imidlertid gi uheldige resultater, dersom den ikke klargjøres ytterligere. Man kan ikke ut fra foreliggende rettskilder slutte at kontroll av virksomhetsrelatert e-post alltid vil være rettmessig. I tillegg til kravene i popplyl. § 8, gjelder lovens øvrige krav fullt ut – herunder grunnkravene i § 11. Tilsvarende vil ulovfestet rett kunne komme inn som begrensning. En ting er at arbeidsgiver *presumptivt* vil ha et reelt, saklig behov for kontroll av virksomhetsrelatert e-post, jf. for så vidt punkt 3.4.2. En annen ting er at den konkrete situasjonen kan tilsi at arbeidsgiver ikke har rettslig adgang til slik kontroll. Dersom kontrolltiltaket ikke har formål som er saklig begrunnet i hans virksomhet, dersom de behandlede opplysningene ikke er relevante i forhold til behandlingens formål, eller dersom kontrolltiltaket går ut over hva som må anses proporsjonalt, er kontrolltiltaket likevel ikke rettmessig. I tillegg til disse kravene kommer også informasjonsplikten inn som begrensning, jf. ovenfor og kapittel 6 nedenfor. Disse presiseringene er utelatt i Datatilsynets retningslinjer, jf. note 166 ovenfor, noe som kan gi uheldige signaleffekter. Tilsvarende gjelder de nevnte lovfestede og ulovfestede begrensningene i forhold til kontroll av privat e-post. Adgangen til å kontrollere

arbeidstakernes private e-post er således ikke ubegrenset selv om det foreligger et gyldig samtykke. Dette følger blant annet av at popplyl. § 11 oppstiller visse grunnkrav *i tillegg* til kravene i popplyl. § 8. På samme måte vil de ulovfestede arbeidsrettslige prinsippene komme inn som begrensning uavhengig av hvilket rettslig grunnlag som ligger til grunn for kontrolltiltaket. Tiltaket må i alle tilfeller være saklig begrunnet, og det må være forholdsmessighet mellom arbeidsgivers interesse i å foreta kontrolltiltaket og de personverninteressene som eventuelt krenkes. At det er avgitt samtykke vil imidlertid kunne få betydning for de skjønnsmessige avveiningene som må foretas i forhold til disse begrensningene, på samme måte som det vil kunne virke inn i vurderingen etter popplyl. § 8 bokstav f) at den registrerte har gitt uttrykk for at han ikke ønsker at behandlingen skal gjennomføres eller fortsette, jf. Ot.prp. nr. 92 (1998-99) på side 109, jf. punkt 3.4.3 ovenfor.

5.2.2 Skillet mellom e-post og logger

I punkt 5.1 flg. ble det gjort rede for logging av personopplysninger og adgangen til å kontrollere innholdet i dataloggene. I punkt 5.2.1 er det videre gjort rede for adgangen til å kontrollere arbeidstakernes e-post. Det kan derfor synes som om man snakker om to vidt forskjellige ting. Dette er imidlertid ikke helt treffende. E-post kan også kontrolleres ved bruk av loggene. Drøftelsene omkring adgangen til å logge opplysninger i datasystemet, samt senere kontroll av innholdet i disse loggene, har derfor i utgangspunktet overføringsverdi hva gjelder kontroll av e-post.

Man må skille mellom de ulike stadiene i kontrollen. Man kan avlese såkalt *trafikkdata* ved hjelp av eksempelvis POP-loggen og SMTP-loggen. Med dette menes typisk avlesning av hvem som har sendt e-posten, hvem som har mottatt den og når dette har skjedd. Trafikkdataene kan gi visse indikasjoner på hvorvidt det er snakk om privat eller virksomhetsrelatert e-post. Dersom avsenderadressen, mottakeradressen eller ”subject-feltet” tydelig tilkjennegir at det er snakk om privat e-post, plikter arbeidsgiver å stoppe behandlingen umiddelbart. Dersom trafikkdataene derimot ikke gir tilstrekkelig informasjon, kan det være nødvendig med ytterligere undersøkelser, eksempelvis ved å bruke loggene til å sjekke det konkrete innholdet i e-posten. Arbeidsgiver har imidlertid ikke adgang til å tilegne seg overskuddsinformasjon, noe som innebærer at

behandlingen av personopplysninger må stoppe i det øyeblikk arbeidsgiver oppdager at det er snakk om privat e-post. Bruk av loggene til å kontrollere såkalt trafikkdata antas å følge reglene for kontroll av datalogger generelt. Nærmere undersøkelser av *innholdet* i e-posten følger imidlertid de regler som har fremkommet gjennom rettspraksis. Det vil si at virksomhetsrelatert e-post kan kontrolleres under visse forutsetninger, mens privat e-post aldri kan kontrolleres uten arbeidstakerens samtykke.

5.2.3 Web-basert e-post

Redegjørelsene ovenfor har vært basert på situasjoner hvor arbeidstakeren har anvendt arbeidsgivers e-postserver i forbindelse med sending og mottak av e-post. Nok et problem reiser seg når arbeidstakeren benytter seg av andre e-posttjenester, eksempelvis en gratis web-basert tjeneste som Hotmail.[169] I disse tilfellene vil e-posten ikke bli avsendt fra eller mottatt via arbeidsgivers e-postsystem, men befinner seg i utgangspunktet på tjenesteleverandørens (Microsofts) server. Når arbeidstakeren benytter seg av Hotmail er arbeidsgiver således ikke "eier" av e-post serverne, selv om han kanskje eier datamaskinen og står ansvarlig for internettforbindelsen.

Opplysninger om *innholdet* i web-basert e-post vil *normalt* ikke kunne logges. Innholdet vil ofte være kryptert, og dermed kun tilgjengelig for brukeren og tjenesteleverandøren. At vedkommende har vært inne på www.hotmail.com kan derimot logges, og det kan også logges opplysninger om tidspunkter for aktivitetene – noe som i sin tur kan gi en viss pekepinn om hvor mye tid vedkommende har brukt på ikke-jobbrelaterte aktiviteter. Opplysningene er derfor tilsvarende de som kan logges i forbindelse med alminnelig bruk av internett. Sondringen mellom de ulike typene e-post er derfor antakelig mindre relevant her. Det eksisterer imidlertid programvare som åpner for logging også av innholdet i denne typen e-post meldinger. Programvaren er visst nok forholdsvis utbredt blant arbeidsgivere i USA, men foreløpig ikke i Norge.

---

[169] Jeg har ikke funnet verken rettspraksis eller litteratur hvor denne problemstillingen har blitt drøftet. Datatilsynet har tilsynelatende heller ikke behandlet denne typen saker. Mine drøftelser vil derfor være basert på reelle hensyn og paralleller fra de retningslinjene som er skissert ovenfor.

Dersom norske arbeidsgivere fikk tilgang til denne typen programvare, vil skillet mellom privat og virksomhetsrelatert e-post likevel kunne være relevant. At e-posten kan tenkes å bli brukt i jobbsammenheng, og at arbeidsgivers interesse i innsyn derfor er stor, er en ting. Noe annet er at denne typen e-posttjenester strengt tatt må anses å være *"mer privat"* enn en e-posttjeneste som er gjort tilgjengelig for arbeidstakerne i regi av arbeidsgiver. Dette synspunktet vil etter min oppfatning ha stor betydning i forhold til den rettslige avveiningen av kontrolltiltakets rettmessighet, og utgangspunktet vil derfor være at kontroll av denne typen opplysninger ikke kan foretas uten samtykke fra arbeidstakeren selv.

5.2.4 Bruk av private e-postkontoer via arbeidsgivers nettverk

En annen tenkelig problemstilling reiser seg der arbeidstaker har opprettet en privat e-postkonto (eksempelvis ola@nordmann.no), men benytter seg av arbeidsgivers internettilkobling når han sender/mottar e-post. Det kan tenkes at vedkommende enten benytter en pc på jobben, en privat bærbar pc som tilknyttes nettet på jobben, eller at arbeidsgiver har tilrettelagt for oppkobling hjemmefra. Her vil opplysningene også kunne logges i arbeidsgivers system. I disse tilfellene må det etter min oppfatning være åpenbart at e-posten er privat – uavhengig av om arbeidsgiver kunne ha en sterk interesse i å gjøre seg kjent med innholdet i e-posten. Arbeidstaker vil i disse tilfellene ha en klar og berettiget forventning om diskresjon, og jeg kan vanskelig tenke meg situasjoner hvor hensynet til arbeidsgiver her må gå foran hensynet til den ansattes personvern.[170] Dersom det ved en tilfeldighet oppdages spor av barnepornografi på arbeidsgivers server, kan ikke arbeidsgiver selv kontrollere sine ansattes private e-postkontoer. Da må han i stedet varsle politiet, som vil ha en videre rettslig adgang til kontroll enn arbeidsgiver. Forfølgelse av straffbare handlinger er et offentlig anliggende, og det er derfor ingen grunn til å gi arbeidsgiver noen utvidede rettigheter i slike tilfeller. Se også punkt 6.2 nedenfor.

---

[170] Arbeidstaker vil i disse tilfellene normalt ha to e-postadresser; en privat og en som er forutsatt virksomhetsrelatert. En slik anordning i regi av arbeidsgiver kunne løse mange vanskelige spørsmål i forhold til grensedragningen med privat og virksomhetsrelatert e-post i de tilfeller de ansatte har fått tillatelse til å benytte IT-utstyret i privat øyemed.

5.2.5 Alternative kontrollmetoder

Det kan tenkes at arbeidsgiver ønsker å benytte seg av andre metoder enn kontroll av loggene for å kontrollere den ansattes e-post. Et eksempel kan være at arbeidsgiver tilegner seg den ansattes brukernavn og passord og går inn på vedkommendes brukerområde, jf. RG 1993 side 77. Deretter kan han enten kontrollere de lokale loggene på vedkommendes brukerområde, eller åpne e-postprogrammet og tilegne seg den ønskede informasjonen. Det kan tenkes at partene har en avtale om dette, og at samtykkereglene eller popplyl. § 8 bokstav a) gir arbeidsgiver rett til dette. Hvis en slik avtale er kommet i stand for å sikre at arbeidstakerens ferieavvikling, sykdom eller liknende ikke rammer virksomheten, må arbeidsgiver likevel holde seg innenfor rammene av samtykket og/eller avtalen. Er det avtalt at arbeidsgiver kun skal kunne lese virksomhetsrelatert e-post, er dette bindende for ham. Privat e-post skal da forbli privat, og stillingen er neppe noen annen enn hvor vedkommende tilegner seg informasjonen via loggene på bedriftens hovedserver. Dersom en slik avtale derimot ikke foreligger, vil denne fremgangsmåten kanskje fremstå som enda mer krenkende overfor arbeidstakeren – til tross for at den informasjonen som behandles ikke atskiller seg fra de opplysninger som kan logges via arbeidsgivers sentrale datasystem. Hvilken rettslig adgang arbeidsgiver har til dette – sett i sammenheng med de retningslinjene som er skissert overfor – er det vanskelig å si noe om. Skillet mellom virksomhetsrelatert og privat e-post er i utgangspunktet oppstilt som en del av den vurdering som må foretas etter § 8 bokstav f). At arbeidsgiver da i tillegg har tilegnet seg brukernavn og passord vil kunne slå desto mer negativt ut i interesseavveiningen. I Raufoss-dommen var det stilt spørsmål om hvorvidt det innebar en ytterligere krenkelse at arbeidsgiver hadde låst seg inn på den ansattes kontor og fysisk kontrollert den ansattes datamaskiner, men Høyesterett tok ikke stilling til dette spørsmålet.[171] Etter min oppfatning innebar arbeidsgivers handling i denne saken en åpenbar tilleggskrenkelse, selv om jeg i og for seg er enig i resultatet i dommen.

[171] Rt. 2001 side 1589.

6 Informasjonsplikt

6.1 Innledning

I dette kapitlet skal det redegjøres for informasjonsplikten etter personopplysningsloven og det ulovfestede arbeidsrettslige regelverket. Bakgrunnen for at denne plikten gjøres rede for, mens bl.a. reglene om innsynsrett og melde- og konsesjonsplikt mv. ikke behandles, er at informasjonsplikten er antatt å være av sentral betydning for den rettslige vurderingen av kontrolltiltakenes rettmessighet. Det er ikke med dette siktet til at de øvrige reglene ikke er viktige; saken er den at tiltakets alvorlighetsgrad til en viss grad avhenger av om arbeidstakeren på forhånd er kjent med arbeidsgivers praksis på dette området. Det foreligger i alle fall en presumsjon for at arbeidstakerne finner det mer krenkende å få høre i ettertid at arbeidsgiver har kontrollert deres e-post e.l., enn å bli gjort kjent med arbeidsgivers praksis gjennom arbeidsavtalen eller interne instrukser på forhånd. Krenkelsesgraden vil i sin tur kunne ha betydning for blant annet avveiningen etter popplyl. § 8 bokstav f).

6.2 Personopplysningslovens regler om informasjonsplikt

I personopplysningsloven er informasjonsplikten regulert i §§ 19 og 20, jf. 23. Bestemmelsene bør sees i sammenheng med arbeidstakerens (og andres) rett til innsyn etter § 18. Popplyl. § 19 regulerer situasjonen når *den behandlingsansvarlige* samler inn personopplysninger *fra den registrerte selv*. Informasjonen skal gis av eget tiltak, dvs. at arbeidstaker ikke trenger å be om den (slik innsynsretten i § 18 er utformet), jf. Ot.prp. nr. 92 (1998-99) på side 119. Bestemmelsen bygger på personverndirektivets artikkel 10.[172] Når personopplysninger samles inn fra *andre enn* den registrerte reguleres forholdet av § 20.

Innsamling fra den registrerte selv vil for det første omfatte situasjoner hvor arbeidsgiver henvender seg direkte til arbeidstakeren og ber denne om opplysninger.

[172] Informasjonsplikt følger også av de ulovfestede reglene, jf. nedenfor, men man har der ingen særskilt regel om tilfeller hvor arbeidstakeren selv er informasjonskilden ved innsamling av opplysninger om seg selv.

Både skriftlige og muntlige henvendelser er omfattet. Lovgiver har brukt formuleringen "samles inn". Dette fordrer følgelig en viss aktivitet fra den behandlingsansvarlige, og omfatter ikke tilfeller hvor han/hun mottar informasjonen fra arbeidstakeren uten å ha bedt om den. For det annet omfattes innsamling av opplysninger som skjer ved elektroniske hjelpemidler. Bestemmelsen passer dårlig i forhold til tilfeller hvor innsamlingen skjer via en datamaskin og hvor opplysningene behandles gjennom denne. Ordlyden synes å forutsette innsamling fra en fysisk person. Tilsvarende er popplyl. § 20 utformet med tanke på andre fysiske personer enn den registrerte. I forarbeidene til § 19 nevnes imidlertid registrering av elektroniske spor som den registrerte etterlater seg i systemer for betalingsformidling, elektroniske informasjonssystemer eller gjennom systemer fra elektronisk handel.[173] Innsamling av opplysninger fra den registrerte omfatter trolig derfor både opplysninger som innsamles via loggtjenestene og opplysninger som arbeidstakerne aktivt legger igjen.[174] At logging omfattes har ingen direkte forankring i verken lovtekst eller forarbeider, men slutningen må kunne trekkes ved å se hen til forarbeidenes eksemplifisering. Reelle hensyn taler derfor for at også elektroniske spor i form av loggopplysninger omfattes, til tross for at det kanskje er vanskelig å lese ut fra lovteksten at innhenting av loggopplysninger innebærer innsamling *"fra den registrerte selv"*.

I Ot.prp. nr. 92 (1998-99) på side 119 er det gjort unntak fra informasjonsplikten for innsamling av elektroniske spor som er nødvendige for å gjennomføre tekniske prosesser, og som utelukkende nyttes til dette. Et slikt eksempel kan være logging av opplysninger i et datasystem som ledd i administrative rutiner eller for å avdekke brudd på informasjonssikkerheten, jf. også Kommentarutgaven på side 159. Denne form for behandling av personopplysninger er jo også unntatt fra meldeplikten etter forskriftens § 7-11. Dersom loggingen derimot skjer med det formål å overvåke den enkelte arbeidstaker, utløses likevel informasjonsplikten.

---

[173] Se Ot.prp. nr. 92 (1998-99) side 119. At bestemmelsen omfatter innsamling som skjer med datamaskiner er også lagt til grunn av Schartum i Norsk Lovkommentar, note 69 til popplyl. § 19.

[174] Se også Kommentarutgaven på side 159.

Etter § 19 (1) bokstav a) skal arbeidsgivers navn og adresse, eventuelt navn og adresse på representanten, fremgå av informasjonen. Etter bokstav b) skal formålet med behandlingen av personopplysninger fremgå. Denne bestemmelsen må følgelig sees i sammenheng med grunnkravene for behandling av personopplysninger, og formålsangivelsen må trolig oppfylle kravene i popplyl. § 11. Etter bokstav c) skal det oppgis hvorvidt andre enn arbeidsgiver/behandlingsansvarlig skal få opplysningene utlevert, eventuelt også hvem disse mottakerne er. Utgangspunktet etter § 19 er jo at den registrerte selv skal få bestemme om han ønsker å gi den behandlingsansvarlige opplysningene, og da vil det ofte være avgjørende å vite hvem som får tilgang til denne informasjonen. Etter bokstav d) skal det klart fremgå om det er frivillig for den registrerte å gi fra seg opplysningene. Arbeidstakerne skal etter dette ikke oppgi informasjonen i den tro at de er forpliktet til dette. Dersom arbeidsgiver med hjemmel i lov kan kreve opplysningene utlevert, har man et tilfelle hvor det ikke er frivillig. Da må arbeidsgiver trolig i stedet oppgi den rettslige hjemmelen hun/han bygger sitt *utleveringskrav* på, jf. Kommentarutgaven på side 160. Som påpekt i Kommentarutgaven følger dette ikke direkte av bokstav d), men er mer en konsekvens av at den behandlingsansvarlige plikter å gi den registrerte nok informasjon til at den registrerte er i stand til på best mulig måte å gjøre bruk av de øvrige rettigheter han har etter loven – eksempelvis innsyn etter § 18 og retting og sletting etter §§ 27 og 28, jf. § 19 (1) bokstav e).[175] Bokstav e) pålegger den behandlingsansvarlige å selv vurdere hvilken informasjon den registrerte trenger for på best mulig måte å ivareta sine øvrige rettigheter, men Datatilsynet kan overprøve denne vurderingen.

Informasjonen kan gis både skriftlig[176], muntlig[177] og elektronisk[178], men skal gis forut for innsamlingen, jf. *"først (...)"*. Ved at det ikke oppstilles noe konkret krav til tidsperspektiv, innebærer dette antakeligvis at arbeidsgiver kan varsle vedkommende allerede i arbeidsavtalen eller i interne instrukser. Konsekvensen er at varslet kanskje

---

[175] Disse rettighetene er kun eksempler, jf. *"f.eks."* i § 19 (1) bokstav e). Oppramsingen er med andre ord ikke ment å være uttømmende.

[176] Se popplyl. § 24.

[177] Den registrerte kan imidlertid kreve informasjonen nedfelt skriftlig med hjemmel i popplyl. § 24.

[178] Se Ot.prp. nr .92 (1998-99) på side 119, annen spalte.

blir gitt lang tid forut for innsamlingen av personopplysningene. Departementet har ikke i forarbeidene uttrykt noen skepsis i denne forbindelse, men personlig synes jeg denne løsningen er noe uheldig. Arbeidsgiver vil kunne samle inn personopplysninger om arbeidstakerne på alle tenkelige tidspunkter (se § 19 (2)), uten at arbeidstakeren har krav på noe spesifisert varsel i så henseende.

Bakgrunnen for at varslet skal gis forut for innsamlingen er følgelig at den registrerte skal gis anledning til å nekte å gi fra seg opplysningene dersom vedkommende ikke har tillitt til at behandlingen skjer på en betryggende måte. Dette hensynet kommer ikke inn der den registrerte ikke frivillig gir fra seg opplysningene, eksempelvis der arbeidsgiver med hjemmel i lov krever dem utlevert. Informasjonen skal likevel gis forut for behandlingen også i disse tilfellene. Det er tilstrekkelig at informasjonen gis en gang, dersom tilsvarende behandling av personopplysninger skjer over tid. Dette følger av annet ledd, som gjør unntak fra informasjonsplikten i de tilfeller "*det er på det rene*" at den registrerte kjenner til den informasjon som skal gis etter første ledd, bokstavene a) til e). Dette er et strengt beviskrav, og innebærer at den behandlingsansvarlige må være helt sikker på at den registrerte er inneforstått med informasjonen som nevnt i første ledd, jf. Ot.prp. nr. 92 (1998-99) på sidene 43 og 119.

Konsekvensen av § 19 er at alle loggopplysninger som ikke samles inn utelukkende for gjennomføring av tekniske prosesser mv., skal varsles arbeidstakerne i forkant, jf. Ot.prp. nr. 92 (1998-99) på side 119. Bestemmelsen omfatter imidlertid kun *innsamling* av personopplysninger. Senere behandling av de innsamlede opplysningene er ikke omfattet av ordlyden. Forarbeidene sier heller ingenting om dette. Det kan således virke som at den behandlingsansvarlige ikke har noen plikt til å varsle om senere bruk av opplysningene, dersom slik senere bruk blir besluttet etter at opplysningene er samlet inn. Det er eksempelvis vanskelig å karakterisere en etterfølgende kontroll av loggopplysninger som en ny innsamling. Kanskje vil en slik etterfølgende behandling være den som er mest betenkelig i et personvernrettslig perspektiv. Resultatet er at arbeidsgiver plikter å opplyse alle ansatte at opplysninger om internettbruk, bruk av e-post o.l. vil bli registrert, men at det ikke foreligger noen plikt til å gi informasjon dersom han senere ønsker å kontrollere nærmere hva slags aktiviteter arbeidstakerne har foretatt. I arbeidslivet vil personopplysningsloven bli supplert av ulovfestede

arbeidsrettslige regler om informasjonsplikt, jf. nedenfor, og de praktiske konsekvensene er derfor ikke særlig store her. Det er likevel betenkelig at lovgiver har valgt å se bort fra, eventuelt oversett, konsekvensene av denne begrensningen i informasjonsplikten. På den annen side vil arbeidsgiver ikke ha lov til å behandle de innsamlede opplysningene i kontrolløyemed, dersom de ble samlet inn på bakgrunn av sikkerhetsmessige eller administrative formål, jf. § 11 (1) bokstav c). Ovenfor er det videre lagt til grunn at den behandlingsansvarlige først samler inn opplysningene, og *deretter* bestemmer seg for ytterligere behandling av disse. Hvis den etterfølgende bruk er besluttet allerede *forut for* innsamlingen, vil han imidlertid plikte å informere den registrerte om dette etter regelen i § 19 (1) bokstav b). Senere bruk av opplysningene vil da være en del av formålet bak innsamlingen, og dette skal klart fremgå av den informasjon som skal gis etter bokstav b).

Popplyl. § 20 regulerer eksempelvis situasjonen der arbeidsgiver henvender seg til leverandørene av nettsidene (for eksempel Microsoft) for å kunne samle inn informasjon om de ansattes internettaktiviteter, jf. *"fra andre enn den registrerte"*. Det kan tenkes at arbeidsgivers egne loggfunksjoner ikke har fanget opp den ønskede informasjonen. Det vil imidlertid føre for langt å drøfte bestemmelsen opp mot denne typen situasjoner.[179]

Det finnes en rekke unntak fra informasjonsplikten i popplyl. § 23, i tillegg til bestemmelsen i § 19 (2). De fleste av unntakene er av mindre interesse i forhold til dette emnet, men § 23 (1) bokstav b) bør behandles kort. Denne bestemmelsen gjør unntak fra informasjonsplikten der hemmelighold er påkrevd av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger. Etter det jeg har erfart gjennom massemedia, og til dels også rettspraksis, har en rekke arbeidsgivere kommet over straffbart materiale ved å kontrollere innholdet i loggene på sine servere. De siste årene har flere arbeidstakere mistet jobben og blitt idømt straff for innsamling, oppbevaring og distribuering av barnepornografi. Det kan også tenkes andre straffbare handlinger enn dette, men eksemplet er tilstrekkelig til å belyse de rettslige

[179] Se imidlertid Ot.prp. nr. 92 (1998-99) på side 119-120, NOU 1997: 19 på side 147-148 og Kommentarutgaven på side 162-167.

spørsmålene. Gitt at arbeidsgiver har mistanke om at en eller flere av sine ansatte har befatning med barnepornografisk materiale. Dersom den/de "skyldige" sitter inne med tilstrekkelig kunnskap til å kunne slette de elektroniske sporene fra serveren, og i tillegg har praktisk mulighet til å gjøre dette, ville det kunne vanskeliggjøre etterforskningen dersom innsamlingen av opplysningene ble varslet på forhånd. Alle spor ville kunne forsvinne før politiet kommer på banen. Popplyl. § 23 (1) bokstav b) vil imidlertid ikke gi *arbeidsgiver* rett til samle inn opplysningene uten å varsle arbeidstakerne. Etterforskning av straffbare handlinger er et offentlig anliggende, og det fremgår av forarbeidene at det i bokstav b) er siktet til etterforskning som reguleres av straffeprosesslovens kapittel 18. Det vil si at unntaket fra informasjonsplikten kun gjelder dersom innsamlingen skjer i regi av politiet eller andre offentlige kontrolletater, jf. Ot.prp. nr. 92 (1998-99) på side 121.[180]

6.3 Informasjonsplikten etter det arbeidsrettslige regelverket

6.3.1 Den ulovfestede informasjonsplikten

Etter det arbeidsrettslige regelverket er det også en forutsetning at arbeidstakerne varsles i forbindelse med kontrolltiltak. Hovedavtalen mellom LO/NHO (2002-2005) har også tatt høyde for denne plikten, og innført konkrete regler om varsling i punkt 3 og 4 i Tilleggsavtale V:

> *3. Spørsmål om behov, utforming og innføring og vesentlig endring av interne kontrolltiltak skal drøftes med de tillitsvalgte. Bedriften skal holde de ansatte gjennom deres tillitsvalgte orientert om planer og arbeid innenfor området, slik at disse så tidlig som mulig, og før bedriftens beslutning, kan gjøre sine synspunkter gjeldende.*
>
> *4. Før tiltak settes i verk, skal de ansatte ha fått informasjon om tiltakenes formål og praktiske konsekvenser. Bedriftsledelsen og de tillitsvalgte skal hver for seg og i fellesskap bidra til at nødvendig informasjon blir gitt de ansatte før tiltak settes i verk.*

[180] Bestemmelsen gjelder også behandling av personopplysninger i regi av toll- og ligningsvesenet, jf. Ot.prp. nr. 92 (1998-99) på samme side.

Etter punkt 3 er det lagt opp drøfting med de tillitsvalgte omkring utforming og bruk av kontrolltiltak på arbeidsplassen, samt varsling til arbeidstakerne gjennom de tillitsvalgte. Etter punkt 4 er det oppstilt en konkret varslingsplikt overfor de ansatte forut for kontrolltiltakene. Jeg er usikker på om partene her har ment varsling rett forut for hvert enkelt kontrolltiltak, eller om plikten ikke strekker lenger enn til varsling på et eller annet tidspunkt før kontrolltiltakene settes i verk. Avtalereguleringen synes i hovedsak å være i samsvar med gjeldende arbeidsrettslig praksis, til tross for at det kanskje ikke kan sies å gjelde noen generell plikt om å benytte seg av tillitsmennene i denne sammenheng. Se imidlertid aml. § 12 nr. 3, jf. nedenfor. En svakhet ved avtalen er at den ikke konkret regulerer følgene av brudd på informasjonsplikten.

I RG 1993 side 77 ble informasjonsplikten drøftet i forhold til kontrolltiltakets alvorlighetsgrad. Retten uttrykte i denne saken at en bedrift i utgangspunktet måtte ha anledning til å gå inn på den enkeltes private brukerområde dersom dette på forhånd var fastsatt i regler eller instrukser på arbeidsplassen, og de ansatte var kjent med disse reglene. Retten uttalte også at det var en viktig side ved det ulovfestede personvernet at den enkelte arbeidstaker er klar over hva andre vet om en selv. Det ble lagt vesentlig vekt på at varsel i denne saken ikke på forhånd var gitt, og at kontrolltiltaket på denne bakgrunn innebar *"en krenkelse av de krav på beskyttelse av privat informasjon som arbeidstaker må ha overfor arbeidsgiver"*. Retten fant derfor at det aktuelle kontrolltiltaket var urettmessig.

I Rt. 1991 side 616 ble vurderingen av kontrolltiltakets rettmessighet også foretatt delvis på bakgrunn av betydningen av informasjonsplikten. Det ble lagt uttrykkelig vekt på at *hemmelig* videoovervåking innebar et slikt inngrep i den personlige integritet at det ut fra alminnelige personvernhensyn burde anses uakseptabelt.

Som man ser vil kontrolltiltakenes rettmessighet til en viss grad avhenge av om varslingsplikten er oppfylt, i alle fall vil brudd på denne måtte tillegges betydelig vekt i avveiningen mellom hensynet til arbeidsgivers behov for kontroll og hensynet til arbeidstakers personlige integritet. Det neste spørsmålet som da oppstår, er hvorvidt det etter ulovfestede arbeidsrettslige regler kreves varsling forut for hvert enkelt kontrolltiltak, eller hvorvidt det er tilstrekkelig med informasjon i ansettelsesavtaler,

instrukser e.l. Jeg har ikke funnet noen dommer hvor dette spørsmålet har vært drøftet konkret. Til tross for at jeg personlig mener arbeidstaker *burde* varsles før e-post og logger kontrolleres i hvert enkelt tilfelle, kan jeg ikke se at dette er påkrevd etter det ulovfestede regelverket. Arbeidstakers forventning om diskresjon vil også måtte være mindre dersom han allerede i arbeidsavtalen er gjort kjent med arbeidsgivers praksis. Dette synet synes også å ha blitt lagt til grunn i RG 1977 side 33. Har arbeidstakeren valgt å ikke sette seg inn i avtalen, må det være vedkommendes egen risiko. Tilsvarende synspunkter bør kunne legges til grunn dersom informasjonen er gjort tilgjengelig på bedriftens intranettsider e.l. Disse sidene er normalt gjort tilgjengelige for samtlige ansatte, og det bør være den enkelte arbeidstakers plikt å sette seg inn i reglementet.

I Raufoss-dommen var informasjonsplikten ikke drøftet. Ovenfor har jeg konstatert at informasjonsplikten etter popplyl. § 19 ikke omfattet logging som ledd i administrative rutiner mv., men at plikten utløses dersom loggopplysningene samles inn i kontrolløyemed. I denne saken var det imidlertid lagt til grunn opplysninger som ble tilveiebrakt gjennom administrative rutiner kunne gi grunnlag for ytterligere behandling av opplysningene. Det kan derfor tenkes at de samme hensyn talte for at unntaket fra informasjonsplikten ble strukket tilsvarende som det rettslige grunnlaget for behandlingen. Høyesterett burde imidlertid da ha uttalt dette i klartekst, slik at informasjonspliktens rekkevidde ble tydeliggjort. Tidligere rettspraksis gir ingen holdepunkter for noe unntak fra informasjonsplikten i slike tilfeller.

Det sentrale etter både personopplysningsloven og den domstolskapte informasjonsplikten, er at arbeidstakerne blir opplyst om at det behandles personopplysninger om dem, og at arbeidsgiver gjør det mulig for arbeidstakeren å ivareta sine rettigheter på best mulig måte. På bakgrunn av de dommer og kjennelser som har vært undersøkt her, må det imidlertid kunne legges til grunn at informasjonsplikten i popplyl. § 19 avviker noe fra det ulovfestede arbeidsrettslige regelverket. Innsamlingen av personopplysninger krever varsling etter begge regelsett, men popplyl. § 19 krever i motsetning til den ulovfestede plikten ingen varsling ved senere behandling av personopplysningene (med mindre den behandlingsansvarlige forut for innsamlingen hadde som formål å behandle opplysningene ytterligere). Det kreves likevel varsling etter de ulovfestede arbeidsrettslige reglene, og de rettslige

konsekvensene er dermed kanskje ikke store. På bakgrunn av den betydning personopplysningsloven har for behandling av personopplysninger i arbeidslivet, burde lovgiver likevel ta lovens informasjonsplikt opp til ny vurdering.

En annen forskjell mellom den ulovfestede- og den lovfestede informasjonsplikten, er at popplyl. § 19 konkretiserer plikten i langt større grad enn det som følger av ulovfestet rett. Kanskje innebærer § 19 derfor noe strengere krav til innholdet i informasjonen, jf. oppramsingen i første ledd, bokstavene a) til e).

6.3.2 Informasjonsplikt etter arbeidsmiljøloven

Aml. § 12 nr. 3 regulerer arbeidsgivers informasjonsplikt i forbindelse med planleggings- og styringssystemer på arbeidsplassen. Etter denne bestemmelsen skal arbeidstakerne og deres tillitsvalgte holdes orientert om systemer som nyttes ved planlegging og gjennomføring av arbeidet, herunder planlagte endringer i disse systemene. Bestemmelsen må sees i sammenheng med at aml. § 12 skal forhindre uheldige psykososiale virkninger av tilretteleggingen av arbeidet, jf. Ot.prp. nr. 3 (1975-76) på side 107. I samme proposisjon på side 107-108 er § 12 nr. 3 kort omtalt, men det er ikke nevnt kontrolltiltak i arbeidslivet. Det fremgår imidlertid klart at den også omhandler datamaskinsystemer på arbeidsplassen.

I Rt. 1991 side 616 ble aml. § 12 nr. 3 trukket frem i en sak om hemmelig videoovervåkning, jf. ovenfor.[181] Høyesterett uttalte at det var mange hensyn som talte for at bestemmelsen fikk anvendelse, men tok ikke direkte stilling til spørsmålet. Uttalelsene kan imidlertid tolkes dit hen at § 12 nr. 3 kan tenkes å komme til anvendelse overfor kontrolltiltak i arbeidslivet, slik at denne bestemmelsen innebærer en selvstendig plikt til å informere de ansatte i så henseende.

---

[181] Aml. § 12 nr. 1 og § 19 ble også drøftet i denne saken, jf. ovenfor. Aml. § 19 nr. 2 regulerer plikt til å melde fra til Arbeidstilsynet ved endringer i lokaler, produksjonsprosesser, maskinutstyr mv. Det kan tenkes at det her oppstilles en meldeplikt også ved innføringer av nye kontrollmekanismer på arbeidsplassen. Bestemmelsen bør således sees i sammenheng med reglene om meldeplikt til Datatilsynet i popplyl. § 31 flg.

Bestemmelsen er videre nevnt i forbindelse med overvåkingstiltak på arbeidsplassen i NOU 1997: 19 på side 34 (punkt 6.1.8), hvor utvalget uttalte at *"utplassering av overvåkingsutstyr på arbeidsplassen vil utløse plikt for arbeidsgiver til å orientere arbeidstakerne og deres tillitsvalgte (...)"*. Uttalelsen tyder imidlertid på at det er *utplasseringen* (installeringen) av overvåkingsutstyr som skal varsles.[182] For kontroll av e-post og datalogger vil det da være installasjon av loggfunksjonene i datasystemene som skal varsles, ikke nødvendigvis kontrollen av innholdet i loggene. Hvis dette er tilfellet, vil aml. § 12 nr. 3 regulere informasjonsplikten ved innføring av nye overvåkingsmekanismer på arbeidsplassen, mens informasjonsplikten i forbindelse med hvert enkelt kontrolltiltak vil måtte forankres i det ulovfestede arbeidsrettslige regelverket og/eller personopplysningslovens bestemmelser.

6.4 Hvilke rettslige konsekvenser har brudd på informasjonsplikten?

Informasjon i forbindelse med kontroll og overvåking i arbeidslivet er en viktig forutsetning for å kunne sette kontrolltiltakene i verk, jf. punktene ovenfor. Domstolene har etter de ulovfestede reglene underkjent kontrolltiltak *blant annet* på bakgrunn av brudd på denne plikten. Er det således en forutsetning for kontrolltiltakets rettmessighet at denne plikten er overholdt?

RG 1993 side 77 bærer bud om at manglende varsel *i seg selv* innebærer en krenkelse av den enkeltes personlige integritet, og at kontrolltiltaket *derfor* må være urettmessig. Min fortolkning av Høyesteretts uttalelser i Rt. 1991 side 616 trekker i samme retning, da det ble lagt vesentlig vekt på at det var snakk om *hemmelige* videoopptak. Jeg har imidlertid vanskelig for å se at kontrolltiltakene alltid må underkjennes dersom ikke samtlige av kravene i popplyl. § 19 er oppfylt, eksempelvis at arbeidsgiver glemmer å oppgi sin adresse e.l., jf. § 19 (1) bokstav a). Hvis derimot formålet med kontrolltiltaket ikke er varslet, jf. § 19 (1) bokstav b), er det derimot større grunn til å underkjenne tiltaket. Konsekvensene av at informasjonsplikten er brutt er imidlertid ikke nevnt i loven eller forarbeidene. Betydningen av plikten har fått mye oppmerksomhet i

[182] Uttalelsene stammer fra forarbeidene til personopplysningsloven, og ikke til arbeidsmiljøloven.

rettspraksis på arbeidsrettens og personvernrettens område, og det er beklagelig at departementet ikke i forarbeidene har lagt bedre til rette for rettsanvendernes vurderinger, ved å gi tydeligere retningslinjer. De lege lata er det vanskelig å gi noe klart svar på denne problemstillingen. Personopplysningslovens formål tilsier imidlertid at enhver behandling av personopplysninger skal varsles på forhånd. De lege ferenda bør (med de modifikasjoner som er gjort i forhold til enkelte av kravene i § 19) derfor brudd på informasjonsplikten innebære at behandlingen kjennes lovstridig – på samme måte som om behandlingen manglet rettslig grunnlag.

Det må uansett være på det rene at informasjonsplikten vil utgjøre et sentralt element i vurderingstemaet for øvrig. Dersom arbeidsgiver ikke har informert de ansatte om at personopplysninger blir samlet inn og at innholdet i dataloggene kontrolleres, vil dette kunne være et sentralt moment i interesseavveiningen etter bl.a. popplyl. § 8 bokstav f) og i den alminnelige proporsjonalitets- og saklighetsvurderingen, jf. for så vidt RG 1993 side 77 og Rt. 1991 side 616.

Et siste poeng som er verdt å nevne, er at informasjonsplikten etter popplyl. § 19 og den ulovfestede informasjonsplikten (eventuelt også aml. § 12 nr. 3) må sees i sammenheng med informasjonsplikten ved innhenting av samtykke, jf. popplyl. § 8, jf. § 2 nr. 7. Dette er i utgangspunktet to selvstendige plikter, noe som understrekes ved at plikten etter § 19 åpenbart må gjelde også i forhold til de øvrige rettslige grunnlagene for behandling av personopplysninger i popplyl. § 8. Dersom arbeidsgiver innhenter arbeidstakers samtykke for å behandle opplysninger om vedkommende, plikter han å gi tilstrekkelig informasjon. Jeg trakk ovenfor den slutning at innholdet i plikten etter § 8, jf. § 2 nr. 7, i det vesentligste burde tilsvare plikten etter popplyl. § 19. Dersom arbeidsgiver oppfyller kravene i § 2 nr. 7, vil han derfor samtidig oppfylle den alminnelige informasjonsplikten i forbindelse med behandlingen.

***

7 KILDEREGISTER

7.1 Litteratur

Blume, Peter

”Databeskyttelse på arbejdsmarkedet”
Peter Blume og Jens Kristiansen (Danmark)
1. utgave
Jurist- og Økonomiforbundets Forlag, 2002

Bygrave, Lee A.

“Data Protection Law – approaching its rationale, logic and limits”
Kluwer Law International, 2002, Information Law Series 10

Eckhoff, Torstein

”Rettskildelære”
5. utgave ved Jan Helgesen
Universitetsforlaget, Oslo, 2001

Eckhoff, Torstein

”Forvaltningsrett”
Torstein Eckhoff og Eivind Smith
6. utgave, revidert av Eivind Smith
Tano Aschehoug, 1997

Friberg, Odd

”Arbeidsmiljøloven Kommentarutgave”
Odd Friberg, Jan Fougner og Lars Holo
7. reviderte utgave
Universitetsforlaget, Oslo, 2001

Jakhelln, Henning

”Fjernarbeid”
Complex nr. 5/1996
Institutt for Rettsinformatikk, utgitt av Norsk Forening for Jus & EDB
Tano Aschehoug, 1996

Johansen, Michal Wiik

”Personopplysningsloven Kommentarutgave” (”Kommentarutgaven”)
Michal Wiik Johansen, Knut-Brede Kaspersen
og Åste Marie Bergseng Skullerud
Universitetsforlaget, 2001

Melsom, Nina

”Ny lov om personopplysninger – noen arbeidsrettslige problemstillinger”
Tidsskrift for Forretningsjus nr. 4/2001

Schartum, Dag Wiese

”Lov om behandling av personopplysninger”
Lov & Rett nr. 4/2000

Sejersted, Fredrik

”EØS-rett”

Fredrik Sejersted, Finn Arnesen, Ole-Andreas Rognstad, Sten Foyn og Helge Stemshaug

Universitetsforlaget, 1995 (3. opplag 1999)

Storeng, Nils

”Arbeidslivets spilleregler”

Nils Storeng, Tom H. Beck og Arve Due Lund (Bind I, II og III)

Universitetsforlaget, 2003

”Underutvalgets rapport”

”Kontroll og overvåking i arbeidslivet”

Underutvalgets rapport avlevert til Arbeidslivslovutvalget 20. juni 2002

Johan Kr. Øydegard, Pål Gundersen, Kari Stautland, Dag Wiese Schartum, Rune Ytre Arna og Turid Oddum

7.2 Rettspraksis

Norsk Retstidende

Rt. 1986 side 1250

Rt. 1991 side 616
(Gatekjøkken-kjennelsen)

Rt. 1997 side 1954

Rt. 2000 side 1602
(Nøkk)

Rt. 2001 side 418
(Kårstø)

Rt. 2001 side 668
(Tippekasse-kjennelsen)

Rt. 2001 side 1589
(Raufoss)

Rt. 2002 side 391
(God Morgen)

Rt. 2002 side 1500

Rettens Gang

RG 1993 side 77 (Asker og Bærum herredsrett)
(Memorex)

RG 2000 side 664 (Gulating lagmannsrett)

RG 2002 side 162 (Gulating lagmannsrett)

Arbeidsretten (ARD)

ARD 1937 side 114

ARD 1951 side 201

ARD 1958 side 189

ARD 1959 side 1

ARD 1961 side 90

ARD 1968 side 44

ARD 1971 side 49

ARD 1978 side 110

Øvrig rettspraksis

05.10.1992 – Agder lagmannsrett
(Tappetårn-saken)
Lov&Data nr. 34, mars 1993

24.04.2002 – Oslo tingrett
(Oslo Sporveier)

24.09.2002 – Borgarting lagmannsrett (LB-2002-02299)
(Se Rt. 2002 side 1500)

19.02.2003 – Gulating lagmannsrett (LG-2003-00090)
(Phillips Petroleum)

7.3 Lover, forskrifter, direktiver og internasjonale avtaler

Lover

Sjømannslov av 30. mai 1975 nr. 18 (sjømannsloven)

Lov om arbeidervern og arbeidsmiljø mv. av 4. februar 1977 nr. 4 (arbeidsmiljøloven, aml.)

Lov om personregistre m.m. av 9. juni 1978 nr. 48 (personregisterloven, pregl.) (Opphevet)

Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det Europeiske Økonomiske Samarbeidsområde (EØS) mv. av 27. november 1992 nr. 109 (EØS-loven)

Lov om vern mot smittsomme sykdommer av 5. august 1994 nr. 55 (smittevernloven)

Lov om styrking av menneskerettighetenes stilling i norsk rett av 21. mai 1999 nr. 30 (menneskerettsloven)

Lov om behandling av personopplysninger av 14. april 2000 nr. 31 (personopplysningsloven, popplyl.)

Forskrifter

Forskrift til personopplysningsloven (personopplysningsforskriften), FOR 2000-12-15 nr. 1265

Direktiver

Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (”personverndirektivet”/”direktivet”)

Internasjonale avtaler

FN-konvensjonen om Sosiale og Politiske Rettigheter (SP)

Inkorporert i norsk lovgivning ved menneskerettsloven av 21. mai 1999 nr. 30

Den Europeiske Menneskerettighetskonvensjon (EMK)

Inkorporert i norsk lovgivning ved menneskerettsloven av 21. mai 1999 nr. 30

Avtale om Det europeiske økonomiske samarbeidsområde (EØS-avtalen)

Inkorporert i norsk lovgivning ved EØS-loven av 27. november 1992 nr. 109

Avtale mellom EFTA-statene om opprettelse av et Overvåkingsorgan og en Domstol (ODA)

Europarådskonvensjonen av 28. januar 1981 nr. 108 om personvern i forbindelse med elektronisk databehandling av personopplysninger

7.4 Forarbeider

Norske forarbeider

Ot.prp. nr. 3 (1975-76)

”Om arbeidstid, oppsigelsesvern, arbeidstilsyn m.v. i lov om arbeidervern og arbeidsmiljø”

Ot.prp. nr. 50 (1993-94)

”Om lov om endringer i lov 4 februar 1977 nr 4 om arbeidervern og arbeidsmiljø mv. Ot.prp.nr.90 (1993-1994) (endringslov)”

Innst.O. nr. 2 (1994-95)

NOU 1997: 19

”Et bedre personvern – forslag til lov om behandling av personopplysninger”

Ot.prp. nr. 92 (1998-99)

“Om lov om behandlinger av personopplysninger (personopplysningsloven)”

Innst.O. nr. 51 (1999-2000)

NOU 2003: 21

”Kriminalbekjempelse og personvern”

Utenlandske forarbeider

SOU 2002: 18

”Integritetsutredningen” (Sverige)

7.5 Elektroniske dokumenter

Datatilsynets retningslinjer

Datatilsynet
”Samtykke til behandling av personopplysninger”
[online]
http://www.datatilsynet.no/arkiv/brosjyrer/pol/samtykke.html
Publisert 2000
Sist sjekket 13.10.2003

Datatilsynet
”Om registrering av hendingar i data-system (loggar)”
[online]
http://www.datatilsynet.no/dtweb/art_831.html
Publisert 29.11.2002
Sist sjekket 13.10.2003

Datatilsynet
”Om registrering av hendingar i data-system (loggar)”
[online]
http://www.datatilsynet.no/dtweb/attachment/895/loggar.html
Publisert 05.01.2001
Sist sjekket 13.10.2003

Datatilsynet
”Arbeidsgiverens innsyn i de ansattes e-post – spørsmål og svar”
[online]
http://www.datatilsynet.no/dtweb/attachment/823/epost.html
Publisert 23.05.2001
Sist sjekket 13.10.2003

Personvernnemnda

Personvernnemnda
”Klagesaker”
[online]
http://www.personvernnemnda.no/klagesaker/klagesaker.html
Sist sjekket 13.10.2003

Norsk Lovkommentar

Schartum, Dag Wiese
Norsk Lovkommentar – Studentutgave (CD-rom)
”Kommentarer til lov om behandling av personopplysninger”

Artikler fra Dagbladets nettside

Lie , Leiv Gunnar
”Ja til porno, nei til musikk”
[online]
http://www.dagbladet.no/nyheter/2002/10/27/352281.html
Publisert 27. oktober 2002 8:31
Sist sjekket 13.10.2003

Teimansen, Even
”Sjefen ser deg på nettet”
[online]
http://www.dagbladet.no/dinside/2002/10/29/352444.html
Publisert 29. oktober 2002 7:26
Sist sjekket 13.10.2003

Odin

St.prp. nr. 34 (1999-2000)

[online]

http://odin.dep.no/ud/norsk/publ/stprp/032005-034007/index-hov001-b-n-a.html

Publikasjonsdato ukjent

Sist sjekket 13.10.2003

Avdeling for Forvaltningsinformatikks (AFINs) nettside

Avdeling for Forvaltningsinformatikk

Personvern på nett

"Personvernavgjørelser"

[online]

http://www.personvern.uio.no/pvpn/avgjorelser/index.html

Publikasjonsdato ukjent

Sist sjekket 13.10.2003