

ARBEIDSGIVERS ADGANG TIL KONTROLL AV ANSATTES BRUK AV ELEKTRONISK UTSTYR



Universitetet i Oslo
Det juridiske fakultet

Kandidatnummer: 584
Leveringsfrist: 25.11.2012

Til sammen 15501 ord

15.11.2012

Innholdsfortegnelse

<u>1</u>	<u>INNLEDNING</u>	<u>1</u>
1.1	Oppgavens tema og problemstilling	1
1.2	Avgrensning og begrepsforklaringer	5
1.2.1	Generelt om kontrolltiltak	7
1.2.2	GPS og sporingsutstyr	7
1.2.3	Datalogger	9
1.2.4	Kort om bevisavskjæring	10
1.3	Rettslig grunnlag	10
1.3.1	Arbeidsmiljøloven	11
1.3.1.1	Arbeidsgivers styringsrett	12
1.3.2	Personopplysningsloven	13
1.3.3	Personopplysningsforskriften	16
1.3.4	Internasjonal rett	17
1.4	Metode	18
1.5	Videre framstillingstilling	19
<u>2</u>	<u>ARBEIDSGIVERS ADGANG TIL KONTROLL AV ANSATTES BRUK AV ELEKTRONISK UTSTYR</u>	<u>21</u>
2.1	Forbud mot overvåkning av elektronisk utstyr, herunder bruk av internett.	
	Personopplysningsforskriften § 9-2 annet ledd.	21
2.1.1	Når foreligger «overvåkning»?	22
2.1.2	Hvilket «elektronisk utstyr» viser forskriften til?	24
2.1.3	«Bruk av» elektronisk utstyr	25
2.1.4	Arbeidsgivers adgang til innsyn i datalogger ved administrasjon eller ved oppklaring/avdekking av brudd på sikkerheten i edb-systemet jfr. personopplysningsforskriften § 7-11.	

2.2	Arbeidsgiver adgang til å kontrollere ansattes bruk ved konkret mistanke om mislighold av arbeidsreglement, illojalitet eller brudd på arbeidsavtale. Herunder adgangen til å bruke opplysningene som fremkommer av kontrolltiltaket.	33
2.2.1	Arbeidsmiljøloven § 9-1 krav til formål ved kontrolltiltak	34
2.2.1.1	GPS saken	36
2.2.2	Saklighetskravet, arbeidsmiljøloven § 9-1 (1) og berettiget interesse, personopplysningsloven § 8 f)	41
2.2.3	Forholdsmessighetskravet, arbeidsmiljøloven § 9-1 (1) og hensynet til ansattes personvern, personopplysningsloven § 8 f)	45
2.2.4	Informasjon og drøftelse, arbeidsmiljøloven § 9-2	47
<u>3</u>	<u>AVSLUTNING</u>	<u>50</u>
<u>4</u>	<u>LITTERATURLISTE</u>	<u>52</u>
4.1	Litteratur:	52
4.2	Lov- og forarbeidsregister	53
4.3	Rettspraksis	54
4.4	Nettdokumenter	55
<u>5</u>	<u>LISTER OVER TABELLER OG FIGURER M V</u>	<u>A</u>

1 INNLEDNING

1.1 Oppgavens tema og problemstilling

Temaet for oppgaven er arbeidsgivers adgang til kontroll av ansattes bruk av arbeidsgivers elektroniske utstyr, herunder bruk av internett. Spørsmålet er *om* arbeidsgiver har innsynsrett i de tilgjengelige opplysningene om bruken og i så tilfelle *når*.

Jeg valgte å skrive om dette tema fordi det er et svært aktuelt tema og reglene på området er vage. Reglene er ikke lett å finne fram i og dermed heller ikke så lett tilgjengelige for brukerne, det vil si arbeidsgivere og arbeidstakere. Jeg ønsker med dette å redegjøre nærmere om grensene for hva som er tillatt og hva som ikke er tillatt etter gjeldende rett.

Oppgaven tar for seg gjeldende regler i arbeidsmiljøloven, personopplysningsloven og personopplysningsforskriften om kontroll og overvåkning av arbeidstakere. Det interessante for en arbeidsgiver er ikke alltid å få tilgang til informasjonen, men om han kan bruke den og i tilfelle når, derfor tar oppgaven også for seg adgangen til å bruke opplysningene i tillegg til retten til innsyn.

Den 1. mars 2009 trådte Personopplysningsforskriften kapittel 9 i kraft.

Personopplysningsforskriften § 9-2 annet ledd inneholder bestemmelser som regulerer arbeidsgivers adgang til å overvåke arbeidstakers bruk av elektronisk utstyr og lyder:

«Arbeidsgiver har ikke rett til å overvåke arbeidstakers bruk av elektronisk utstyr, herunder bruk av Internett, ut over det som følger av denne forskriften § 7-11».

Forskriften er et viktig supplement til de allerede eksisterende regler. Jeg vil gå nærmere inn på forskriftens betydning og forsøke å svare på hva som inngår i betegnelsen å «overvåke», hva regnes som «elektronisk utstyr» og når kan man si at det er «bruk av» elektronisk utstyr/internett.

Spørsmålet om adgang til kontroll av bruk av elektronisk utstyr vil i mange tilfeller først bli problematisk når det legges igjen spor/informasjon om den ansatte som kan knyttes til den ansatte som individ, såkalte personopplysninger. Oppgavens tema tar for seg kun slikt utstyr. Annet utstyr som for eksempel lysbrytere, kaffemaskiner, bakeovner, støvsugere og lignende er normalt ikke utsyr som legger igjen personopplysninger.

Oppgaven tar for seg de tilfellene der arbeidsgiver ønsker tilgang til lagret informasjon om arbeidstakerne. Informasjonen framkommer ofte som en sidevirkning av et kontrolltiltak eller på bakgrunn av andre lovlige sikkerhetstiltak som for eksempel brannmurlogger i datanettverk. Denne tilleggsinformasjonen er personopplysninger om den kan knyttes til enkeltperson jfr. personopplysningsloven § 2 nr. 1. Dette innebærer at problemstillingen arbeidsgivers styringsrett versus arbeidstakers personvern blir satt på spissen.

Behovet for regler om kontroll av arbeidstakers bruk av elektronisk utstyr har økt betraktelig de siste årene da det teknologiske samfunnet er i rask utvikling. Det er ikke alltid like enkelt å følge med på denne utviklingen, fordi det utvikles mengder av elektronisk kommunikasjonsutstyr til alle salgs forskjellige behov.

I dag er det helt vanlig å bruke smart telefoner, GPS (Global Position System) og PDA (Personlig Digital Assistent), ord som for noen år siden ikke ga mening, men nå er blitt dagligtale.

Alt dette elektroniske hjelpeutstyret har funksjoner som er gjør at arbeidsgivere gjerne vil ta i bruk disse for blant annet å effektivisere arbeidet. Datamaskiner, som PC og Mac vil trolig anses som et av de viktigste og vanligste elektroniske utstyr som brukes i dag på arbeidsplasser i Norge.

En stor del av det elektroniske utstyret som benyttes på arbeidsplassene er kommunikasjonsutstyr som legger igjen elektroniske spor, i form av personopplysninger. Det er derfor svært viktig at personvernet blir ivaretatt når en skal ta stilling til spørsmål om kontroll og overvåkning ved bruk av slikt utstyr.

Utviklingen av teknologien åpner for at arbeidsgiver i dag har muligheten til å kontrollere og overvåke i en mye større skala enn tidligere. De siste 20 årene har som sagt datamaskinen blitt et uunnngåelig hjelpemiddel i mange bedrifter. Datamaskinens utvikling har bidratt til å gjøre det enklere å kontrollere arbeidstakere og arbeidet de utfører, blant annet fordi datamaskiner er utstyrt med harddisker/minnefunksjon som registrerer og lagrer data. Dagens datamaskiner kommer ikke lenger bare i store, tunge, stasjonære utgaver, men i lette og nette utgaver som bærbar PC, nettbrett og smart telefoner, også kalt PDA (Personlig digital assistent). Alle disse utgavene av datamaskiner åpner for muligheten til å kontrollere og overvåke de ansattes arbeid på en avansert og detaljert måte. De fleste datamaskiner vil på grunn av minnefunksjonen lagre logger ved bruk, og de fleste datanettverk vil ha en brannmurslogg hvor muligheten for å innhente detaljert informasjon er til stede.

Spørsmålet blir spesielt satt på spissen fordi det i dag er blitt mer og mer vanlig at grensen mellom arbeid og privatliv viskes ut. Arbeidsgivere deler ut bærbare datamaskiner og smart telefoner til sine ansatte, slik at de kan være lettere tilgjengelige utenom arbeidstiden og i tillegg ha anledningen til jobbe effektivt også utenfor arbeidsplassen. For eksempel kan det tenkes at en PC i sin helhet er eid av arbeidsgiver mens deler av innholdet på PC-en er privat, eller som følge av at den ansatte har lagt igjen personlige spor på PC-en som er beskyttelsesverdige etter personvernlovgivningen. Spørsmålet blir så om hvor grensen går for hva som kan være gjenstand for overvåkning og kontroll i denne sammenheng? Hvor langt strekker arbeidsgivers styringsrett seg i forhold til kontroll av bruk av elektronisk utstyr eid av arbeidsgiver i forhold til de begrensninger som reglene om ansattes personvern setter. Dette er overordnede spørsmål som jeg skal forsøke å gjøre rede for i oppgaven.

På bakgrunn av den teknologiske utviklingen og den økende bruken av elektroniske hjelpemidler i både arbeidslivet (og privatliv) opprettet Regjeringen ved Fornyings- og arbeidsdepartementet 25. mai 2007 en egen kommisjon, Personvernkommisjonen. Kommisjonens oppdrag var blant annet å se på hvilke utfordringer informasjonsteknologien medfører i arbeidslivet. I NOU 2009:1 skriver kommisjonen:

«Man ser også at økt informasjonsmengde vil kunne medføre en økt fare for at opplysninger blir brukt til andre formål; det vil si at opplysninger som opprinnelig er innhentet og lagret for et bestemt formål senere blir benyttet til andre formål som ikke nødvendigvis er forenlige med det opprinnelige formålet. Et eksempel på dette er opplysninger om ansattes bruk av Internett på arbeidsplassen. Slik bruk vil automatisk generere data som kan lagres i logger for administrasjons- og sikkerhetsmessige formål. Dersom det oppstår en arbeidsrettslig konflikt mellom den ansatte og bedriften, finnes det flere eksempler på at arbeidsgiver ønsker å legge fram slike logger som bevis for domstolene, for å underbygge sin sak.»¹

En FAFO rapport fra 2010 om overvåking og kontroll i arbeidslivet understreker problemstillingen. Mellom 20 og 30 % av de spurte arbeidstakerne svarte at de opplever nye teknologiske overvåkningsformer, som overvåking av e-post, internettbruk og flåtestyring som problematisk. Slik overvåking og kontroll oppleves som krenkende og svekker tilliten til ledelsen.²

I de tilfeller der bedriften følger gjeldende regler om overvåking og kontroll av elektronisk utstyr vil nok dette foregå uten særlige etterfølgende rettslige problemer i forhold til kontrollen. Det er tilfellene der reglene ikke er fulgt det det kan oppstå konflikter av juridisk art. Rettspraksis viser at behovet for kontroll av ansattes IT-ressursbruk oftest blir satt på spissen når arbeidsgiver har konkret mistanke om illojal opptreden i forhold til bedriften og ønsker å bekrefte/avkrefte mistanken ved bruk av innhentet logginformasjon, som også Personvernkommisjonen påpeker over i NOU 2009:1. Flere av sakene fra rettspraksis handler om spørsmål om usaklig oppsigelse på grunn av ulovlig bruk av personopplysninger innhentet fra elektronisk utstyr som inneholder lagret informasjon som kan gi svar på om oppsigelsen var saklig.³ Alle sakene som er kommet opp for domstolene per dags dato, som omhandler tema, er fra før personopplysningsforskriften var trådt i kraft i 1.mars 2009, foruten om saken nevnt nedenfor.

¹ NOU 2009:1 Individ og integritet s. 150 og 151.

² Bråten, Mona Fafo rapport 2010:2 Overvåking og kontroll i arbeidslivet s. 55

³ Eksempelvis Rt. 2005 s. 518 og LB-2007-121782.

Det ble i juli i fjor avsagt en dom i forbindelse med oppsigelse av en renovasjonsbilsjåfør på grunnlag av data/informasjon innhentet fra GPS installert i renovasjonsbilen han kjørte.⁴ Et av spørsmålene for retten var om arbeidsgiveren hadde adgang til å kontrollere og bruke informasjonen innhentet fra sporingssystemet som grunnlag for oppsigelsen.⁵

GPS saken er interessant i forhold til at personopplysningsforskriften § 9-2 annet ledd aldri blir nevnt i saken, hvorfor den ikke er det skal jeg forsøke å gi et svar på. Videre gir dommen svar på flere av problemstillingene i forhold til adgangen til å bruke opplysninger til et annet formål enn det opprinnelige formålet med innsamlingen. Denne problemstillingen er interessant fordi de i mange tilfeller vil være slik at arbeidsgiver ikke bare ønsker adgangen til informasjonen elektronisk utsyr legger igjen, men de ønsker også å bruke den, for eksempel i oppsigelsessaker.

1.2 Avgrensning og begrepsforklaringer

Oppgaven tar ikke for seg reglene om arbeidsgivers adgang til innsyn i e-post.⁶ Det vil ikke bli redegjort for behandling av sensitive opplysninger jfr. personopplysningsloven § 9. Med sensitive opplysninger menes rasemessig eller etnisk bakgrunn politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold og medlemskap i fagforeninger jfr. personopplysningsloven § 2 nr. 8). Når det gjelder adgangen til å behandle personopplysningen åpner personopplysningsloven § 8 for flere alternativer;

«Personopplysninger (jf. § 2 nr. 1) kan bare behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik behandling, eller behandlingen er nødvendig for

⁴ TNHER-2010-144876-2

⁵ RG 2011 s. 321

⁶ Gjeldende rett i forhold til reglene om innsyn i e-post er redegjort av Mette Borchgrevink i *Arbeidstakers personvern - EMK og nye e-postregler (2009)* og *Norsk forskriftsendring 1. mars 2009: Arbeidsgivers innsyn i arbeidstakers e-post (2009-03-00)* ref. Lovdata.no

- a) å oppfylle en avtale med den registrerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås,
- b) at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse,
- c) å vareta den registrertes vitale interesser,
- d) å utføre en oppgave av allmenn interesse,
- e) å utøve offentlig myndighet, eller
- f) at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.»

Jeg vil kun fokusere på § 8 f) da den er mest aktuell i arbeidsforhold.

Med *personopplysninger* menes opplysninger og vurderinger som kan knyttes til en enkeltperson jfr personopplysningsloven § 2 nr. 1).

Den *behandlingsansvarlige* er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal benyttes jfr. personopplysningsloven § 2 nr. 4). Den behandlingsansvarlige skal sørge for at personopplysningen bare behandles når dette er tillatt etter personopplysningsloven §§ 8, 9 og 11.

Databehandler er den som behandler personopplysninger på vegne av den behandlingsansvarlige jfr. personopplysningsloven § 2 nr. 5).

Med *IT- ressursbruk* mener jeg bruk av informasjons teknologi.

1.2.1 Generelt om kontrolltiltak

Spekteret av ulike kontrolltiltak en arbeidsplass kan iverksette er stort. Det kan være alt fra tiltak som tidsregistrering i forhold til pauser og arbeidstid, lyd- og videoovervåkning, innhenting av helseopplysninger, til mere inngripende tiltak som rusmiddeltesting og medisinske undersøkelser av de ansatte. Arbeidsmiljøloven har ingen definisjon på hva som omfattes av begrepet. I juridisk teori definerer Jakhelln kontrolltiltak slik; «... med kontrolltiltak menes ethvert tiltak som skal sikre at arbeidstakere utfører sitt arbeid slik de skal, og for øvrig opptrer innen de rammer som gjelder for arbeidsforholdet».⁷

Ved tvilstilfeller der man er usikker på om man har med et kontrolltiltak å gjøre sier forarbeidene til arbeidsmiljøloven at «... det kan være vanskelig å foreta en presis avgrensning av begrepet «nedad». I forhold til utvalgets forslag til generalklausul, synes det heller ikke nødvendig å trekke en slik grense. For det første må det generelt legges til grunn at arbeidsgivers utøvelse av styringsretten begrenses av alminnelige saklighetsnormer. For det andre må det regelmessig antas at de tilfeller hvor det rent praktisk vil kunne være tvil om man står overfor et «kontrolltiltak» eller ikke, vil tiltaket uansett være så lite inngripende overfor arbeidstakerne at en interesseavveining uansett vil gå i arbeidsgivers favør.»⁸ Kontroll og overvåkning av elektronisk utstyr vil i mange tilfeller omfattes av arbeidsmiljølovens begrep «kontrolltiltak», men ikke i alle tiltak omfattes jfr. personopplysningsforskriften § 7-11(sikkerhetstiltak) som jeg kommer tilbake til senere.

1.2.2 GPS og sporingsutstyr

Et eksempel på et kontrolltiltak som har blitt mer vanlig de siste årene er GPS, eller Global Positioning System. GPS er et satellittbasert nettverk som kan lokalisere en mottakers posisjon til en hver tid. GPS er ofte brukt innen sjøfart, men i senere tid også

⁷ Jakhelln, Oversikt over arbeidsretten s. 392

⁸ NOU 2004:5 Arbeidslivslovutvalget s. 435

blitt mer vanlig i kjøretøy på land. Systemet er også blitt mer vanlig å bruke i arbeidssammenheng der transport er en del av arbeidet, spesielt i såkalt flåtestyring. Med sporingsutstyr menes håndholdt GPS, fastmontert GPS, flåtestyring, sporingsbrikke o.l som innhenter og lagrer informasjon om hvor et bestemt objekt befinner seg til enhver tid.

Slik sporingsteknologi reiser flere personvernrettslige spørsmål, fordi informasjonen som kommer fram kan knyttes til enkeltperson. Spesielt vil prinsippet om retten til privatliv stå i fokus, ved teknologi som GPS kan muligheten til å overvåke ansatte til en hver tid. Som eksempel kan det tenkes at en taxisjåfør blir overvåket av sin arbeidsgiver til enhver tid. Hva om taxisjåføren i sin lunsjpause (eller for så vidt i arbeidstiden, uten passasjer i bilen) velger å gjøre et av disse alternativene a) hente og kjøre sin kone til legevakten b) besøke et bordell på kjent adresse c) besøke sin bror på hospits for narkomane. Uansett hva han velger å gjøre vil informasjonen om hvor han er til enhver tid være tilgjengelig for hans arbeidsgiver. Denne informasjonen er personopplysninger jfr. personopplysningsloven § 2 nr. 1). Det personvernrettslige problemet blir at arbeidsgiver også enkelt kan få tilgang til slike opplysninger, selv om hensikten med sporingsutstyr ofte vil være begrunnet i sikkerhet og effektivitet. Denne problemstillingen vil jeg gå nærmere innpå i punkt 3 i oppgaven.

Juridisk sett skilles det mellom håndholdt GPS og fastmontert sporingsutstyr. En håndholdt GPS kan enkelt avinstalleres i kjøretøyet og tas med inn og ut av kjøretøyet ved behov. Fastmontert sporingsutstyr derimot er fastmontert permanent i kjøretøyet. De to forskjellige formene for GPS-utstyr omfattes av to forskjellige regelsett som jeg skal se nærmere på senere i oppgaven. Ofte blir både håndholdt og fastmontert GPS anvendt samtidig. Med såkalt sporingsbrikke kan arbeidsgiver til enhver tid spore og registrere detaljert informasjon om kjøretøyets posisjon og dermed vite hvor arbeidstakeren befinner seg.

Med *sporingsutstyr* menes håndholdt GPS, fastmontert GPS, flåtestyring, sporingsbrikke o.l

1.2.3 Datalogger

Med *datalogger* menes logger fra brannmur eller andre sikkerhetssystemer. Som regel er slike systemer programvare. Brannmuren har som formål å beskytte datanettet mot uønsket kommunikasjon og ivareta sikkerheten. Brannmuren registrer og lagrer all datatrafikk i nettverket i logger.

På grunn av minnefunksjonen i datamaskiner vil det også være mulig å hente inn informasjon ved å sjekke aktivitetsloggen på den enkelte enhet. Loggene kan gi detaljerte svar på aktiviteter på maskinen, for eksempel tidspunktet når en PC er blitt tatt i bruk og hvilke programmer som ble brukt og hvilke internettsider som har blitt besøkt. De fleste bedrifter i dag som anvender datamaskiner i sitt arbeide benytter seg av brannmurer av sikkerhetsmessige årsaker. Imidlertid vil brannmuren kunne gi informasjon foruten om de sikkerhetsmessige. I loggene kan arbeidsgiver få tilgang til hvilke internettsider som har blitt besøk av den enkelte ansatte. Hvis vi tar opp eksempelet fra over og bytter ut taxisjåføren med en kundekonsulent som har PC og internett som sitt viktigste arbeidsverktøy. En gang i løpet av arbeidsdagen velger konsulenten og benytte seg av internettet og gjøre et av følgende alternativer: a) besøke nav.no for å søke etter ny stilling b) besøke facebook.com og «snoke» på sjefens profil c) google «homofili». Uansett hvilket alternativ konsulenten velger å foreta seg vil disse opplysningene lagres og hans arbeidsgiver kan via brannmuren få tilgang til disse opplysningene. Problemet med datalogger er nettopp det at de gir svar på mye mere enn nettopp formålet med dem som er å ivareta sikkerheten. Under punkt 2.1 vil jeg redegjøre nærmere for denne problemstillingen.

Noen bedrifter velger å sette opp «sperrer» mot enkelte nettsider som de ikke anser som forenelig med arbeidet som skal utføres. Disse sperrere kan for eksempel være nettsider som inneholder pornografisk materiale eller det kan være sider som i dag omtales som sosiale medier, for eksempel facebook og twitter.

Spesifiserte telefonregninger kan også være gjenstand for kontroll av private opplysninger. Formålet med spesifiserte telefonregninger er som regel fakturakontroll. Imidlertid kan en spesifisert telefonregning gi svar på hvem den ansatte kontakter både i

og utenfor arbeidssammenheng. Adgangen til å innhente informasjon fra spesifisert telefonregning vil bli gjennomgått under punkt 2.1.

1.2.4 Kort om bevisavskjæring

I de sakene som omhandler oppsigelse eller avskjed ønsker arbeidsgiver ofte å legge fram bevis innhentet enten fra datalogger eller sporingsutstyr for å bevise at oppsigelsen eller avskjeden er saklig begrunnet. Retten må da vurdere om beviset skal tillates ført i de tilfeller beviset er innhentet i strid med personopplysningsloven og arbeidsmiljøloven.⁹

I de tilfeller hvor reglene vil komme opp for domstolsbehandling, vil det i noen tilfeller være spørsmål om det er tillatt å føre beviset som er innhentet på bakgrunn av kontroll eller overvåkning om disse er innhentet i strid med loven.

Norsk rett bygger på prinsippet om fri bevisførsel i sivile saker jfr. tvisteloven av 17. juni 2005 nr. 90 (heretter tvl.) § 21-2 (1). Ved bevis innhentet på «utilbørlig måte», kan beviset i særlige tilfeller nektes ført for retten jfr. tvisteloven § 22-7. I GPS-kjennelsen påpeker lagmannsretten at «Dette er en unntaksregel med et forholdsvis snevert anvendelsesområde. Bevisavskjæring forutsetter at beviset er skaffet til veie på utilbørlig vis, og at føring av beviset medfører en krenkelse av tungtveiende rettsikkerhets- eller personvern hensyn.»¹⁰

1.3 Rettslig grunnlag

I hovedsak er det tre regelsett som gjelder ved arbeidsgivers adgang til kontroll av ansatte elektronisk utstyr; Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. av 17. juni 2005 nr. 62 (heretter kalt arbeidsmiljøloven), Lov om behandling av personopplysninger av 14. april 2000 nr. 31 (heretter kalt personopplysningsloven) og

⁹ Eksempelvis i RG 2011 s. 321 og RG 2004 s. 347

¹⁰ RG 2011 s. 321 Hålogaland lagmannsrett –kjennelse, s. 324.

Forskrift om behandling av personopplysninger av 15. desember 2000 nr. 1265 (heretter kalt personopplysningsforskriften).

I GPS kjennelsen omtalte lagmannsretten i sin begrunnelse at «Hvorvidt et kontrolltiltak kan iverksettes reguleres av arbeidsmiljøloven, mens personopplysningsloven regulerer hvorvidt opplysningene kan behandles.»¹¹

1.3.1 Arbeidsmiljøloven

I de tilfeller der arbeidsgiver ønsker å iverksette et kontrolltiltak hvor det skal benyttes elektronisk utstyr, som for eksempel overvåkning ved hjelp sporingsutstyr skal det utføres i henhold må arbeidsgiver ha et hjemmelsgrunnlag. I forarbeidene til arbeidsmiljøloven står det at «Aktuelle hjemmelsgrunnlag kan være bestemmelser i lov eller forskrift, samtykke fra arbeidstakeren, tariffavtale, arbeidsavtale, arbeidsreglement og arbeidsgivers styringsrett. Hvilke krav som må stilles til rettsgrunnlaget for at kontrollen skal være rettmessig, vil særlig bero på begrunnelsen og behovet for kontrollen, kontrolltiltakets art og på hvor inngripende det vil virke i forhold til den enkelte ansatte.»¹²

I motsetning til den nå opphevede lov om arbeidervern og arbeidsmiljø av 2. april 1977 nr. 4 inneholder någjeldende arbeidsmiljølov et eget kapittel som regulerer «kontrolltiltak i virksomheten» jfr. kapittel 9. Tidligere var adgangen til å iverksette og utføre kontroll og overvåkning regulert av personopplysningsloven, personopplysningsforskriften (fra 2000), prinsipper utarbeidet i rettspraksis og generelle personvernrettslige prinsipper. I forarbeidene til någjeldende arbeidsmiljølov presiserer arbeidslivslovutvalget at integreringen av datasystemer byr på nye utfordringer i arbeidslivet med tanke på kontrollmulighetene i henhold til dette.¹³

Arbeidsmiljøloven kapittel 9 er en kodifisering av allerede gjeldende materielle rett før ikrafttredelsen i 1. januar 2006.

¹¹ RG 2011 s. 321

¹² NOU-2004-5 Arbeidslivslovutvalget, Kapittel 17, Kontroll og overvåkning i arbeidslivet s. 408.

¹³ NOU 2004:5 Arbeidslivslovutvalget s. 429

Kapittelet inneholder i § 9-1 materielle krav og i § 9-2 prosessuelle krav til iverksettelse og gjennomføring av kontrolltiltak. De prosessuelle kravene i § 9-2 er ny i någjeldende lov. I § 9-1 fastsettes det at «Arbeidsgiver kan bare iverksette kontrolltiltak overfor arbeidstaker når tiltaket har saklig grunn i virksomhetens forhold og det ikke innebærer en uforholdsmessig belastning for arbeidstakeren.»

Videre bestemmer § 9-1 annet ledd at «Personopplysningsloven gjelder for arbeidsgivers behandling av opplysninger om arbeidstakere i forbindelse med kontrolltiltak med mindre annet er fastsatt i denne eller annen lov.»

I § 9-2 stilles det krav om at kontrolltiltak skal drøftes, informeres og evalueres med de ansatte i forbindelse med iverksettelse av tiltak.

I tillegg til kapittel 9 vil også § 4-2 om fullt forsvarlig arbeidsmiljø spille inn ved iverksettelse av kontrolltiltak. Bestemmelsen vil kunne fungere som en sikkerhetsventil om kapittel 9 og personopplysningsloven ikke ivaretar arbeidsmiljølovens formål som blant annet er «å sikre et arbeidsmiljø som gir grunnlag for en helsefremmende og meningsfylt arbeidssituasjon, som gir full trygghet mot fysiske og psykiske skadevirkninger, og med en velferdsmessig standard som til enhver tid er i samsvar med den teknologiske og sosiale utvikling i samfunnet» jfr. § 1-1 a).

1.3.1.1 Arbeidsgivers styringsrett

Adgangen til å iverksette kontrolltiltak er blant annet basert på samspillet mellom arbeidsgivers styringsrett og arbeidstakers lojalitetsplikt. Styringsretten er med på å danne det rettslige grunnlaget for iverksettelse av kontrolltiltak. Med styringsrett menes det at arbeidsgiver har rett til å lede, fordele og kontrollere arbeidet.

Med arbeidstakers lojalitetsplikt siktes det til at de ansatte skal etterleve de instruksjoner som blir gitt av arbeidsgiver i medhold av styringsretten.

Styringsretten er basert på rettspraksis.¹⁴ Det er grunnleggende for arbeidsgivers styringsrett, at arbeidsgiver har rett til å føre kontroll av arbeidet som utføres av sine ansatte. Styringsretten er derimot ikke ubegrenset. I forhold til kontrolltiltak som gjennomføres begrenser saklighetskravet og forholdsmessighetskravet i

¹⁴ Rt. 2000 s. 1602, NØKK dommen.

arbeidsmiljøloven §§ 9-1 (1) og 9-1 (2) arbeidsgivers styringsrett med tanke på hva arbeidsgiver kan iverksette av tiltak.

En annen viktig begrensning i styringsretten er at personvernprinsipper setter rammer for hva arbeidsgiver kan innføre av kontrolltiltak i virksomheten. I arbeidsmiljøloven § 9-1 (2) står det at «Personopplysningsloven gjelder for arbeidsgivers behandling av opplysninger om arbeidstakere i forbindelse med kontrolltiltak med mindre annet er fastsatt i denne eller annen lov.» Et annet viktig moment som setter begrensninger for bruk av styringsretten ved iverksettelse av kontrolltiltak er at arbeidsgiver må se hen til kravet om et fullt forsvarlig arbeidsmiljø jfr. arbeidsmiljøloven § 4-1 (1). Kontrolltiltak som medfører en betydelig belastning for de ansatte kan stride i mot regelen om fullt forsvarlig arbeidsmiljø.

1.3.2 Personopplysningsloven

Uavhengig av om det ikke er iverksatt kontrolltiltak etter arbeidsmiljøloven eller ikke, vil innsynsretten uansett bero på om personopplysningslovens grunnkrav til behandling av personopplysninger er oppfylt jfr. § 11 og § 8.

Personopplysningsloven trådte i kraft 1. januar 2001, og avløste den tidligere lov om personregistre av 9. juni 1978 nr. 48. Før arbeidsmiljøloven av 2005 trådte i kraft var det personopplysningsloven den loven som regulerte adgangen til kontroll i arbeidsforhold. Personopplysningsloven samsvarer i stor grad med EUs personverndirektiv 95/46 EF. Personopplysningsloven regulerer blant annet arbeidsgivers adgang til å bruke og behandle den informasjonen som kommer fram om arbeidstakere på bakgrunn av det iverksatte kontrolltiltak hvor elektronisk utstyr er brukt jfr. § 3 a).

Som hovedregel skal den behandlingsansvarlige gi melding til Datatilsynet før det iverksettes tiltak som medfører at personopplysninger behandles når dette blir utført ved hjelp av elektroniske hjelpemidler jfr. personopplysningsloven § 31 bokstav a).

Bestemmelsens siste ledd åpner derimot at «Kongen kan gi forskrift om at visse behandlingsmåter eller behandlingsansvarlige er unntatt fra meldeplikt, underlagt

forenklet meldeplikt eller underlagt konsesjonsplikt». For slike unntak kan det også gis forskrift for å begrense ulemper som behandlingen ellers kan medføre for den registrerte. Personopplysningsloven § 31 gir blant annet hjemmel for Personopplysningsforskriften § 7-11 hvor det gis unntak fra meldeplikten ved gitte vilkår, se punkt 2.1.1.

Personopplysningslovens formål er å «beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger» jfr. § 1. Videre skal loven «bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvern hensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger» jfr. personopplysningsloven § 1. Når det gjelder behovet for personlig integritet er det snakk om individers krav, som for eksempel arbeidstakers krav på å ha kontroll over personlige opplysninger om seg selv. For å ha kontroll over disse, må det forutsetningsvis innhentes samtykke fra individet/den ansatte for at hensynet til personlig integritet skal bli ivaretatt jfr. personopplysningsloven § 8.

I utgangspunktet baserer loven seg på at samtykke er det foretrukne behandlingsgrunnlag. Om samtykke ikke foreligger skal det foretas en avveining mellom arbeidsgivers behov for innhenting og behandling av personopplysninger og hensynet til arbeidstakers personvern jfr. personopplysningsloven § 8 f).

I følge § 8 kan arbeidsgiver kontrollere de ansattes IT-ressurs bruk om arbeidstaker gir sitt *samtykke* til det. Forutsetningen for samtykke skal ha virkning er at det skal være frivilling uttrykt, derfor er ikke samtykke spesielt egnet som rettsgrunnlag fordi arbeidstaker kan føle seg pliktet til å samtykke for å holde opprette nødvendig tillitt.

I forarbeidene fra personvernkommissjonen er det spesielt fire personvernprinsipper som gjør seg gjeldene i arbeidsforhold, retten til medbestemmelse, saklig begrunnelse, proporsjonalitet og kvalitet.¹⁵ Prinsippene samsvarer forøvrig i stor del med de prinsipper som arbeidsmiljølovens kapittel 9 stiller i forhold til kontrolltiltak.

¹⁵ NOU 1997: 19 Et bedre personvern

Prinsippet om retten til medbestemmelse gir arbeidstakerne en rett til å være med i avgjørelser om iverksettelse av kontrolltiltak der personopplysninger behandles. Prinsippet om medbestemmelse tar for seg noe av de samme utgangspunktene som samtykke gjør. Ved at arbeidstakerne skal være med å drøfte eventuelle tiltak før de iverksettes kan arbeidstakerne gi sin mening om tiltaket. For at arbeidstakere skal kunne være med å bestemme dette, er det i utgangspunktet viktig at det gis tilstrekkelig informasjon i forkant av eventuelle planer om tiltak. Det må videre åpnes for at arbeidstakere skal kunne komme med tilbakemeldinger enten direkte eller gjennom tillitsvalgte og/eller verneombud på arbeidsplassen, og det forutsettes videre at arbeidstakernes tilbakemeldinger faktisk blir gjennomgått av arbeidsgiver.

Prinsippet om saklig begrunnelse viser i stor grad til at virksomheten/arbeidsgiver må vise til et bestemt og saklig formål for å iverksette tiltak der det innhentes personopplysninger, og at formålet må være saklig begrunnet ut i fra virksomhetens behov før tiltak som innebærer innhenting av personopplysninger iverksettes.

Kravet til proporsjonalitet viser til at det må foretas en avveining mellom virksomhetens behov for å innhente personopplysningene og de ulemper dette medfører for den enkelte arbeidstaker, og at tiltaket må være adekvat i forhold til krenkelsen tiltaket medfører. Formålet er her at arbeidsgiver skal søke etter å iverksette det tiltaket som er minst inngripende ovenfor den ansatte.

Kravet til kvalitet innebærer at de opplysninger som registreres og behandles er riktige. Personopplysningsloven regulerer også når arbeidsgiver kan bruke opplysningene innhentet ved kontrolltiltak jfr. § 11. Som hovedregel har arbeidsgiver gyldig behandlingsgrunnlag når han har en «berettiget interesse» jfr. § 8.

Som et annet alternativ til behandlingsgrunnlag i personopplysningsloven § 8 kan den ansatte samtykke til at arbeidsgiver innhenter opplysninger om den ansatte. Samtykke som rettsgrunnlag i arbeidsforhold er som tidligere nevnt ikke særlig gunstig, da arbeidstaker kan føle seg forpliktet til å samtykke ovenfor arbeidsgiver, og den ansatte har dermed ikke en reell valgmulighet til å avstå fra å samtykke.

1.3.3 Personopplysningsforskriften

Når det gjelder overvåkning av ansattes bruk av elektronisk utstyr er personopplysningsforskriften § 9-2 2.ledd den sentrale bestemmelsen, fordi den direkte sier at «Arbeidsgiver ikke har rett til å overvåke arbeidstakers bruk av elektronisk utstyr, herunder bruk av internett».

Personopplysningsforskriften er hjemlet i personopplysningsloven og trådte i kraft samtidig med loven 1. januar 2001. Forskriftens kapittel 9 ble tilføyd ved forskrift 29 januar 2009 nr. 84 og trådte i kraft 1. mars 2009, kapittelet har fått overskriften «Innsyn i e-postkasse mv.». Kapittelets bestemmelser er med andre ord relativt nye i rekken av bestemmelser som omhandler kontroll og overvåkning på arbeidsplassen.

Forut for forskriften hadde personvernkommissjonen som oppgave å kartlegge blant annet personvernet i arbeidslivet. I følge Fornyings- og administrasjonsdepartementet var det behov for en avklaring av rettstilstanden på dette området, da grensen mellom lovlig og ulovlig innsyn ble opplevd som uklar av både arbeidsgivere og arbeidstakere. Overskriften «Innsyn i e-postkasse mv.» gir ikke direkte svar på at kapittelet også omhandler regler om arbeidsgivers begrensninger i og forbud mot å overvåke ansattes IT ressurs bruk generelt. Kapittelets formål er blant annet å klargjøre overfor brukerne hvor grensene for lovlig overvåkning på arbeidsplassen går.

Det som imidlertid er aktuelt for oppgavens tema er benevnelsen «mv.» som står for med videre. I § 9-1 annet ledd spesifiseres det at reglene i kapittelets virkeområde også omhandler «arbeidsgivers adgang til gjennom søkning av og innsyn i arbeidstakers personlige område i virksomhetens datanettverk og i andre elektroniske kommunikasjonsmedier eller elektronisk utstyr som arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet ved virksomheten.» Bestemmelsen tar med andre ord sikte på å dekke alle former for kommunikasjonsmedier, for eksempel tekstmeldinger/SMS og MMS sendt via mobiltelefon. Det forutsettes at det elektroniske utstyret er arbeidsgivers eiendom og er utstyret er ment for bruk i arbeidet, helt eller delvis. I hovedsak er det to bestemmelser som er treffende for oppgavens tema. § 9-2 annet ledd sier at «Arbeidsgiver har ikke rett til å overvåke arbeidstakers bruk av

elektronisk utstyr, herunder bruk av Internett, ut over det som følger av denne forskriften § 7-11.» Bestemmelsen i § 7-11 åpner for at logging av hendelser i datanettet er unntatt meldeplikten i personopplysningsloven § 31 i tilfeller hvor formålet er å administrere systemet eller for å avdekke/oppklare brudd på sikkerheten i edb-systemet. se punkt 2.1.1.

1.3.4 Internasjonal rett

Den europeiske menneskerettighetskonvensjonen av 4. november 1950 artikkel 8 nr. 1 slår fast at «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.»

EMK art. 8 nr. 1 gjelder også i arbeidssammenheng, dette bekreftes av blant annet i saken Copland mot UK, EMD 2007-04-03. Saken gjaldt overvåkning av en ansatts telefon, e-post og internettlinje. Arbeidsgiver hadde fått mistanke om at den ansatte, en assistent for rektor ved en skole i Wales, brukte arbeidsgivers kommunikasjonslinjer til private formål. Den ansatte ble ikke informert om at overvåkingen fant sted. Spørsmålet her var om bruk av arbeidsgivers utstyr til bruk ved privat korrespondanse var beskyttet av EMK art. 8 nr. 1. EMD har i tidligere avgjørelser sagt at EMK art 8 også gjelder på arbeidsplassen. EMD konkluderte med at innhenting, lagring og bruk av den private informasjonen som kom fram av overvåkingen var et inngrep i den ansattes «rett til privatliv» og følgelig et brudd på konvensjonen.

Vår personopplysningslov bygger på EUs personverndirektiv (1995/46/EF) og vil ha betydning ved tolkningen av loven. Direktivet omfatter de samme prinsipper som personopplysningsloven som formodes å være i overensstemmelse med internasjonal lovgivning.

Videre har den internasjonale arbeiderorganisasjonen ILO utarbeidet veiledende retningslinjer for beskyttelse av personvernet til arbeidstakere i *Protection of Workers' Personal Data* (ILO 1997) ved utarbeidelse av lovgivning og kollektive avtaler.

1.4 Metode

Oppgavens framstilling bygger på vanlig juridisk metode/rettskildelære.¹⁶

Utgangspunktet er tolkning av lovbestemmelser med respektive forarbeider. Jeg har anvendt Lovdatas database for søk på relevant rettspraksis i forhold til de gjeldende bestemmelsene. Fordi problemstillingen er av moderne tid er det ikke så mange treff på saker som omhandler tema, hverken juridisk litteratur eller saker som har kommet opp for domstolene. Det er fire dommer som er mest relevant for oppgaven, disse er brukt gjennomgående under de respektive punktene i oppgaven. Tre av dommene er fra tiden før personopplysningsforskriften trådte i kraft, men er fortsatt interessante for temaet. Jeg vil forsøke å gi svar på om utfallet av sakene ville fått et annet resultat om personopplysningsforskriften hadde vært trådt i kraft på tidspunktet. GPS-saken er den nyeste saken og har vært den saken av størst betydning da den tar for seg flere av problemstillingene kontroll ved bruk av elektronisk utstyr byr på.

Ved søk i lovdatas database på personopplysningsforskriftens § 9-2 er det per dags dato ingen relevante treff på rettsavgjørelser eller juridiske artikler som omhandler paragrafens annet ledd. De treff som kommer fram under søk på avgjørelser og litteratur omhandler alle arbeidsgivers rett til innsyn i e-postkasse.

Etter kontakt med Datatilsynet fikk jeg i midlertid tilgang til merknader de har gjort i forhold til kapittel 9. Disse vil ha mindre rettskildemessig vekt men er med på gi et bilde av hvordan tilsynet tolker bestemmelsene. Tilsynet er ansvarlig tilsynsmyndighet og har fått delegert forskriftskompetanse av Fornyings- og administrasjonsdepartementet (heretter kalt FAD). Datatilsynets oppgaver er blant annet å kontrollere at lover og forskrifter for behandling av personopplysninger blir fulgt, og at feil og mangler blir rettet jfr. personopplysningsloven § 42. Videre har jeg tolket høringsnotatet/ forslaget til ny personopplysningsforskriften utarbeidet av FAD.¹⁷ Høringsnotatet har vært den kilden som jeg har lagt mest vekt ved tolkning av personopplysningsforskriften på fordi det er de som har laget forskriften. Reelle hensyn har også blitt vektlagt som en sekundær kilde. Spesielt har reelle hensyn blitt vurdert der det har vært mangel på andre kilder. På grunn av lite rettspraksis tilhørende

¹⁶ Eckhoff, *Rettskildelære* (2005)

¹⁷ http://www.regjeringen.no/upload/kilde/fad/hdk/2006/0011/ddd/pdfv/293858-horingsnotat_epost.pdf

personopplysningsforskriften § 9-2 annet ledd, har jeg sett på rettstilstanden også før personopplysningsforskriften § 9-2 annet ledd trådte i kraft i 2009. Jeg har forsøkt å gi et svar om de sakene som omhandler tema vill fått et annet utfall om personopplysningsforskriften § 9-2 annet ledd hadde vært trådt i kraft på tidspunktet for fakta i sakene. Før 2009 var temaet regulert av arbeidsmiljøloven kapittel 9 og personopplysningsloven § 8 f) og § 11 og personopplysningsforskriften § 7-11. Disse bestemmelsene har fortsatt betydning ved spørsmålet om arbeidsgivers adgang til kontroll av ansattes bruk av elektronisk utstyr. Både Datatilsynets og Personvernemdas nettsider har jeg brukt som støttelitteratur og veiledning. Innholdet på sidene har ikke blitt vektlagt da de i har særlig rettskildemessig vekt. Personvernemda er klageorgan for Datatilsynets vedtak.

1.5 Videre framstillingstilling

I den videre framstillingen skal jeg ta for meg adgangen til kontroll av ansattes bruk av elektronisk utstyr under punkt 2.

Under punkt 2.1 er det bestemmelsen i personopplysningsforskriften § 9-2 annet ledd som er tema. . Bestemmelsen lyder: «Arbeidsgiver har ikke rett til å overvåke arbeidstakers bruk av elektronisk utstyr, herunder bruk av internett, ut over det som følger av denne forskriften § 7-11». Regelen er relativt ny i rekken, men en av de mest sentrale bestemmelsene når det gjelder kontroll og overvåkning av ansattes bruk av elektronisk utsyr. I punkt 2.1.1 vil jeg forsøke å redegjøre for hvilke tiltak karakteriseres som kontroll og når karakteriseres tiltaket som overvåkning? Dette er viktig fordi personopplysningsforskriften § 9-2 annet ledd omhandler kun *overvåking*.

Videre må det avklares hvilket *elektronisk utstyr* som omfattes av bestemmelsen, under punkt 2.1.2 skal jeg ta for meg nettopp dette. Til slutt bruker bestemmelsen ordene *arbeidstakers bruk*, under punkt 2.1.3 vil jeg se nærmere på hva som menes med dette.

I punkt 2.1. 4 er unntaket fra personopplysningsforskriften § 9-2 annet ledd jfr. § 7-11 tema. Unntaket gir arbeidsgiver adgang til innsyn i datalogger når formålet med innsynet er å administrere systemet eller når formålet er å avdekke/oppklare brudd på sikkerheten i edb-systemet.

I punkt 2.2 skal vi se at selv om personopplysningsforskriften § 9-2 forbyr overvåkning av ansattes bruk av elektronisk utstyr, kan arbeidsgiver ved konkret mistanke om brudd på arbeidsavtale eller illojalitet være berettiget til innsyn i bruk av elektronisk utstyr. Imidlertid må dette innsynet utføres som et kontrolltiltak jfr. arbeidsmiljøloven §§ 9-1 og 9-2. Om innsynet ikke utføres som kontrolltiltak etter arbeidsmiljøloven, blir det avgjørende om arbeidsgiver har adgang til å behandle opplysningene etter personopplysningsloven § 8 f). Imidlertid viser forarbeidene at de samme hensyn og vurderinger ligger bak arbeidsmiljøloven § 9-1 og personopplysningsloven § 8 f); «Kravet om saklig grunn vil normalt føre til at personopplysningslovens vilkår om berettiget interesse vil være oppfylt, mens vilkåret om forholdsmessighet/proporsjonalitet i alminnelighet vil innebære at kravet om at hensynet til arbeidstakernes personvern ikke må overstige arbeidsgivers berettigede interesse ikke vil være krenket.»¹⁸

Årsaken er fordi den ene fungerer ikke uten den andre; For de fleste arbeidsgivere er personopplysningene uinteressante hvis de ikke kan bruke de/behandle de. Derfor falt det naturlig og behandle begge bestemmelsene under ett i det følgende.

Under punkt 2.2.1 behandles formålskravet, alle kontrolltiltak skal ha et formål som skal være relatert til virksomhetens behov. GPS-saken er illustrerende for betydningen hvilke begrensninger formålet setter når det gjelder adgangen til å bruke opplysningene innhentet ved kontrolltiltak utover formålet, saken gjennomgås i punkt 2.2.1.1.

Under punkt 2.2.2 behandles saklighetskravet og kravet til berettiget interesse. Formålet med kontrolltiltak er bare rettmessig dersom det kan saklig begrunnes i forhold som vedrører virksomheten jfr. § 9-1 (1). Videre kan personopplysningene som følge av et iverksatt kontrolltiltak kun behandles om arbeidsgiveren har en «berettiget interesse» jfr. personopplysningsloven § 8 f).

I punkt 2.2.3 behandles forholdsmessighetskravet. Kravet baserer seg på det samme hensyn som personopplysningsloven § 8 f) stiller til arbeidsgiver som skal behandle

¹⁸ NOU 2004:5 s. 434

personopplysninger; arbeidsgivers berettigete interesse skal veies opp mot hensynet arbeidstakernes personvern.

I punkt 2.2.4 behandles kravet til informasjon og medinnflytelse ved iverksettelse av kontrolltiltak jfr. arbeidsmiljøloven § 9-2.

Til slutt vil jeg i punkt 3 oppsummere hva jeg har kommet fram til etter og ha skrevet denne oppgaven og mine synspunkter på rettstilstanden og reglens betydning i praksis.

2 ARBEIDSGIVERS ADGANG TIL KONTROLL AV ANSATTES BRUK AV ELEKTRONISK UTSTYR

2.1 Forbud mot overvåkning av elektronisk utstyr, herunder bruk av internett. Personopplysningsforskriften § 9-2 annet ledd.

Personopplysningsforskriften § 9-2 første ledd omhandler materielle vilkår for innsyn i arbeidstakers e-postkasse. Innsyn i e-postkasse er som nevnt tidligere ikke tema for denne oppgaven, men det kan kort sies her at arbeidsgiver som regel ikke har innsynsrett i e-post foruten om når det er nødvendig for å ivareta den daglige driften, berettiget interesse hos virksomheten eller ved begrunnet mistanke om grovt pliktbrudd. Forskriftens § 9-2 annet ledd derimot omhandler arbeidsgivers forbud mot å overvåke ansattes IT-ressursbruk:

«Arbeidsgiver har ikke rett til å overvåke arbeidstakers bruk av elektronisk utstyr, herunder bruk av internett, ut over det som følger av denne forskriften § 7-11».

Ordlyden i § 9-2 annet ledd sier at arbeidsgiver ikke har rett til å overvåke hverken internettbruk eller bruk av annet elektronisk utstyr. Bestemmelsen setter dermed

begrensninger i forhold til iverksettelse av kontrolltiltak hvor kontrollen innebærer overvåking av ansattes bruk av elektronisk utstyr. Generelle kontrolltiltak som har som formål å overvåkes ansattes bruk av for eksempel internett kan ikke iverksettes fordi dette vil stride i mot personopplysningsforskriften § 9-2.

Spørsmålene som stiller seg i forhold til tolkningen av personopplysningsforskriften § 9-2 annet ledd er hva som inngår i betegnelsen «å overvåke», hva regnes som «*elektronisk utstyr*» og når kan man si at det er «*arbeidstakers bruk av*» elektronisk utstyr/internett.

2.1.1 Når foreligger «overvåking»?

Det er viktig her at det skilles mellom tiltak som omhandler *kontroll* (punkt 2.2 og 2.3) og tiltak som utelukkende gjelder *overvåking* fordi § 9-2 annet ledd kun gjelder ved overvåking. Arbeidsmiljøloven kapittel 9 bruker uttrykket «kontrolltiltak», men overvåkingstiltak er også omfattet av begrepet kontrolltiltak og arbeidsmiljøloven §§ 9-1 og 9-2 gjelder også ved overvåking.

I Datatilsynets merknader til forskriftens kapittel 9 er det sagt «at forskriften ikke gir rettslig grunnlag for kontinuerlig overvåking av arbeidstakers bruk av elektronisk kommunikasjonsutstyr. Bestemmelsene i forskriften gjelder kun innsyn i enkeltstående tilfeller for konkrete formål. Logg i edb-systemer vil være en form for overvåking av arbeidstakers bruk av edb-systemet. Henvisningen til forskriftens § 7-11 om innsyn i og bruk av logg i edb-systemer, er derfor ment å tydeliggjøre at overvåking er tillatt i visse tilfeller, men bare til de klart definerte formålene som fremgår av forskriften (administrasjon av og/eller avdekking og oppklaring av sikkerhetsbrudd i edb-systemene).»¹⁹

Spørsmålet blir så om hvor lang tid må et innsyn vare for at det kan karakteriseres som kontinuerlig overvåking? En naturlig språklig forståelse av ordlyden tilsier at

¹⁹ http://www.datatilsynet.no/Global/05_regelverk/epostforskriften_merknader.pdf

kontinuerlig overvåkning ikke er en gangstille, men foregår over lengere tid. Ordlyden dekker med andre ord ikke en enkeltstående kontroll av ansattes bruk av elektronisk utstyr. Tidsaspektet vil her være avgjørende for om innsynet karakteriseres som overvåking. Men når kan man si at det er en kontinuerlig overvåkning? Kan arbeidsgiver sjekke dataloggen til kundekonsulenten som velge å besøke eksempelvis www.facebook.com i det hele tatt? Eller kan arbeidsgiver sjekke det en gang? Eller to ganger? Eller fire ganger? Hvor går grensa for at det er snakk om overvåkning?

I TINE kjennelsen (RG 2007 s.855) hadde arbeidsgiver iverksatt spaning med fotografering av en bestemt ansatt etter mistanker om at den ansatte stjal varer fra TINE. Spaningen var antatt å vare i ca. 1,5 timer. En vokter og en Tine ansatt fulgte etter den ansatte i bil til hans hjem. Retten ser på om spaningen kan likestilles med skjult videoovervåkning, noe som er ulovlig jfr. Rt. 2001 s. 668. En målrettet spaning som i denne saken kan ikke sidestilles med skjult videoovervåkning, fordi slik overvåkning blir karakterisert som «vedvarende», noe spaningen i denne saken ikke var. Om overvåkingen uttaler retten «at arbeidsgiver i dette tilfelle har basert iverksettelsen av kontrolltiltaket på en antatt konkret mistanke om misligheter, i det det er anført at det var kommet et tips om at A urettmessig tilegnet seg varer fra arbeidsgiver. Det var et målrettet tiltak mot en ansatt ved en konkret anledning; ikke løpende overvåking av ansatte på generelt grunnlag.»

Av dommen er det to momenter som er av betydning. For det første så er overvåking karakterisert som «vedvarende». For det andre kan man tolke det slik at vilkårlig kontroll er å anses som overvåking. Det vil si at om Tine ikke hadde hatt en konkret begrunnet mistanke om at den ansatte stjal varer vil spaningen ha bli ansett som ulovlig. Kjennelsen er fra før personopplysningsforskriften § 9-2 annet ledd trådte i kraft og gjelder riktignok ikke spaning med elektronisk utstyr, men saken illustrerer definisjonen av overvåking. Når det gjelder arbeidsgivers ønske om å overvåke en bestemt ansatt på bakgrunn av konkrete mistanke om illojal opptreden vil dette bli nærmere gjennomgått under punkt 2.3.

Reelle hensyn taler for at et enkelt innsyn i datalogger mest sannsynlig vil bli oppfattet som overvåking hvis muligheten for arbeidsgiver til et engangsinnsyn er vedvarende. Et innsyn som et engangstilfelle vil oppleves som overvåking fra den ansattes side hvis den ansatte ikke vet om når det et eventuelt innsyn vil skje. Dessuten kan loggen vise datatrafikk over en lengere tidsperiode noe som taler mot at skulle være tillatt.

I høringsnotatet fra FAD står det at ««Overvåke» innebærer at tiltaket har en viss varighet eller at det skjer gjentatte ganger. Motsatsen er det innsyn som er tillatt etter forskriften her.»²⁰

Høringsnotatet antyder at vil et enkeltstående innsyn ikke kan utelukkes. Eksempelvis ved konkret mistanke om mislighold av arbeidsreglement, illojalitet eller brudd på arbeidsavtale (punkt 2.2).

2.1.2 Hvilket «elektronisk utstyr» viser forskriften til?

Ut i fra en naturlig språklig forståelse av ordlyden er det naturlig å tenke at alt elektronisk utstyr omfattes. I forarbeidene til forskriften derimot definerer FAD at ««Elektronisk utstyr» omfatter datamaskiner-herunder printere, mobiltelefoner, PDAer og lignende. Elektronisk utstyr står i motsetning til ordinært «elektrisk utstyr» hvor behandling av personopplysninger ikke er forutsatt eller nødvendig som følge av systemet».²¹

I Datatilsynets merknader står det at den omfatter elektronisk lagrede dokumenter og elektronisk kommunikasjonsmedier, herunder PCer og mobiltelefoner.²² Hverken høringsnotatet fra FAD eller Datatilsynets merknaden sier noe om den også gjelder for

²⁰ http://www.regjeringen.no/upload/kilde/fad/hdk/2006/0011/ddd/pdfv/293858-horingsnotat_epost.pdf

s. 26

²¹ http://www.regjeringen.no/upload/kilde/fad/hdk/2006/0011/ddd/pdfv/293858-horingsnotat_epost.pdf

²² http://www.datatilsynet.no/Global/05_regelverk/epostforskriften_merknader.pdf

sporingsutstyr. Selv om det vil det være naturlig å forstå at også slikt utstyr omfattes, taler det i mot at sporingsutstyr er omfattet siden ikke noen av kilden tilsier det.

Imidlertid påpeker Datatilsynets merknad videre at håndholdte enheter omfattes, så lenge disse er stilt til arbeidstakers personlige disposisjon under utførelsen av arbeidet.²³ Som tidligere nevnt i punkt 1.2.2 skilles det mellom håndholdt GPS som enkelt kan tas med inn og ut av kjøretøyet og fastmontert sporingsutstyr. Den håndholdte GPS-en vil med andre ord være omfattet av bestemmelsen. Om sporingsutstyr omfattes vil bero på en tolkning av begrepet «bruk av», se punkt 2.1.3

Både merknaden og høringsnotatet sier videre at private mobiltelefoner og annet elektronisk utstyr eid av arbeidstakerne er ikke omhandlet av forskriftens kapittel 9.

Innsynsretten gjelder heller ikke i de tilfeller der arbeidsgiver låner ut elektronisk utstyr som er ment for kun privat bruk.

I følge høringsnotatet gjelder bestemmelsen for gjennomgang av aktivitetslogger, gjennomgang av selve utstyret og gjennomgang ved fjerntilganger (skygging). Det er irrelevant om hvordan informasjonen hentes inn, det vil si at speilkopier og andre back-up metoder er omfattet. Videre påpekes det at elektronisk kommunikasjon som bruk av SMS, MMS, MSN, Skype o.l er omfattet av reglene.²⁴

2.1.3 «Bruk av» elektronisk utstyr

Bestemmelsen bruker ordlyden «bruk av» elektronisk utstyr. Her må det antas at bestemmelsen ikke omfatter overvåkning av elektronisk utstyr som ikke blir brukt aktivt av arbeidstaker. Men hvilke krav stilles til at utstyret skal være brukt av den ansatte? Er det fysisk berøring eller at utstyret er «tatt i bruk»? Eksempelvis vil et sporingsutstyr som er fastmontert i kjøretøyet og ikke kan fjernes med enkle grep, ikke bli fysisk berørt av arbeidstakeren. Sporingsutstyret er ikke et utstyr som den ansatte aktivt bruker, men inneholder en elektronisk sender og mottaker i kjøretøyet som gir arbeidsgiver muligheten til å overvåke den ansattes bevegelser. Selv om bestemmelsen i første omgang kan gi inntrykk av at den også gjelder for sporingsutstyr viser GPS saken

²³ http://www.datatilsynet.no/Global/05_regelverk/epostforskriften_merknader.pdf

²⁴ http://www.regjeringen.no/upload/kilde/fad/hdk/2006/0011/ddd/pdfv/293858-horingsnotat_epost.pdf

det motsatte. Personopplysningsforskriften § 9-2 annet ledd var trådt i kraft på tidspunktet da innføringen av sporingsutstyr ble innført i GPS saken, men bestemmelsen er hverken nevnt i dommen eller kjennelsen.²⁵ Rettspraksis taler dermed i mot at sporingsutstyr er omfattet av forskriftens § 9-2 annet ledd. Begrunnelsen er sannsynligvis nettopp den at sporingsutstyret ikke ble aktivt brukt av den ansatte og bestemmelsen treffer dermed ikke sakens fakta.

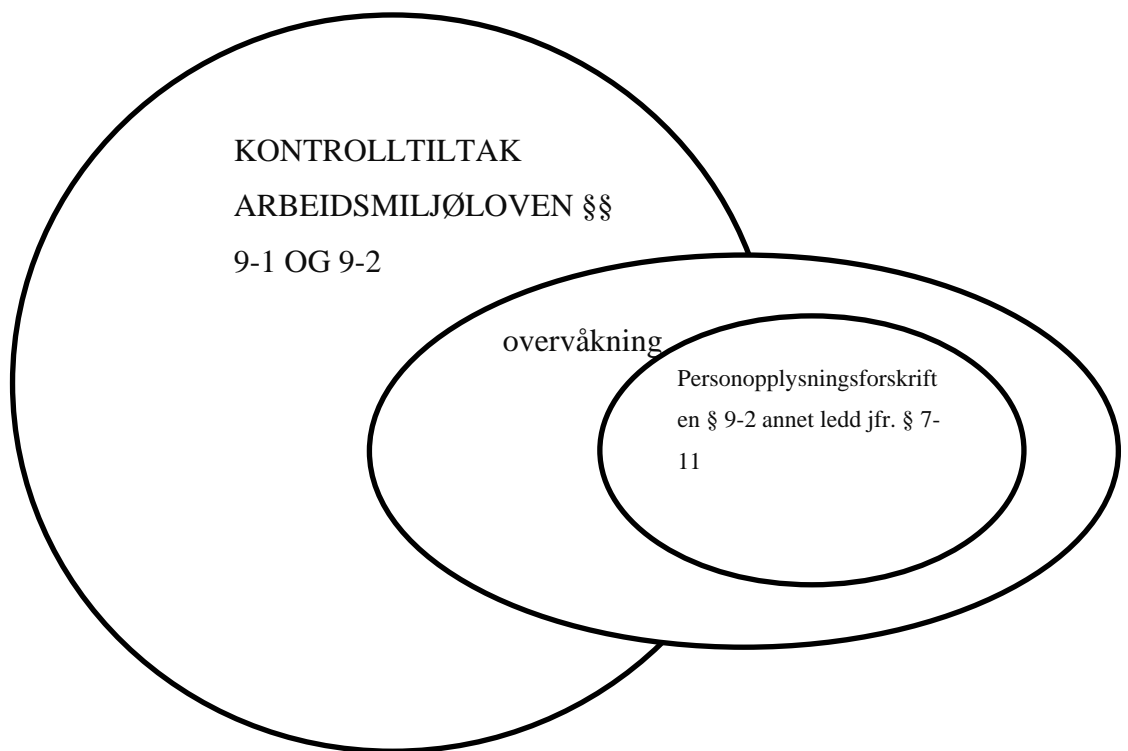
Personopplysningsforskriften § 9-2 2. ledd er heller ikke nevnt i Datatilsynets veileder om «GPS og sporing i yrkesbiler», derimot presiseres viktigheten av etterlevelse av overnevnte regler i personopplysningsloven og arbeidsmiljøloven.²⁶

Som tidligere nevnt omfattes mobiltelefonbruk av bestemmelsen, men spørsmålet er om den også omfatter spesifisert telefonregning. Telefonselskapene har muligheten til å spesifisere telefonregninger for kunden (her arbeidsgiver). En spesifisert telefonregning vil kunne gi opplysninger om den ansatte som kan karakteriseres som personopplysninger. Den spesifiserte telefonregningen er et dokument som viser kommunikasjon mellom den ansatte og hans korrespondenter. Om denne informasjonen blir brukt til annet enn fakturakontroll vil reelle hensyn tale for at § 9-2 annet ledd forbyr at arbeidsgiver gjør innsyn i en spesifisert telefonregning på vilkårlig basis, da dette må antas å være overvåkning. Man kan i så tilfelle spørre seg om lovligheten med å ha spesifisert regning som gir mere informasjon enn bare hvor mye som er brukt i kroner og øre. Svaret vil antageligvis bero på at en spesifisert telefonregning ikke er så annerledes enn en logg i et datanettverk, som er tillatt jfr. personopplysningsforskriften § 7-11 (se punkt 2.1.4).

²⁵ RG 2011 s.321 og TNHER-2010-144876-2. Personopplysningsforskriften trådte i kraft 1. mars 2009. Bedriften i GPS saken innførte sporingsutstyret sommeren 2009.

²⁶ http://www.datatilsynet.no/templates/article___3578.aspx

Figur 1)



Figuren over illustrerer personopplysningsforskriften § 9-2 annet ledds virkeområde i forhold til andre kontroll- og overvåkningstiltak. Ikke all overvåkning er omfattet av personopplysningsforskriften § 9-2 annet ledd jfr. § 7-11, for eksempel overvåkning med sporingsutstyr. Men overvåkning med sporingsutstyr vil omfattes av arbeidsmiljølovens regler om kontrolltiltak jfr. kapittel 9 i arbeidsmiljøloven.

Bestemmelsen i § 9-2 annet ledd er ufravikelig jfr. forskriftens § 9-5, det vil si at det ikke er adgang for arbeidsgiver å inngå avtale med arbeidstakere at overvåkning i henhold til § 9-2 annet ledd iverksettes.

2.1.4 Arbeidsgivers adgang til innsyn i datalogger ved administrasjon eller ved oppklaring/avdekking av brudd på sikkerheten i edb-systemet jfr. personopplysningsforskriften § 7-11.

I følge personopplysningsforskriften § 9-2 annet ledd har arbeidsgiver ikke innsyn i datalogger som registrer datatrafikk, med unntak av i to tilfeller jfr.

personopplysningsforskriften § 7-11 som lyder:

«Behandling av personopplysninger som følge av registrering av aktiviteter (hendelser) i et edb-system, samt behandling av personopplysninger om disposisjoner til ressurser i systemet, er unntatt fra meldeplikten etter personopplysningsloven § 31 første ledd.

Unntak fra meldeplikt gjelder bare dersom behandlingen har som formål

- a) å administrere systemet, eller
- b) å avdekke/oppklare brudd på sikkerheten i edb-systemet.

Personopplysninger som fremkommer som følge av behandlinger etter annet ledd, kan ikke senere behandles for å overvåke eller kontrollere den enkelte.»

I følge forarbeidene til arbeidsmiljøloven vil arbeidsgiver normalt ved bruk av datalogger til de formål som er beskrevet i § 7-11 ha en berettiget interesse etter personopplysningsloven § 8 f).²⁷

²⁷ NOU 2004:5 s. 428

Administrasjon av systemet vil typisk være vedlikehold av dataprogrammer og datanettverk i form av oppdateringer og oppgraderinger ofte utført av bedriftens IT avdeling.

Rt. 2001 s. 1589, Raufoss, illustrerer temaet. Saken gjaldt oppsigelse på grunn av bruk av arbeidsgiverens internettlinje til private formål. Arbeidstakeren, A, var ansatt som driftskonsulent ved IT-avdelingen ved bedriften. Bedriften fattet mistanke om at noen brukte internettlinjen til nedlastning fordi de hadde mottatt flere klager fra de ansatte. Klagene var begrunnet med at internettlinjen ved bedriften ikke hadde tilfredsstillende kapasitet, blant annet var det lang ventetid og av og til falt brukerne ut av internettlinjen. Bedriften brukte så ressurser på å forbedre internettlinjens kapasitet uten at dette ga tilfredsstillende resultat. Arbeidsgiveren ved IT-sjefen valgte derfor å ta ut en utskrift av brannmurloggen over den interne internettbruken ved en tilfeldig valgt dato. Det viste seg at en av de ansattes (en driftskonsulent ved IT avdelingen(A) PCer sto for ca. halvparten av nedlastningen både denne dagen og ved etterfølgende brannmurslogg utskrifter gjort senere. Den ansattes internettbruk sto for ca. 16-20 PCers normale internettforbruk ved bedriften.

Dette førte til at IT-sjefen og en kollega låste seg inn på As kontor etter endt arbeidsdag for å undersøke hans to PCer nærmere. Dette resulterte i at de fant ca. 500 lagrede musikkfiler på den ene PC-en, og ca. 1000 på den andre PC-en han hadde til disposisjon i arbeidet. Arbeidsgiveren reagerte med oppsigelse av A.

A gikk til sak mot sin arbeidsgiver og mente at bedriften hadde overtrådt grensen for både ulovfestet og lovfestet personvern og at oppsigelsen var usaklig etter dagjeldende arbeidsmiljøloven § 60 nr. 1.

Vedrørende spørsmålet om oppsigelsen var usaklig mente retten at den ansattes misbruk av internettlinjen ble ansett for å være et brudd på den lojalitetsplikt en arbeidstaker har ovenfor sin arbeidsgiver, spesielt hvor den ansatte her hadde som arbeidsoppgaver å yte dataservice internt i avdelingen, og var kjent med følgene av misbruket. Det ble videre lagt vekt på at bedriften hadde opprettet en instruks for de ansatte hvor det blant annet sto: «Datautstyr skal kun brukes for tjenesteformål godkjent av linjeledelsen».

Reglementet var kjent for alle ansatte ved at den var lagt ut på nettet og var tilgjengelig for alle. Retten konkluderte med at oppsigelsen var saklig.

Når det gjelder spørsmålet om arbeidsgiveren hadde rett til å ta utskrift av loggen og gjennomføre As PC vurdere retten dette i forhold til dagjeldende personregisterlovens hovedforskrift § 2-20 som samsvarer med gjeldende personopplysningsforskrift § 7-11 første og annet ledd, tredje ledd er ny. Retten uttaler at: «Selv om utskriften av loggen og de øvrige undersøkelsene av brannmurloggene i desember 1999 ga informasjon om aktiviteten på As PCer, måtte undersøkelsen aksepteres som « administrasjon av systemet », jf. annet ledd. Bedriften hadde et legitimt behov for å søke å få bedret utnyttelsen av internettlinjen, som var et tiltagende problem i det løpende arbeid på IT-avdelingen, og jeg kan ikke se at hovedforskriftens § 2-20 annet ledd utgjør noe hinder for bedriften til i dette tilfellet å gå videre med den informasjon man så langt hadde innhentet om As belastning av internettlinjen, og eventuelt benytte denne ved oppsigelse av A.»²⁸ Videre uttaler retten om rettmessigheten av å låse seg inn på den ansattes kontor og ta utskrift fra den ansattes harddisk: «Jeg finner det ikke påkrevet å ta stilling til dette spørsmålet. Bedriftens handlemåte må sees i lys av at ordningen ved IT-avdelingen etter det opplyste var slik at det var vanlig og akseptert at de ansatte gikk inn på hverandres kontorer og til dels brukte hverandres PC'er. Utskriften ble tatt da man med dette som utgangspunkt oppdaget at As PC'er fortløpende lastet ned musikkfiler fra internett. Jeg kan ut fra dette vanskelig se at det kan rettes kritikk av betydning mot at ledelsen av IT-avdelingen gikk frem som den gjorde, og bedriften kan ikke være avskåret fra å bruke opplysningene i utskriften i forbindelse med oppsigelsen.»²⁹

I forhold til dagens § 7-11 tredje kan det stilles spørsmålstegn ved arbeidsgiveres undersøkelser av As PC på bakgrunn av utskriften av brannmurloggen. Gjeldende § 7-11 tredje ledd sier at «Personopplysninger som fremkommer som følge av behandlinger etter annet ledd, kan ikke senere behandles for å overvåke eller kontrollere den enkelte.» Tredje ledd var ikke en del av dagjeldende personregister forskrift § 2-20. Om hendelsen hadde funnet sted i dag, ville trolig hendelsen hvor IT-sjefen låste seg

²⁸ Sitat s.1598

²⁹ Sitat s.1598 og s.1599

inn på As kontor og undersøkelser av As PC blitt ansett som brudd på dagens personopplysningsforskriften § 7-11 tredje ledd.

Arbeidsmiljøloven kapittel 9 var heller ikke trådt i kraft på tidspunktet for hendelsen. Retten hadde trolig gått inn og vurdert om bestemmelsen for iverksettelse av kontrolltiltak jfr. arbeidsmiljøloven §§ 9-1 og 9-2 var fulgt om hendelsen hadde skjedd i dag. Imidlertid ville antakeligvis ikke saken ha fått et annet utfall fordi arbeidsgiveren hadde en konkret begrunnet mistanke om illojalitet, som er vi skal se er godkjent som saklig grunn/berettiget interesse for iverksette kontroll jfr. arbeidsmiljøloven § 9-1 og personopplysningsloven § 8 f) (Se punkt 2.2). Endelig ville retten antageligvis etter dagens regler uansett tillatt beviset (loggene + undersøkelsen av PC-en) ført selv om det forelå brudd på § 7-11 tredje ledd av hensyn til sakens opplysning og betydningen av å oppnå en materielt riktig avgjørelse jfr. RG 2011 s.321, GPS kjennelsen (Se punkt 2.2.1.1).

I forhold til arbeidsgivers adgang til innsyn etter alternativ b), avdekke/oppklare brudd på sikkerheten i edb-systemet må det antas at det faktisk må foreligge en mistanke om at brudd foreligger jfr. ordlyden «avdekke/oppklare».

I Rt. 2005 s.518, ConocoPhillips, var det spørsmål om avskjedingen av to ansatte ved petroleumsselskapet ConocoPhillips var gyldig. Begrunnelsen for avskjedighetene var at de to ansatte hadde vesentlig misligholdt arbeidsavtalene ved å besøke nettsted, laste ned og lagre materiale med pornografisk innhold på arbeidsplassens PCer. Dette var forbudt etter arbeidsreglementet som de ansatte var kjent med. Ledelsen var kjent med at bedriftens PCer ble brukt til slike formål, men forholdt seg passiv til dette over lengere tid. Det var først etter at det ble rapportert om mulig nedlastning av barnepornografisk materiale at arbeidsgiveren foretok undersøkelser av PCene som var disponert av de ansatte. Som begrunnelse for avskjedighetene la arbeidsgiveren fram logger fra de respektive PCer som var brukt av de ansatte. Arbeidsgiveren anførte at brudd på arbeidsreglementet medførte en sikkerhetsrisiko og at muligheten for virus økte ved besøk på nettsider og nedlastning av pornografisk materiale.

Spørsmålet for retten var om undersøkelsen kunne hjemles i personopplysningsforskriften § 7-11 b) som gir arbeidsgiver adgang til å behandle personopplysninger om formålet er å avdekke brudd på sikkerheten i systemet. Videre om det egentlig var avdekkingen av mulige straffbare forhold som var utslagsgivende for iverksettelsen av undersøkelsene, og ikke på grunn av sikkerhetsmessige årsaker jfr. personopplysningsforskriften § 7-11 b).

Arbeidsgiveren hadde bedt Datatilsynet om å uttale seg om undersøkelsen av PCene etter at de ansatte hadde påpekt at det forelå brudd på personvernlovgivningen ved undersøkelsen av PCene; «Datatilsynet kom til at det klart var adgang til å søke generelt i systemet etter filer, og at det heller ikke var grunnlag for kritikk mot bedriften for at man hadde gått inn på den enkelte brukers område. Det ble lagt vekt på at de filer man søkte etter, så tydelig var definert som ulovlig på grunn av systemets sårbarhet. Derimot var tilsynet i sterk tvil om hvorvidt bedriften sto fritt til å bruke de funn som ble gjort, som grunnlag for arbeidsrettslige reaksjoner mot de ansatte. Når dette ble akseptert, ble det blant annet lagt vekt på at den aktuelle bruken var et så klart brudd på fastsatte retningslinjer at det ville være urimelig om man skulle være avskåret fra å aksjonere.»³⁰ Videre uttaler retten i forhold til personopplysningsforskriften § 7-11 b) sitt anvendelsesområde: «Så langt de undersøkelser som foretas har som formål å avdekke ansattes nedlastning av filer med pornografisk materiale i klar strid med bedriftens regler ut fra en saklig begrunnet oppfatning om at slik aktivitet utgjør en reell sikkerhetsrisiko, kan jeg vanskelig se at dette skulle være i strid med de nevnte reglene i personopplysningslov med forskrift. Jeg må videre legge til grunn at bedriften kunne ha valgt en alternativ fremgangsmåte ved at man i forkant hadde tatt opp med tilsynet på generelt grunnlag behovet for en nærmere kontroll av hensyn til det særlige behov for et høyt sikkerhetsnivå ved petroleumsutvinning. At man skulle være avskåret fra å foreta undersøkelser i slikt øyemed, kan jeg ikke anta.»³¹ Retten konkluderer imidlertid med at avskjedighet var en uforholdsmessig reaksjon og at undersøkelsene ga uttrykk for å ha vært av vilkårlig utført overfor de ansatte, fordi arbeidsgiver over lang tid hadde forholdt seg passiv til surfing på pornografi.

³⁰ Avsnitt (56) i dommen.

³¹ Sitatet er hentet fra avsnitt (58) i dommen.

Bruddet på arbeidsreglementet kunne heller ikke føre til oppsigelse og de ansatte ble tilkjent en erstatning for urettmessig avskjedighet.

Dommen viser at personopplysningsforskriften § 7-11 b) ikke skal brukes om andre alternative metoder kan anvendes for å oppklare brudd, spesielt i de tilfeller der arbeidsgiver vet om at slike brudd foregår. Eksempelvis kan ikke en arbeidsgiver legge fram brannmurlogg for å vise at ansatte besøker for eksempel Facebook, selv om det er forbudt i arbeidsinstruksen, om det ikke beviselig kan anses å være en sikkerhetstrussel. I ConocoPhillips uttaler en sakkyndig at det ikke innebærer en større sikkerhetsrisiko å besøke nettsider med pornografisk innhold enn andre nettsider.³²

2.2 Arbeidsgiver adgang til å kontrollere ansattes bruk ved konkret mistanke om mislighold av arbeidsreglement, illojalitet eller brudd på arbeidsavtale. Herunder adgangen til å bruke opplysningene som fremkommer av kontrolltiltaket.

I mange tilfeller ønsker arbeidsgiver å gjøre innsyn i ansattes bruk av elektronisk utstyr fordi de har en konkret mistanke om at den ansatte misligholder arbeidsreglementet, opptrer illojalitet eller bryter arbeidsavtalen på annen måte. Slike konkrete mistanker er temaer som går igjen i flere av de rettssakene som omhandler arbeidsgivers kontroll av ansattes bruk av elektronisk utstyr.³³

Når det gjelder konkret mistanke om brudd på arbeidsreglement og arbeidsavtale er vurderingen mer sammensatt fordi iverksettelsen av et kontrolltiltak gjort etter arbeidsmiljølovens prosessuelle regler ofte ikke er praktisk gjennomførbare i slike tilfeller. Dette fordi behovet for kontroll gjerne oppstår tidsmessig akutt og faren for at

³² Rt. 2005 s. 518, avsnitt (46).

³³ Rt. 2005 s.518, Rt. 2001 s.1581, RG 2011 s.321.

den ansatte kan forspille bevis er særlig aktuell hvor det er tatt i bruk elektronisk utstyr.³⁴

Når mistanken om illojalitet oppstår iverksetter arbeidsgiver tiltak for å avklare mistanken, dette kan for eksempel være innhenting av opplysninger fra en brannmurlogg. Denne innhenting og bruken av informasjonen ansees som et kontrolltiltak som må iverksettes etter arbeidsmiljølovens §§ 9-1 og 9-2. Denne kontrollen vil ikke bli berørt av personopplysningsforskriften § 9-2 annet ledd, fordi kontrollen ikke er å anse som overvåkning, fordi den ikke er vedvarende, ei heller vilkårlig, men iverksatt mot den ansatte mistanken retter seg mot.

Under vil jeg redegjøre for hvordan et kontrolltiltak iverksettes, både generelt og i forhold til tiltak for å avdekke illojalitet ved konkret mistanke.

2.2.1 Arbeidsmiljøloven § 9-1 krav til formål ved kontrolltiltak

Det stilles krav til alle kontrolltiltak at de skal ha et bestemt formål.

Formålet med kontrolltiltak kan være mange, det kan for eksempel å effektivisere driften, kvalitetssikring av produksjonen, innføring av tiltak på grunn av sikkerhetsmessige årsaker eller tiltak som er nødvendig for å oppfylle krav som loven stiller. I tilleggssavtale V til Hovedavtalen mellom LO og NHO (2002-2005) punkt 1 står det at kontrolltiltak kan ha sitt grunnlag i teknologiske, økonomiske, sikkerhets- og helsemessige omstendigheter, samt andre sosiale og organisatoriske forhold i bedriften. Formålet i seg selv kan også være å avdekke illojalitet eller ineffektivitet.

Imidlertid er det ofte slik at hovedformålet med tiltaket ikke er den kontrollmuligheten tiltaket gir, men andre hensyn, som nevnt ovenfor. En kan på en måte si at kontrollmuligheten er noe som «følger med på kjøpet». For eksempel kan formålet med innføring av elektroniske adgangskort (tilgangskontroll) på arbeidsplassen kan ha sikkerhetsmessige årsaker, man ønsker for eksempel ikke at uvedkommende skal

³⁴ I noen tilfeller kan speilkopi anvendes for å sikre informasjonen, dette er en operasjon som forutsetter en del datakyndighet og ikke er enkel å utføre hos mindre bedrifter uten datahjelp.

komme seg inn i lokalene. Men samtidig som man for kontroll på dette vil informasjon om den ansatte som benytter kortet, komme fram. Informasjon om hvor og når en ansatt passerer en dør, og hvor lenge personen blir der registreres. Dette er informasjonen som «følger med på kjøpet». Det samme gjelder ved brannmurlogging av datanettverk, hvor formålet er å administrere systemet og ivareta datasikkerheten, men loggingen vil også kunne gi svar på de ansattes aktivitet i datanettverket.

Dette åpner for at arbeidsgiver har muligheten til å bruke en og samme informasjonskilde til vidt forskjellige former for kontroll. Denne problemstillingen kan i teorien virke uproblematisk. I følge personopplysningsloven § 11 b) skal informasjonen som kommer fram på bakgrunn av kontrolltiltaket kun brukes til det «uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet». Videre sier § 11 c) at «den behandlingsansvarlige skal sørge for at personopplysningene som behandles ikke brukes senere til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker».

I Ot.prp.nr. 92 (1998-1999) side 113 står det:

«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.»

«Et eksempel på formål som ofte vil være uforenlig med innsamlingsformålet, er bruk av opplysningene til kontrollformål, særlig når kontrollen ikke er en naturlig del av den virksomheten den behandlingsansvarlige driver, eller når ubehaget for den registrerte ikke står i et rimelig forhold til fordelene kontrollen oppnår.»

Et viktig hensyn som ligger bak personopplysningsloven § 11 b) og c) er arbeidstakernes/den registrertes krav til forutberegnelighet. Arbeidstakerne skal til enhver tid vite hva som registreres av opplysninger om de og hvilket formål opplysningene skal brukes til. Bestemmelsen er også ment for å beskytte de ansatte mot at tilleggsinformasjonen som kontrolltiltaket frambringer brukes på en uønsket/uforutsett måte. I følge loven er det kun samtykke som er gyldig

behandlingsgrunnlag for å kunne bruke opplysningene til annet formål enn det opprinnelige.

Eksempelvis om en bedrift innfører et kontrolltiltak med formål A og B, så kan ikke opplysningene brukes til formål C. I utgangspunktet vil det være slik at et kontrolltiltak nettopp defineres av sitt formål. Med det menes det at om opplysningene skal kunne bli brukt til formål C, så må tiltaket defineres som et nytt kontrolltiltak som må hjemles i arbeidsmiljøloven §§ 9-1 og 9-2 og personopplysningsloven § 8.³⁵ I praksis kan denne problemstilling vise seg å være noe annerledes. Det kan tenkes at arbeidsgiver har konkrete mistanker om at en ansatt opptrer illojalt ved at han bryter arbeidsreglement eller arbeidsavtale og at arbeidsgiver ønsker å bruke opplysningene innhentet ved kontrolltiltaket til å bekrefte/avkrefte mistanken. I så tilfelle skal det iverksettes et nytt enkeltstående kontrolltiltak for å avdekke mistanken. Om dette ikke blir utført etter arbeidsmiljølovens regler om iverksettelse av kontrolltiltak, blir spørsmålet om arbeidsgiver allikevel har adgang til å bruke denne tilleggsinformasjonen, og i så tilfelle når?

2.2.1.1 GPS saken³⁶

GPS- saken illustrerer hvor viktig det er at formålet defineres før et kontrolltiltak iverksettes. Saken viser også hvordan såkalte tilleggsopplysninger et kontrolltiltak gir kan bli gjenstand for konflikt når arbeidsgiver ønsker å bruke disse til annet enn det opprinnelige formålet med iverksettelse av et kontrolltiltak.

I september 2010 gikk en renovasjonsbilsjåfør til sak mot sin tidligere arbeidsgiver med påstand om usaklig oppsigelse jfr. arbeidsmiljøloven § 15-7. Arbeidsgiveren mente at renovasjonsbil sjåføren hadde tatt uforholdsmessige lange pauser som igjen førte til uberettiget overtidssjobbing. Som bevis la arbeidsgiveren fram logger fra sporingsutstyr

³⁶ Saken omfatter kjennelse angående bevisavskjæringsspørsmålet fra Hålogaland lagmannsrett, RG 2011 s. 321, dom fra Nord Troms tingrett, TNHER-2010-144876-2 og dom fra Hålogaland lagmannsrett, LH-2011-155315.

installert i renovasjonsbilen han brukte i sitt arbeid og sammenstilte disse med den ansattes timelister som grunnlag for oppsigelsen. Spøringsutstyret var blitt innført ved bedriften sommeren 2009.

Under saksforberedelsen til tingretten begjærte arbeidstakeren sammenstillingen av timelistene hans og GPS-loggen avskåret som bevis. Arbeidstakeren anførte at beviset var framskaffet på en «utilbørlig måte» jfr. tvl. § 22-7, og at bruken av opplysningene fra GPS-systemet ikke var forenelig med det opprinnelige formålet med innføringen av systemet.

I mars 2011 ble bevisavskjæringsspørsmålet behandlet av lagmannsretten, RG 2011 s. 321. I kjennelsen ble det påpekt at «det opprinnelige formålet med innføringen av systemet var primært å få på plass en effektiv administrasjon og drift av en vesentlig del av bedriftens oppgaver, samt bruke det til å utarbeide arbeidsplaner og normere tidsforbruket på rutene.»³⁷

At GPS-loggene ble sammenstilt med timelistene til en ansatt og lagt fram i etterkant som et bevis i en oppsigelsessak var ikke tiltenkt som en del av formålet med innføringen av systemet. Retten konkluderer med at det nye formålet var uforenelig med det opprinnelige.

Selve innføringen av GPS-systemet ble ansett som et lovlig iverksatt kontrolltiltak jfr. arbeidsmiljøloven og personopplysningsloven § 8 f), men behandlingen av opplysningene til et nytt formål måtte derfor anses som et nytt kontrolltiltak.

Lagmannsretten påpekte at personopplysningsloven § 11 c) forhindrer arbeidsgiveren å bruke opplysningene til senere formål som er uforenelige med det opprinnelige formålet med innsamlingen. Videre ble det konkludert med at det ikke forelå samtykke fra arbeidstakeren til å bruke opplysningene utover det opprinnelige formålet. Det ble konkludert med at bedriften ikke hadde gyldig hjemmelsgrunnlag for å behandle de nye opplysningene jfr. personopplysningsloven § 8 f), det ble her sett hen til vurderingsmomentene etter arbeidsmiljøloven §§ 9-1 og 9-2. Retten bemerker at sammenstillingen av opplysningene kunne vært rettmessig om bedriften hadde opplyst om dette i forkant jfr. drøftelses og informasjonsplikten jfr. arbeidsmiljøloven § 9-2.

³⁷ RG 2011 s. 321, sitat s. 324

Imidlertid konkluderer retten med GPS-loggene sammenholdt med timelistene kunne fremlegges som bevis i saken fordi krenkelsen var begrenset, utilbørligheten ved fremskaffelsen av beviset ikke var grov. I tillegg var beviset av vesentlig betydning for å oppnå en materielt riktig avgjørelse. Ved vurderingen ble det sett hen til om føringen av beviset medførte en krenkelse av tungtveiende rettsikkerhets- eller personvern hensyn.³⁸ I sin begrunnelse sammenligner retten saken med en annen sak der en arbeidstaker ble utsatt for skjult video-overvåkning på arbeidsplassen, hvor krenkelsen ble ansett som grov.³⁹ I GPS-saken derimot sier retten at «krenkelsen ikke er mer alvorlig enn at opplysningene sannsynligvis kunne vært lovlig ervervet i henhold til personopplysningsloven dersom B AS hadde innledet en prosess for et nytt og fremtidig kontrolltiltak»⁴⁰, videre sammenholder retten dette med at opplysningene som var registrert om arbeidstakeren var kjent for ham. Retten bemerker videre at «bruk av GPS karakteriseres som mindre inngripende i sentrale rettsgoder enn overvåkning ved bruk av lyd og bilde.»⁴¹ Til slutt uttaler lagmannsretten at: «Sammenstillingen av opplysningene fra GPS-systemet med timelistene har mer karakter av det som i proposisjonene er betegnet som «tradisjonelle kontrolltiltak» enn et tiltak som medfører et «ikke ubetydelig inngrep» i sentrale rettsgoder. Lagmannsretten mener følgelig at graden av krenkelse er begrenset.»⁴²

Selv om GPS saken ikke omhandler elektronisk utstyr *brukt av* den ansatte, så vil saken ha betydning for saker som gjelder *bruk av* elektronisk utstyr. Begrunnelsen er som nevnt at personopplysningsforskriften § 9-2 annet ledd gjelder ved overvåkning og hindrer ikke for at arbeidsgiver kan iverksette et enkeltstående tiltak for å avdekke

³⁸ I RG 2004 s. 347 hadde en arbeidsgiver hentet ut filer med pornografisk innhold fra arbeidstakers PC og ønsket å legge disse fram som bevis i en oppsigelsessak. Arbeidstakeren påberopte bevisavskjæring. Lagmannsretten konkluderte med at beviset var innhentet i strid med personopplysningsloven, men at det likevel skulle tillates ført. Hensynet til sakens opplysning og den fri bevisdømmelse måtte veie tyngre enn personvern hensynet.

³⁹ Rt. 1991 s.616

⁴⁰ RG 2011 s.321, sitat s. 326

⁴¹ RG 2011 s.321, sitat s. 327

⁴² RG 2011 s.321, sitat s. 327

illojalitet ved konkret mistanke, selv på utsyr som omfattes av personopplysningsforskriften § 9-2 annet ledd.

Imidlertid vil den skille seg på et punkt; retten bemerker at om arbeidsgiver hadde informert om at opplysningene ville bli brukt til kontrollformål i forkant, ville det antageligvis blitt ansett som et rettmessig tiltak. Kontrolltiltak som har som formål å sammenstille opplysninger fra en datalogg og timelister, for å sjekke hva arbeidstakerne gjør på en datamaskin er ikke tillatt etter personopplysningsforskriften § 9-2 annet ledd. Det er vanskelig å si om en sak som omhandlet bevisavskjæring av datalogger ville fått et annet utfall på bakgrunn av personopplysningsforskriften § 9-2 annet ledd.

Sannsynligvis vil det ikke være et ja/nei svar, men et svar basert på en helhetsvurdering utfra prinsippene som ligger bak tvl. § 22-7 og om tiltaket eller kunne vært rettmessig etter personopplysningsforskriften § 7-11. Svaret vil nok trolig også bero på om beviset avdekker ulovligheter eller ikke. Problematikken med det siste er at arbeidsgiver da fullt ut kan misbruke dette til sin fordel ved å snoke på logger, og hvis de ikke oppdager noe mistenksomt så ties det om snokingen og vise versa. Hvis vi ser videre på hva som skjedde i tingrettsdommen fra juli 2011 finner vi derimot et moment som kan tilsi at generell snoking ikke er å anerkjenne fra domstolene uansett om det avdekkes illojalitet. Under behandlingen av saken i tingretten var et av spørsmålene retten skulle svare på om oppsigelsen var saklig begrunnet jfr. arbeidsmiljøloven § 15-7. Retten viser her blant annet til at det forelå en *konkret mistanke* om at den ansatte tok uforholdsmessige lange pauser i arbeidstiden forut for sammenligningen av loggen og timelistene. Økonomisjefen ved bedriften ante mistanke da den ansatte leverte inn timelister med mye overtid og dette ikke tilsa et normert bruk på den aktuelle søppeltømmingsruta. Totalt viste det seg renovasjonsbilsjåføren hadde hatt 2 timer og 59 minutter pause den aktuelle dagen det ble foretatt en sammenligning av timelistene og logg fra GPS-systemet. Det framkommer også at bilen han kjørte observert parkert i arbeidstiden.⁴³

Selv om tingretten mente at bruken av opplysningene som kontrollformål fremsto som uventet og lite forut beregnelig for den ansatte, uttaler en enstemmig rett at det var rimelig at sjåføren ble sagt opp på bakgrunn av at han hadde tatt uforholdsmessige

⁴³ TNHER 2010-144876-2

lange pauser og krevd overtidsgodtgjørelse for dette. Oppsigelsen var med andre ord saklig.

Utfallet av saken kan ved første øyekast virke urimelig fordi det tilsynelatende kan virke som personopplysningsloven § 11 c) ikke har en funksjon i det hele tatt siden retten tillater arbeidsgiveren å bruke opplysningene til et senere formål som er uforenelig med det opprinnelige. Imidlertid vil det antageligvis virke logisk og rimelig for de fleste av oss at den som «stjeler» fra sin arbeidsgiver blir oppsagt. Og den som sitter på informasjon som beviser et så alvorlig brudd må få lov å fremlegge dette. Når det er sagt vil jeg anta at personopplysningsloven § 11 c) vil komme til sin nytte hvor det ikke avdekkes brudd som er så alvorlig som «tyveri» av lønn. Eksempelvis ville antagelig ikke opplysningene blitt tillatt ført som bevis hvis arbeidsgiveren hadde som mål å avdekke mindre alvorlige brudd som for eksempel feilparkeringer.

Arbeidstakeren krevde også erstatning for brudd på personopplysningsloven jfr. § 49, noe som ble konstatert av retten, men ingen erstatning ble tilkjent.⁴⁴ I sin begrunnelse uttaler retten: «Det er vanskelig å identifisere arbeidstakers skade av ikke-økonomisk art, når utgangspunktet for behandlingen var mistanke om misligheter på arbeidstakers side og kontrollen bekreftet arbeidsgivers mistanke. Etter en helhetsvurdering er lagmannsretten kommet til at krenkelsens art og omfang ikke er av en slik karakter at det i denne saken er rimelig å tilkjenne oppreisning.»⁴⁵

⁴⁴ Erstatningskravet ble anket til lagmannsretten, som forkastet anken, LH-2011-155315.

Erstatningskravet er anket til Høyesterett i skrivende stund, HR-2012-01730-U

⁴⁵ LH-2011-155315, sitat hentet fra s.16

2.2.2 Saklighetskravet, arbeidsmiljøloven § 9-1 (1) og berettiget interesse, personopplysningsloven § 8 f)

Ikke alle formål kan forsvares legitimt ved iverksettelse av kontrolltiltak, formålet må være *saklig begrunnet*. Arbeidsmiljøloven § 9-1 (1) stiller generelle materielle vilkår for innføring av alle typer kontrolltiltak i virksomheten;

«arbeidsgiver kan bare iverksette kontrolltiltak overfor arbeidstaker når tiltaket har saklig grunn i virksomhetens forhold og det ikke innebærer en uforholdsmessig belastning for arbeidstakeren».

I forarbeidene til arbeidsmiljøloven er saklighetskravet forklart slik at «tiltaket skal være begrunnet i forhold som vedrører virksomheten, tiltaket skal være egnet til å fremme formålet, og tiltaket skal ikke settes i verk vilkårlig overfor arbeidstakerne.»⁴⁶

I følge personopplysningsloven § 8 f) er arbeidsgiver berettiget til å behandle personopplysninger når den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen. Saklighetsvurderingen som skal foretas etter arbeidsmiljøloven § 9-1 (1) er sammenfallende med den interesseavveilingen som personopplysningsloven § 8 f) stiller opp, dette bekreftes av forarbeidene til arbeidsmiljøloven;

«I og med at adgangen til å gjennomføre kontrolltiltak som innebærer behandling av personopplysninger antagelig må underkastes mer eller mindre den samme saklighets- og forholdsmessighetsvurderingen, både i forhold til de arbeidsrettslige prinsipper og i forhold til personopplysningsloven, vil selve rettmessigheten av tiltaket neppe stå i en vesentlig annen stilling etter ikrafttredelsen av personopplysningsloven.»⁴⁷

Det stilles krav om at kontrolltiltaket må begrunnes i forhold som vedrører bedriften. Det vil si at tiltaket må være tilpasset den enkelte bedrifts behov for kontroll. Innføring

⁴⁶ NOU 2004:5 Arbeidslivlovsutvalget, s. 413

⁴⁷ NOU 2004:5 Arbeidslivlovsutvalget, s. 424

av sporingsutstyr i biler ved en virksomhet der arbeidet foregår med transportmidler vil generelt være saklig da slikt utstyr kan relateres til slik type arbeid. Det er viktig at saklighetsvurderingen må sees i sammenheng med formålskravet. Selv om det er saklig at en bedrift innfører sporingsutstyr kan for eksempel ikke formålet være at arbeidsgiver har et ønske om å overvåke sine ansatt fordi de ikke stoler på dem.

Tiltaket må være egnet til å fremme formålet, det vil si at om formålet er å ivareta datasikkerheten hos bedriften, vil det et tiltak som brannmurlogg være egnet til å fremme formålet. Imidlertid er det et viktig moment ved saklighetsvurderingen er at tiltaket som iverksettes skal være det best egnede tiltaket. Det vil si at hvis formålet med tiltaket kan oppnås ved en mindre inngripende metode skal dette benyttes. I Rt. 2005 s. 518, Conoco Phillips uttaler Høyesterett; «... bedriften kunne ha valgt en alternativ fremgangsmåte ved at man i forkant hadde tatt opp med tilsynet på generelt grunnlag behovet for en nærmere kontroll av hensyn til det særlige behov for et høyt sikkerhetsnivå ved petroleumsutvinning.»⁴⁸

Datatilsynet hadde i etterkant av selskapets undersøkelser behandlet spørsmål vedrørende undersøkelsene av PC-ene. Høyesterett sikter her til at selskapet kunne forut for undersøkelsene søke Datatilsynet om råd spesifikt for petroleumsvirksomheter hvor det stilles høye krav til sikkerheten. Hvis arbeidsgiver ved for eksempel å utføre samtaler kan oppnå samme resultat som ved innføring av kontrolltiltak, skal samtaler benyttes.

Den kanskje viktigste årsaken til at tiltaket skal være saklig begrunnet er for at arbeidsgiver ikke skal utøve vilkårlig overvåkning og kontroll ovenfor sine ansatte. De ansatte skal føle seg trygge på at overvåkning og kontroll ikke iverksettes for den minste grunn. Overvåkning og kontroll er metoder som ikke må misbrukes og kun anvendes når det er nødvendig jfr. grunnleggende personvernprinsipper som «Retten til privatliv» jfr. Den europeiske menneskerettighets-konvensjon artikkel 8 og FN-konvensjonen om sivile og politiske rettigheter artikkel 17.

⁴⁸ Rt. 2005 s. 518 avsnitt (58)

Domstolene har anerkjent konkret mistanke om illojalitet, brudd på arbeidsavtalen eller arbeidsreglement som saklig grunn(berettiget interesse) for at arbeidsgiver kan iverksette tiltak som innebærer undersøkelse av elektronisk utstyr brukt av den ansatte.⁴⁹ Imidlertid er det ikke alle mistanker som anses som saklig, det stilles krav om at mistanken må være konkret og begrunnet, for at ikke tiltaket skal ansees som vilkårlig. Arbeidsgiver må ha tilstrekkelig dokumentasjon på at slik mistanke foreligger.

I Billakkererdommen (LB-2007-121782) gikk en ansatt med ansvar for lønn og regnskap ved et billakkeringsfirma gikk til søksmål mot sin arbeidsgiver med blant annet krav om erstatning etter personopplysningsloven § 49 for brudd på personopplysningsloven regler. Arbeidsgiverens revisor hadde påpekt overfor arbeidsgiveren at den ansatte ikke hadde trukket seg i lønn for dager hun hadde ferie. Arbeidsgiveren hevdet at hun hadde uberettiget fravær med 30 % av hele 2005 og dermed at hun hadde tatt ut uberettiget lønn. Den ansatte bestred påstandene men kunne ikke bevis at hun faktisk hadde vært på arbeid, fordi hun selv hadde valgt å ikke benytte seg av stemplingsuret. Etter et drøftelsesmøte der den ansattes advokat forlangte dokumentasjon på arbeidsgivers påstander om uberettiget fravær, valgte arbeidsgiver å utføre en kontroll av den ansattes PC. Ved hjelp av dataselskapet IBAS foretok arbeidsgiveren en speilkopi og analyse av tidspunkter for av- og pålogging for å «avklare hvilke dager hun hadde vært på jobb, og hvor lenge hun hadde arbeidet den enkelte dag.» Det ble ikke gjort undersøkelser av e-post, internettlogger eller dokumenter. Arbeidsgiveren hevdet loggen beviste hans påstand om uberettiget fravær hos den ansatte. Arbeidstakeren mente at innhenting av logininformasjon fra PC-en var brudd på personopplysningslovens regler.

Retten påpeker at bedriften hadde et behov for å avklare arbeidstakerens eventuelle pliktbrudd, og at denne avklaringen var nødvendig for det tillitsforhold som er avgjørende i et arbeidsforhold.

⁴⁹Billakkererdommen (LB-2007-121782), Conoco Phillips (Rt. 2005 s. 518), Raufoss (Rt. 2001 s. 1589)

Vedrørende spørsmålet om arbeidsgiver hadde overtrådt personvernsbestemmelsene ved å ta speilkopi av arbeidstakerens PC ser retten først på om arbeidsgiveren hadde saklig grunn jfr. arbeidsmiljøloven § 9-1 (1). Ved saklighetsvurderingen ble det lagt vekt på at arbeidsgiver i forkant av undersøkelsen hadde en «konkret og begrunnet mistanke om at det var utbetalt ikke ubetydelige beløp i lønn for tid arbeidstaker ikke hadde vært til stede.» Det ble videre ansett som saklig da største parten av hennes arbeid ble utført på PC. Det forelå ikke andre metoder å undersøke den ansattes tilstedeværelse på jobb, da hun selv hadde valgt å ikke bruke stemplingsuret. Retten konkluderer med at kravet til saklig grunn for innføring av kontrolltiltak etter arbeidsmiljøloven § 9-1 (1) var oppfylt da de ikke kunne se at dette innebar en uforholdsmessig belastning for den ansatte i forhold til arbeidsgiverens kontrollbehov. Imidlertid ble arbeidsgiveren dømt til å betale den ansatt erstatning som følge av brudd på personopplysningsloven § 8, fordi han ikke hadde et gyldig behandlingsgrunnlag for å bruke opplysningene fra speilkopien. Arbeidstakeren hadde ikke samtykket i bruken. Ved vurdering av lovligheten av behandlingen av informasjonen fra speilkopien viser retten til at utgangspunktet for vurderingen av personopplysningsloven § 8 f) er den samme som i arbeidsmiljøloven § 9-1 (1).

Retten vurderer det slik at speilkopien ikke var et egent tiltak for å oppnå formålet med tiltaket, fordi det ikke alle hennes arbeidsoppgaver var tilknyttet bruk av PC. Videre viste det seg å være betydelige svakheter ved metoden IBAS brukte.⁵⁰

Retten konkluderte med at arbeidsgiveren ikke hadde gyldig et behandlingsgrunnlag for å hente ut loggen fra PC-en og tilkjente den ansatte oppreisning med 5000 NOK for brudd på personopplysningsloven.

Billakkererdommen illustrerer at konkret mistanke om illojalitet kan innfri kravet til saklig grunn til å iverksette kontrolltiltak som innebærer innsyn i logger. Det stilles imidlertid krav til at mistanken må være dokumenterbar jfr. bedriftens regnskap som beviste hennes uberettigete lønn. Dessuten stiller arbeidsmiljøloven § 9-1 (2) krav til at personopplysningslovens regler om behandling av personopplysninger som framkommer av tiltaket må ha et gyldig grunnlag. Hvis ikke samtykke foreligger må arbeidsgiver ha en «berettiget interesse». Interesseavveilingen i personopplysningsloven

⁵⁰ I følge personopplysningsloven § 11 e) må opplysningene være «korrekte og oppdatert».

§ 8 f) baserer seg som tidligere nevnt på de samme momentene som arbeidsmiljølovens § 9-1; Formålskravet (punkt 2.2.1), saklighetskravet (punkt 2.2.2), forholdsmessighetskravet (punkt 2.2.3) og medinnflytelse (2.2.4).

Dommen er fra før personopplysningsforskriften § 9-2 annet ledd trådte i kraft, men utfallet av dommen ville trolig ikke blitt et annet. Dette fordi nyere rettspraksis viser at selv om arbeidsgiver har innhentet bevis i strid med personopplysningsloven vil hensynet til sakens opplysning og betydningen av å oppnå en materielt riktig avgjørelse gå foran dersom «utilbørligheten ved framskaffelsen av beviset ikke var grov, og krenkelsen begrenset» jfr. RG 2011 s 321, GPS kjennelsen⁵¹

Når det gjelder konkret mistanke om straffbare handlinger har Høyesterett i RG 2002 s.162 Butikkmedarbeiderkjennelsen fastslått at mistanke om straffbare forhold i utgangspunktet gir saklig grunn til kontrolltiltak.

2.2.3 Forholdsmessighetskravet, arbeidsmiljøloven § 9-1 (1) og hensynet til ansattes personvern, personopplysningsloven § 8 f)

I tillegg til at kontrolltiltaket skal ha et formål og være saklig begrunnet, stiller arbeidsmiljøloven § 9-1 (1) krav til at *tiltaket ikke skal innebære en uforholdsmessig belastning* for arbeidstakeren. Det skal med andre ord foretas en avveining av virksomhetens behov og hensynet til arbeidstakerne. Denne interesseavveilingen er sammenfallende med avveilingen i personopplysningsloven § 8 f) som åpner for at personopplysninger kan behandles dersom arbeidsgiver kan vareta en berettiget interesse, og *hensynet til den registrertes personvern ikke overstiger denne interessen*.

Forarbeidene til arbeidsmiljøloven sier følgende om forholdsmessighetskravet:

«Vurderingen av om kontrollen vil medføre en uforholdsmessig belastning, vil ellers bero på tiltakets formål (hvor tungtveiende er bedriftens behov), kontrollens art (enkelstående kontroll, vedvarende kontroll, hyppighet osv.), hvordan den praktisk skal gjennomføres, hvilke inngrep i arbeidstakernes personvern det vil være tale om, om

⁵¹ Sitat s. 327 og 328.

sentrale personvern hensyn er ivaretatt gjennom forsvarlige metoder som sikrer klare testresultater, i hvilken grad arbeidsgiver har sikret begrenset tilgang til de data som fremkommer osv. Dersom kontrolltiltaket vil medføre ikke ubetydelig inngrep i rettsgoder som personlig integritet, verdighet, privatlivets fred, legemets ukrenkelighet eller lignende, vil vilkårene for å gjennomføre kontrollen i utgangspunktet bare unntaksvis være oppfylt. Motsatt skal det mye til for at mer tradisjonelle kontrolltiltak i arbeidslivet som for eksempel tidsregistrering, adgangskontroll, produksjons- og resultatkontroll, kontroll i forbindelse med konkret mistanke om straffbare og andre mislige forhold i arbeidsforholdet osv., vil bli ansett som uforholdsmessig.»⁵²

Eksempelvis vil et tiltak der bedriften ønsker å overvåke ansattes nettaktivitet for å få dem til å bli mere effektive når de jobber med datamaskiner, vil ikke kunne ansees som forholdsmessig, fordi mindre inngripende tiltak kan anvendes. I stedet for kan tiltak som for eksempel å stenge for enkelte nettsider, klare arbeidsinstruksjoner og arbeidsreglement som forbyr privat bruk av internett anvendes i stedet.

Problematikken i forhold til tiltak der elektronisk utstyr blir anvendt er ofte tilknyttet de tilfeller der den ansatte benytter seg av arbeidsgivers smarttelefoner, PC eller Mac til private formål og privat kommunikasjon via internett. Opplysninger som kan karakteriseres som private vil lagres en brannmurlogg. Opplysninger om personlige forhold og opplysninger arbeidsgiver ellers ikke har lov å stille ved ansettelse jfr. arbeidsmiljøloven § 13-4 burde heller ikke være tilgjengelige ved innføring av kontrolltiltak. Ved for eksempel mistanke om brudd på arbeidsreglement der besøk av spesifikke internettsider ikke er tillatt, skal arbeidsgiver sørge for at opplysninger nevnt over ikke blir gjort tilgjengelige. For eksempel vil det være krenkende for en ansatt om arbeidsgiver får informasjon om en ansatts seksuelle legning eller rusproblemer fordi den ansatte har besøkt nettsider med innhold som kan relateres til dette.

Ergo vil et tiltak som har som formål og effektivisere arbeidet på PC ansees uforholdsmessig dersom om arbeidsgiver får tilgang til slik privat informasjon.

⁵² Ot.prop nr. 49 (2004-2005) Om lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven), kapittel 12 om kontroll og overvåking i arbeidslivet, s. 145

I forarbeidene nevnt over nevnes det at forsvarlige metoder for å sikre klare testresultater er et moment ved forholdsmessighetsvurderingen. I Billakkererdommen, LB-2007-121782, ble den ansatte tilkjent erstatning for brudd på personopplysningsloven fordi logginformasjonen som arbeidsgiver innhentet og la fram som bevis i saken «ikke var egnet til å gi noe helhetlig bilde av As tilstedeværelse på jobb.» Denne problematikken vil alltid være sentral ved tiltak som omhandler elektronisk utstyr. Informasjonen alene kan ikke alltid være til å stole på.

Forarbeidene nevner eksempler på tradisjonelle kontrolltiltak som tidsregistrering og adgangskontroll og at det skal mye til for at disse vil bli ansett som uforholdsmessige.

2.2.4 Informasjon og drøftelse, arbeidsmiljøloven § 9-2

Både arbeidsmiljøloven og personopplysningsloven legger opp til at den ansatte skal ha en viss grad av innflytelse i forkant av iverksettelsen av et eventuelt kontrolltiltak. Arbeidsmiljøloven § 9-2 stiller krav til at «Arbeidsgiver plikter så tidlig som mulig å drøfte behov, utforming, gjennomføring og vesentlig endring av kontrolltiltak i virksomheten med arbeidstakernes tillitsvalgte. (2) Før tiltaket iverksettes, skal arbeidsgiver gi de berørte arbeidstakerne informasjon om:

- a) formålet med kontrolltiltaket,
- b) praktiske konsekvenser av kontrolltiltaket, herunder hvordan kontrolltiltaket vil bli gjennomført,
- c) kontrolltiltakets antatte varighet.

(3) Arbeidsgiver skal sammen med arbeidstakernes tillitsvalgte jevnlig evaluere behovet for de kontrolltiltak som iverksettes.»

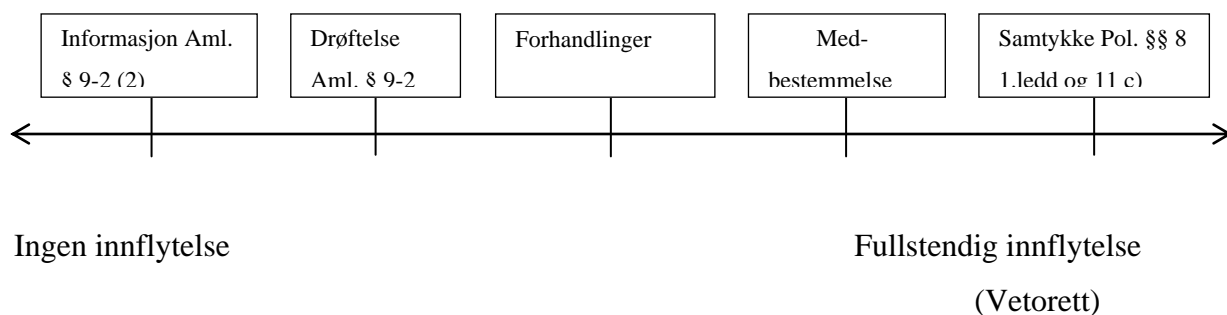
En lignende bestemmelse finner vi i personopplysningsloven § 20 «En behandlingsansvarlig som samler inn personopplysninger fra andre enn den registrerte selv, skal av eget tiltak informere den registrerte om hvilke opplysninger som samles inn og gi informasjon som nevnt i § 19 første ledd så snart opplysningene er innhentet. Dersom formålet med innsamling av opplysningene er å gi dem videre til andre, kan den behandlingsansvarlige vente med å varsle den registrerte til utleveringen skjer.»

Både arbeidsmiljølovens og personopplysningslovens regler om drøftelse og informasjon er også med på å skape forutberegnelighet for de ansatte.

Imidlertid er det slik at i arbeidsforhold bestemmer arbeidsmiljøloven at drøftelse med de tillitsvalgte er den eneste innflytelse de ansatte har på iverksettelse av kontrolltiltak.⁵³ De ansatte har med andre ord ikke krav på å bli tatt hensyn til når det gjelder innflytelse. Det kan stilles spørsmål om styringsretten her kan føre til at tillitten mellom arbeidsgiver og arbeidstaker kan bli satt på prøve om arbeidsgiver fordi de ansatte ikke direkte kan komme med innvendinger.

Skalaen under illustrerer graden av innflytelse arbeidstaker har på iverksettelse av kontrolltiltak. Ved informasjon har de ansatte ingen innflytelse på utformingen av tiltaket. Der tiltaket drøftes med de tillitsvalgte har de ansatte en viss mulighet til å påvirke via de tillitsvalgte som skal drøfte tiltaket med arbeidsgiver.

Figur 2)



Arbeidsmiljøloven § 9-2 har imidlertid i rettspraksis blitt omtalt som en ordensregel, det vil si at om den ikke er fulgt, vil det ikke dermed være et ulovlig iverksatt kontrolltiltak.⁵⁴ Som nevnt over vil det uansett på grunn av tillitsforholdet være en

⁵³ Motsetningsvis må samtykke som hovedregel anvendes i tilfeller der det samles inn og behandles personopplysninger utenfor arbeidsforhold jfr. personopplysningsloven § 8 første ledd.

⁵⁴ Tine kjennelsen, RG 2007 s. 855

fordel at arbeidsmiljøloven § 9-2 følges, selv om arbeidstaker uansett skal opptre lojalt og irettesette seg overfor arbeidsgivers styringsrett.⁵⁵ Derimot er styringsretten ikke ubegrenset og prinsippene i arbeidsmiljøloven, personopplysningsloven og personopplysningsforskriften setter grenser for hvor langt arbeidsgivers styringsrett går når det gjelder iverksettelse av kontrolltiltak.

Det kan oppfattes slik at det stilles mindre krav til at personopplysningsloven § 20 er oppfylt på grunn av at regelen bruker ordet *informasjon*, som kan tyde på en ensidig meddelelse, mens arbeidsmiljøloven stiller krav til drøftelse med de tillitsvalgte, noe som åpner for diskusjon og større grad av innflytelse. Personopplysningsloven § 20 gjelder ikke for behandling av personopplysninger, men kun ved innsamling. Ved behandling må som sagt § 8 jfr. § 11 være oppfylt. I følge rettspraksis kan det tyde på at det må avgjøres konkret i hvert enkelt tilfelle om kravet til medbestemmelse og drøfting etter arbeidsmiljøloven § 9-2 er nødvendig, eller om informasjonsplikten etter personopplysningsloven § 20 er tilfredsstillende for om tiltaket ansees som saklig.⁵⁶ I GPS saken uttaler retten følgende om arbeidsmiljøloven § 9-2: «Bestemmelsen regnes som en ordensforskrift. Dette innebærer at brudd mot drøftelses- eller informasjonsplikten ikke i seg selv vil innebære at tiltaket er ulovlig. Manglende informasjon eller drøfting vil imidlertid være et moment i den alminnelige saklighetsvurderingen og vil etter omstendigheten kunne medføre at tiltaket blir ansett for å være ulovmessig, se Ot.prp.nr 49 (2004-2005) side 314.»⁵⁷

⁵⁵ En kan her stille spørsmål om de ansattes krav på personvern blir innskrenket på bakgrunn av arbeidsgivers styringsrett. Temaet ble belyst i en publikasjon som omhandlet avgrensning av arbeidsgivers styringsrett på grunn av arbeidstakers personvern. Publikasjonen tar for seg en gjennomgang av rettspraksis de siste ti årene hvor arbeidsgiver har innført kontrolltiltak som registrerer personopplysninger. Borchgrevink, *Om avgrensning av arbeidsgivers styringsrett på grunn av arbeidstakers personvern – En gjennomgang av norsk rettspraksis*, Oslo, 2011.

⁵⁶ RG 2011 s. 321

⁵⁷ LH-2011-155315, sitat s. 14

3 Avslutning

Formålet med reglene om arbeidsgivers adgang til kontroll av elektronisk utstyr vil først og fremst være å gi retningslinjer til brukerne, arbeidsgiverne og arbeidstakerne.

Retningslinjene vil gi føringer og begrensninger for arbeidsgivers styringsrett og mens de vil ivareta arbeidstakernes personvern.

Andre viktige hensyn bak reglene er å hindre vilkårlige innsyn og begrense at de ansatte føler seg overvåket av sin arbeidsgiver. Hvordan reglene fungerer i praksis vil imidlertid bero på kunnskapen om reglene. At arbeidsgiver har kunnskap og forståelse av reglene må være det grunnleggende for at reglene skal kunne overholdes. Problemet er trolig at mange arbeidsgivere ikke har denne kunnskapen, og ei heller har muligheter til å tilegne seg den fordi regelsettet er såpass uoversiktlig og kompleks. For eksempel GPS saken viser at arbeidsgiveren trolig ville fått medhold i at kontrolltiltaket (sammenstillingen av GPS logg og timelister) var rettmessig om reglene var blitt fulgt.⁵⁸

Et annet moment som kan være med på å bekrefte at hverken arbeidsgiver eller arbeidstaker har kunnskap om reglene, er den lille andelen saker som kommer opp for domstolene. Hvis man ikke vet at det har skjedd et lovbrudd vil man ikke gå videre med saken. Derimot vil saker som omhandler temaet trolig ikke kunne opp for domstolene i særlig grad uansett. Begrunnelsen er det spesielle forhold mellom arbeidsgiver og arbeidstaker, arbeidstaker står nærmest i et avhengighetsforhold til sin arbeidsgiver.

Hvis for eksempel en arbeidsgiver opplyser at han vil følge med på alt som blir gjort på arbeidstakernes datamaskiner, vil nok mange ansatte være påpasselig med kun å utføre arbeidsrelaterte oppgaver på datamaskinen. Dette uavhengig om de har kunnskap om personopplysningsforskriften § 9-2 annet ledd eller ikke. De ansatte som eventuelt har kunnskap om personopplysningsforskriften § 9-2 annet ledd og ikke godtar arbeidsgiverens overvåkning vil trolig ikke gå så langt som til domstolene. Årsaken er nettopp det spesielle forhold mellom partene, som i store deler er basert på tillitt. Dette tillitsforholdet vil allerede være brutt om arbeidsgiver bryter reglene. Selvfølgelig vil tillitsforholdets framtid bero på om arbeidsgiver var uvitende om at

⁵⁸ RG 2011 s. 321

personopplysningsforskriften § 9-2 annet ledd eksisterte og forbød overvåkning eller om arbeidsgiver bevisst brøt reglene.

Selv om ikke GPS saken gjaldt personopplysningsforskriften § 9-2 annet ledd illustrerer den omfanget av både tid og ressurser som går med i en tvist av slik karakter. Saken startet allerede i mai 2010 hvor arbeidsgiveren innkalte renovasjonsbilsjåføren til et møte for å utale seg om forholdet og saken har vært behandlet flere ganger i rettsapparatet, i tillegg har Datatilsynet og Personvernemnda uttalt seg om saken. Erstatningskravet er i skrivende stund anket til Høyesterett.

Både Datatilsynet og Personvernemnda konkluderte med at sammenstillingen av GPS-loggen og timelistene stred mot personopplysningsloven § 11 c) og at det ikke forelå berettiget interesse som overgikk den ansattes personvern jfr. personopplysningsloven f).⁵⁹ I den siste dommen i GPS-saken har Datatilsynet i medhold av tvl. § 15-8 fremmet et skriftlig innlegg hvor de uttaler: «Datatilsynet har fått mange henvendelser som gir uttrykk for usikkerhet med hensyn til hvilke konsekvenser brudd på personopplysningsloven får. I dette tilfellet kom Hålogaland lagmannsrett til at Avfallservice AS kunne bruke de ulovlig sammenstilte data som bevis i oppsigelsessaken. Vernet av arbeidstaker fremstår som illusorisk. Datatilsynet finner det uheldig at arbeidsgiver som bryter regelverket på sett og vis kommer gunstigere ut av enkelte situasjoner enn pliktoppfyllede virksomheter.»⁶⁰ Det som kan virke merkelig i denne sammenheng er at Datatilsynet ikke benyttet seg av muligheten til bøtelegge arbeidsgiveren enda de mente at det forelå brudd. Trolig vil Datatilsynet ilegge bøter i framtiden ved lignende brudd for å hindre at arbeidsgivere bevisst misbruker reglene, når GPS saken foreløpig når arbeidsgiveren går «fri» ved å misbruke reglene og arbeidstakeren ikke får erstatning. For det kan virke som om Datatilsynet hadde trudd at domstolene ville enten ikke tillat beviset først eller at erstatning ville bli gitt.

Uansett kan jeg konkludere med at sammensetningen av reglene i arbeidsmiljøloven, tvisteloven, personopplysningsloven og personopplysningsforskriften bidrar ikke til at reglene er lett tilgjengelige og enkle å forstå for brukerne. Denne problemstillingen ble

⁵⁹ PVN-2011-04 Avfallservice

⁶⁰ LH-2011-155315 s. 10

også påpekt av Personvernkommisjonen i NOU 2009:1; Kommisjonen er kritisk til plasseringen av regelverket og mener av hensynet til notoritet og tilgjengelighet at reglene burde forankres i arbeidsrettens regelverk. Etter kommisjonens oppfatning vil et hensiktsmessig og balansert regelverk være med på å sikre at reglene skal kunne etterleves av partene i praksis.⁶¹

En kan trygt si at man må enten være jurist eller ha veldig god tid til å sette seg inn i regelverket hvis man skal få full oversikt over temaet.

Slik jeg ser det vil et samlet regelverk skape trygghet i arbeidslivet i henhold til kontroll og overvåkning, jo klarere regler, desto tryggere vil partene være. Klare arbeidsinstrukser og arbeidsreglementer basert på reglene vil kunne være med på skape denne forutberegneligheten, spesielt i forhold til ansattes disposisjon av elektroniske hjelpemidler som registrerer personopplysninger.

Imidlertid må en ikke glemme at forholdet mellom arbeidsgiver og arbeidstaker må som nevnt baseres på tillitt mellom partene. I arbeidsforhold der arbeidsgiveren ikke fysisk ser at de ansatte jobber (som ved arbeid via datamaskin) vil tillitt være avgjørende. En annen viktig ting er at arbeidsgivere bør forsøke å begrense bruken av overvåkning. Arbeidsgiver må ikke kun ta i bruk teknologien for å føre kontroll med sine ansatte, den personlige oppfølgingen og kommunikasjonen må være til stede, det slik tillitten opprettholdes. Arbeidsmiljøloven § 4-2 om krav til et fullt forsvarlig arbeidsmiljø vil være med på å ivareta det overfor nevnte.

4 Litteraturliste

4.1 Litteratur:

Eckhoff, Torstein *Rettskildelære*. 5. utg. ved Jan Helgesen. Oslo, 2001.

Jakhelln, Henning *Oversikt over arbeidsretten*. 4.utg. Oslo, 2007.

⁶¹ NOU 2009: 1, s. 156-158.

Borchgrevink, Mette *Om avgrensning av arbeidsgivers styringsrett på grunn av arbeidstakers personvern –En gjennomgang av norsk rettspraksis*. Oslo, 2011.

4.2 Lov- og forarbeidsregister

Lover:

- 1814 Kongeriget Norges Grundlov, given i Rigsforsamlingen paa Eidsvold den 17de Mai 1814 (Grunnloven) av 17. mai 1814.
- 1977 Lov om arbeidervern og arbeidsmiljø m.v. av 4. februar 1977 nr. 4. (Opphevet)
- 1978 Lov om personregistre m.m av 9. juni 1978 nr 48. (Opphevet)
- 1999 Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven) av 21. mai 1999 nr. 30.
- 2000 Lov om behandling av personopplysninger (personopplysningsloven) av 14. april 2000 nr 31.
- 2005 Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven) av 17. juni 2005 nr 62.
- 2005 Lov om mekling og rettergang i sivile tvister (tvisteloven) av 17. juni 2005 nr. 90.

Forarbeider:

- NOU 1997:19 Et bedre personvern.
- NOU 2004:5 Arbeidslivslovutvalget.
- NOU 2009:1 Individ og integritet. Personvern i det digitale samfunnet.
- Ot.prop nr. 49 (2004-2005) Om lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven), kapittel 12 om kontroll og overvåking i arbeidslivet.

Høringsnotater:

(FAD) Forslag til regler om arbeidsgivers adgang til ansattes e-post mv.
-Endring av personopplysningsloven § 3 og § 46, Nytt kapittel i personopplysningsforskriften og ny bestemmelse i arbeidsmiljøloven av 17. oktober 2006.

Forskrifter:

(FAD) Forskrift om behandling av personopplysninger
(personopplysningsforskriften) av 15. desember 2000 nr. 1265.

(FAD) Forskrift om endring i forskrift om personopplysninger
(personopplysningsforskriften) av 29. januar 2009 nr. 84.

Konvensjoner:

EMK Den europeiske menneskerettighetskonvensjonen, Roma 1950.

Direktiver:

EP/Rdir 95/46EP Europa-parlamentets og Rådets direktiv 95/46EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om den fri utveksling av slike opplysninger (Personverndirektivet)

4.3 Rettspraksis

Menneskerettighetsdomstolen:

Copland vs. United Kingdom The European Court of Human Rights,
Strasbourg, 3. April 2007

Norsk rettstidene:

Rt. 1991 s. 616

Rt. 2000 s. 1602

Rt. 2001 s. 1589

Rt. 2005 s. 518

Rettsens gang:

RG 2004 s. 347 (Borgarting)

RG 2007 s. 855 (Frostating)

RG 2011 s. 321 (Hålogaland)

Upubliserte dommer:

LB-2007-121782

TNHER-2010-144876-2

LH-2011-155315

4.4 Nettdokumenter

Rapporter:

Bråten, Mona. *Fafo rapport 2010: 22 Kontroll og overvåking i arbeidslivet*. Oslo 2010.

<http://www.fafo.no/pub/rapp/20166/20166.pdf>

Personvernemndas avgjørelser:

Personvernemnda: *Klage på Datatilsynets vedtak. PVN-2011-04 Avfallservice*.

http://www.personvernemnda.no/vedtak/2011_04.htm

Databaser:

www.lovdatabasen.no

www.rettssystemet.no

Datatilsynets merknader:

Datatilsynets merknader til personopplysningsforskriften kapittel 9.

http://www.datatilsynet.no/Global/05_regelverk/epostforskriften_merknader.pdf

Datatilsynets veiledere:

GPS og sporing i yrkesbiler, 2010

http://www.datatilsynet.no/templates/article__3578.aspx

Bruk av sporingsteknologi i virksomheters kjøretøy, 2012

http://www.datatilsynet.no/Global/04_veiledere/Veileder_GPS_sporing_jan2012_3.pdf

Tilgangskontroll i arbeidslivet, 2012

<http://www.datatilsynet.no/verktoy-skjema/Publikasjoner/Veiledere/Tilgangskontroll/#om>

5 Lister over tabeller og figurer m v

Figur 1) av Kari Huru, Oslo 2012

Figur 2) av Kari Huru, Oslo 2012