

**Rapport
fra Datatilsynet
om fjernsynsovervåking
13. desember 2005**

Notat fra Datatilsynet i forbindelse med forestående revisjon av personopplysningslovens bestemmelser om fjernsynsovervåking

1	Innledning	1
2	Gjeldende rett	4
2.1	Behandlingsgrunnlag	4
2.2	Merking	5
2.3	Kamera med lydopptak	5
2.4	Kontrollinstans og sanksjonsmuligheter	5
3	Internasjonal regulering	6
3.1	Artikkel 29-gruppen	7
3.2	Artikkel 29-gruppens uttalelse om kameraovervåking	7
4	Vurdering av dagens situasjon i Norge	23
4.1	Utdrag av noen av Datatilsynet avgjørelser:	23
4.2	Noen problemer ved gjeldende regulering	25
4.2.1	Skjønnsmessige vurderinger	25
4.2.2	Behandlingsansvar	26
5	Forslag til endringer	26
5.1	Teknisk utvikling	26
5.2	Fra fjernsynsovervåking til kameraovervåking	27
5.3	Behandlingsgrunnlag	27
5.4	Proporsjonalitet	28
5.5	Sondre mellom opptak og monitorering	28
5.6	Skillet mellom analoge og digitale system	28
5.7	Melde- og konsesjonsplikt	29
5.8	Sikring av billedopptak	30
5.9	Web-kamera	31
5.10	Forskjell mellom offentlig og privat overvåking – og overvåkingssentraler ...	31
5.11	Biometri/gjenkjenningsteknologi/digital bearbeiding	32
5.12	Lydopptak	33
5.13	Informasjon/varslings	33
5.14	Særlig bestemmelse om innsynsrett og utlevering	34
5.15	Personvernforenning muligheter i digitale systemer	34
5.16	Andre overvåkingsformer	35
5.17	Reaksjoner fra tilsynsmyndigheten	35
5.18	Andre aktører	35
5.19	Andre tendenser i utviklingen	36
	Vedlegg: 1	37

1 Innledning

London skal være den byen i Europa med størst tetthet av overvåkingskameraer. I følge uformelle undersøkelser ligger Oslo også høyt på listen. I Storbritannia oppgis antallet kameraer til 2,5 millioner; en londonbeboer fotograferes ca 300 ganger om dagen. I Berlin må butikker ha overvåkingskameraer fordi forsikringsselskapene setter det som vilkår for å tegne forsikring.

Kameraovervåking kan anvendes til en rekke forskjellige formål. De viktigste anvendelsesområdene¹, kan imidlertid inndeles i noen hovedgrupper. Beskyttelse av fysiske

¹ Ref. Artikkel 29-gruppens uttalelse om videoovervåking.
Der anvendes forskjelligt videoovervågningsudstyr:

personer og eiendom står sentralt. I tillegg kommer beskyttelse av offentlige interesser, avsløring, forebygging og kontroll av lovovertridelser samt bevisførsel.

Et paradoks er at kameraovervåking ikke ser ut til å redusere kriminalitet i særlig grad ifølge en forskergruppe fra Universitetet i Leicester. Gruppen har sett på 14 større kameraovervåkingsprosjekter på oppdrag fra det britiske innenriksdepartementet. Storbritannia er Europas tettest kameraovervåkede land, og et land der det har blitt lagt mye politiske prestisje i bruken av denne typen overvåking. Det offentlige, ved sitt program *CCTV Initiatives* har brukt over to milliarder kroner til finansiell støtte til i underkant av 700 kameraanlegg. Mellom 1994 og 1997 brukte Home Office hele 78 % av midlene som skulle bidra til forebygging av kriminalitet til støtte til kameraovervåkingstiltak.

Forskergruppen fra Universitetet i Leicester studerte hvordan kameraovervåking påvirket kriminalitetsutviklingen i 14 større kameraovervåkingssystemer. Alle systemene hadde to hovedformål – å redusere kriminaliteten, samt å gjøre folk mindre redde.

Forskerne fant redusert kriminalitet i kun to av de aktuelle områdene som ble vurdert. Bare i ett av disse tilfellene, et overvåkingssystem for parkeringsplasser, fant forskerne at kameraovervåkingen kunne sies å medvirke til redusert kriminalitet. Folk i områder med tett kameraovervåking følte seg heller ikke tryggere med kameraanleggene. Publikum uttrykte likevel ikke noe ønske om at kameraene skulle tas bort, og var generelt lite bekymret for innhogg i sin frihet.

Funnene antyder at det kan være en sammenheng mellom størrelsen på det overvåkede området og effekt – at kameraovervåking kanskje reduserer kriminaliteten noe i små innelukkede områder. De antyder også en sammenheng mellom kameratetthet og effekt, samt at overvåkingen virket bedre på vinningskriminalitet enn på annen type kriminalitet. Funnene på disse områdene er imidlertid ikke entydige.

-
- a) i og omkring offentlige og/eller offentlig tilgjengelige bygninger, f.eks. museer, kultsteder eller monumenter, med henblik på å forhindre krænkelser og/eller vandalisme, markedsføring og/eller udarbejdelse af kundeprofiler, personer, eller overvågning af patienter på intensivafdelinger og/eller i afdelinger med alvorligt syge patienter og/eller patienter, der er sat i karantæne,
 - b) på stadioner og idrætsanlæg, særlig i forbindelse med visse begivenheder,
 - c) inden for transportsektoren og i forbindelse med de trafikale forhold med henblik på at regulere trafikken på lande- og motorveje, konstatere overskridelser af hastighedsbegrænsningerne og/eller overtrædelser af færdselsregler i byzoner, eller kontrollere adgangsforholdene til undergrundsbaner, overvåge benzintanke og kabinen i taxaer,
 - d) for at forebygge og/eller afsløre ulovlig adfærd omkring skoler, herunder i forbindelse med opfordring til utugt af de unge,
 - e) på behandlingssteder under operationer og/eller med henblik på f.eks. fjernbehandling
 - f) i lufthavne, om bord på skibe og i grænseområder med henblik på at overvåge menneskesmugling og fremme eftersøgningen af mindreårige og andre savnede
 - g) af privatdetektiver,
 - h) i og omkring supermarkeder og forretninger, særlig i forbindelse med handel med luksusvarer med henblik på bevisførelse i tilfælde af tyveri samt med henblik på
 - i) i og omkring private boliger med henblik på sikkerhed og bevisførelse i tilfælde af tyveri,
 - j) til journalistiske eller reklamemæssige anvendelser, der finder sted online ved hjælp af enten webkameraer eller onlinekameraer, der anvendes til fremme af turismen og reklameformål, herunder i forbindelse med badestrande og dansesteder, ved at filme kunder og besøgende med regelmæssige mellemrum og uden varsel.

Forskergruppen problematiserer kriminalitetsreduksjon og reduksjon av frykt som målestokk for effekten av kameraovervåking. De peker på at flere faktorer antakelig bør tas med i vurderingen, som for eksempel oppdagelses- og oppklaringsmuligheter for kriminalitet.

Forskerne mener at overvåkerne i utvalget har hatt lite realistiske oppfatninger om hvilke resultater man kan vente seg med kameraovervåking. Kameraovervåking har etter forskernes mening, vært fremstilt som et vidundermiddel mot kriminalitet, og kameraene er til dels hengt opp uten at man har tenkt på om tiltaket er riktig middel for å løse problemet. Gruppen konkluderer videre med at for at kameraovervåking skal ha effekt, må man erkjenne at å forebygge eller å redusere kriminalitet ikke er enkelt, og at mangelfullt vurderte tiltak sjelden virker uansett hvor mange penger man bruker på dem.

Mens kameraovervåking under visse omstendigheter synes å være vel begrunnet, er det også tilfeller hvor overvåkingen uten videre anvendes til beskyttelsesformål, uten at de nødvendige garantier eller foranstaltninger treffes.

Det er også et psykologisk aspekt forbundet med kameraovervåking, idet offentligheten – med rette eller urette - betrakter det som et "uvurderlig verktøy", fordi det har vist seg å være av verdi i etterforskningen av enkelte kriminelle handlinger.

Forsker Inger-Anne Ravlum ved Transportøkonomisk institutt har publisert rapporten "Setter vår lit til Storebror ... og alle småbrødrene med?". Mer enn 90% av befolkningen føler seg i følge rapporten stort sett trygge der de ferdes til daglig. Nesten fire av fem oppgir at de føler seg tryggere der det er kameraovervåking. De som i utgangspunktet ikke føler seg trygge, føler seg tryggere i mindre grad enn de som oppgir at de stort sett føler trygghet der de ferdes til vanlig. Det er også blant de utrygge man finner flest motforestillinger mot kameraovervåking. Færre av dem mener at folk med "rent mel i posen" ikke har noe å frykte ved kameraovervåking, og færre av dem synes det er greit med kamera på offentlige steder.

Likevel er et stort flertall av de spurte enige i at kameraovervåking er overveiende positivt i de fleste sammenhenger. Kun på spørsmål om kameraovervåking på egen arbeidsplass, i barer og restauranter og ved vaskene på offentlige toaletter er det et flertall som mener overvåkingen er overveiende negativ.

Datatilsynet og Statistisk Sentralbyrå foretok en undersøkelse av holdninger til personvern også i 1997. Tallene er ikke uten videre sammenliknbare, men kan antyde at stadig flere nordmenn anser kameraovervåking som greit i de fleste tilfeller.

Det er viktig at overdreven bruk av billedopptakssystemer på offentlige og private områder ikke medfører en ubegrunnet begrensning av borgernes rettigheter og grunnleggende friheter. Dette fordi slike systemer fort vil kunne benyttes til uforholdsmessig omfattende datainnsamling, som i stort omfang kan gjøre enkeltmennesker identifiserbare i en rekke offentlige og private områder.

Enkelte tendenser i utviklingen innen kameraovervåkingsteknikk kan med fordel begrenses. Spesielt for å unngå videre utvikling av softwareapplikasjoner, som bygger på både ansiktsgjenkjenning, undersøkelse og mulighetene til å forutsi filmede personers adferd.

Tendensene i utviklingen vil kunne føre til stor grad av dynamisk forebyggende overvåking, i motsetning til alminnelig statisk overvåking, som hovedsaklig har til formål å dokumentere

spesifikke begivenheter og de angjeldende aktører. Denne nye form for overvåking (dynamisk forebyggende) bygger på den automatiske opptakelse av personers ansiktstrekk samt deres "avvikende" adferd i assosiasjon med en eventuell automatisk alarm og varsling, som kan medføre diskriminering. Forskningsresultater har vist at kameraoperatørene faktisk diskriminerer på bakgrunn av utseende. Folk med "sjuskete" fremtoning og unge menn med minoritetsutseende blir oftere overvåket enn andre. Faren for sosial eksklusjon på bakgrunn av utseende er derfor tilstede. Se NTNU forskerne Sætnan, Dahl og Lomells undersøkelse fra Jernbanetorget i Oslo samt en artikkel av Heidi Lomell. Prosjektet er en del av Urbaneye-undersøkelsen (se urbaneye.net), et stort samarbeidsprosjekt mellom forskere i flere land.

2 Gjeldende rett

Fjernsynsovervåking er regulert i personopplysningsloven kapittel VII og personopplysningsforskriften kapittel 8. Med fjernsynsovervåking menes vedvarende eller regelmessig gjentatt personovervåking ved hjelp av *"fjernbetjent eller automatisk virkende fjernsynskamera, fotografiapparat eller lignende apparat"*, jf. personopplysningsloven § 36.

Reglene i lovens §§ 38-41 gjelder for all fjernsynsovervåking. Det samme gjelder §§ 8, 9, 11, 31 og 32. Kravene om tilfredsstillende informasjonssikkerhet og internkontroll, jf. §§ 13 og 14, kommer således ikke til anvendelse med mindre bildeopptak lagres på en slik måte at det er mulig å finne igjen opplysninger om en bestemt person. Fjernsynsovervåking som har som formål å avdekke opplysninger om at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, jf. § 2 nr. 8 bokstav b, er tillatt, selv om vilkårene i § 9 første ledd ikke er oppfylt. Det er heller ikke konsesjonsplikt for den type fjernsynsovervåking, jf. lovens § 37.

Når bildeopptak fra fjernsynsovervåking lagres på en måte som gjør det mulig å finne igjen opplysninger om en bestemt person, jf. § 3 første ledd, gjelder også lovens øvrige bestemmelser. Bestemmelsen er primært aktuell ved digital lagring av bildeopptak og bruk av særlige gjenkjennelsessystemer.

Det er et grunnkrav til fjernsynsovervåking av sted hvor en begrenset krets av personer ferdes jevnlig, at det ut fra virksomheten er et særskilt behov for overvåkingen, jf. personopplysningsloven § 38.

Personopplysninger som er innsamlet ved fjernsynsovervåking, kan bare utleveres til andre enn den behandlingsansvarlige dersom den som er avbildet samtykker, eller utleveringsadgangen følger av lov. Bildeopptak kan likevel utleveres til politiet ved etterforskning av straffbare handlinger eller ulykker hvis ikke lovbestemt taushetsplikt er til hinder for dette, jf. § 39.

2.1 Behandlingsgrunnlag

Et grunnleggende krav etter loven, er at den behandlingsansvarlige (jf. personopplysningslovens § 2 nr. 4), kan vise til et gyldig behandlingsgrunnlag, jf. personopplysningslovens § 11, bokstav a. Datatilsynet har gjennom praksis lagt til grunn at det mest relevante behandlingsgrunnlaget er en interesseavveining etter personopplysningslovens § 8, bokstav f. Det er etter lovens system, i første omgang den behandlingsansvarlige selv som må foreta en vurdering av hvorvidt tiltaket kan iverksettes med hjemmel i § 8, bokstav f. Det kan imidlertid påpekes at sikring mot tyveri eller hærverk, i praksis ofte vil oppfylle vilkåret om *"berettiget interesse"* etter bestemmelsen, forutsatt at

virksomheten kan dokumentere, eller vise til overhengende fare for et problem av en viss størrelse. Det vises i denne sammenheng videre til personopplysningslovens § 38, som fastsetter at det må foreligge et ”*særskilt behov*” for overvåking av områder hvor en begrenset krets av personer ferdes jevnlig (for eksempel arbeidsplass). Forutsetningen er imidlertid at tiltaket ellers er lovlig iverksatt.

Personopplysningslovens § 11, bokstav b, fastsetter at den behandlingsansvarlige skal sikre at personopplysninger bare skal nyttes til formål som er saklig begrunnet i den behandlingsansvarliges virksomhet. Formålet med behandlingen av personopplysninger må ha nær og naturlig sammenheng med den aktuelle virksomheten som sådan. Er formålet bevisinnhenting til bruk i straffesaker, foretatt av virksomheten selv, kan dette vanskelig oppfylle kravet til saklig formål. Dette begrunnes med at slik bevisinnhenting er en oppgave tillagt politiet. Overvåking som er iverksatt for å forebygge tyverier ved en arbeidsplass, kan derimot være saklig begrunnet i virksomheten etter en konkret vurdering.

2.2 Merking

Ved fjernsynsovervåking på offentlig sted eller sted hvor en begrenset krets av personer ferdes jevnlig, skal det ved skilting eller på annen måte gjøres tydelig oppmerksom på at stedet blir overvåket og hvem som er behandlingsansvarlig, jf. § 40.

Personopplysningslovens § 40 setter et absolutt forbud mot skjult overvåking. Det bemerkes imidlertid at lovens § 40 likestiller varsling ved skilting og varsling ”*på annen måte*”. Muntlig eller skriftlig informasjon om overvåkingen kan etter forarbeidene til straffelovens § 390, bokstav b, således aksepteres. Straffelovens bestemmelse i § 390, bokstav b, ble videreført i personopplysningsloven. Det beskyttelsesverdige formålet med overvåkingen (sikring mot tyveri med preventiv hensikt) taler for tydelig varsling om tiltaket. Dette kommer til uttrykk ved at overvåking som hovedregel bare skal foretas i preventiv hensikt, og at det er politiet som er tillagt oppgaven med å innhente bevis til bruk i straffesaker.

2.3 Kamera med lydopptak

En tilleggsfunksjon ved mange overvåkingsløsninger som leveres i dag er lydopptak. I den grad muligheten faktisk benyttes, vil det kunne rammes av forbud mot romavlytting i straffeloven 145a.

Romavlytting foregår vanligvis ved at lytteutstyr plasseres i et rom eller sted hvor det gis mulighet for å avlytte samtaler eller annen registrerbar virksomhet uten de berørtes kunnskap. Slik avlytting har inntil ganske nylig vært forbudt i Norge. I kjølvannet av terroranslagene i USA i 2001 er det de to siste årene gitt en begrenset adgang for politiet, med domstolenes godkjenning, til å foreta romavlytting.

I hvilken grad slikt lydopptak kan aksepteres dersom det informeres om dette, er ikke utredet nærmere.

2.4 Kontrollinstans og sanksjonsmuligheter

Både Datatilsynet og Personvernemnda kan kreve de opplysningene som trengs for at de kan gjennomføre sine oppgaver, jf. § 44. Datatilsynet kan som ledd i sin kontroll med at lovens regler etterleves, kreve adgang til steder hvor det finnes personregistre, overvåkingsutstyr og

bildeopptak som nevnt i § 37. Tilsynet kan gjennomføre de prøver eller kontroller som det finner nødvendig, og kreve bistand fra personalet på stedet i den grad dette må til. Retten til å kreve opplysninger eller tilgang til lokaler og hjelpemidler, gjelder uten hinder av taushetsplikt.

Datatilsynet har kompetanse til å gripe inn og stoppe overvåking som skjer i strid med loven, for eksempel fordi overvåkingen ikke kan sies å være saklig begrunnet. Det er også meldeplikt for fjernsynsovervåking, jf. Personopplysningsloven § 31.

Forbudet i straffeloven § 390 b om fjernsynsovervåking av offentlig sted eller arbeidssted uten tilstrekkelig skilting ble flyttet til personopplysningsloven, fordi forbudet bør ses i sammenheng med de øvrige varslingsreglene.

Datatilsynet kan gi pålegg om at behandling av personopplysninger i strid med bestemmelser i eller i medhold av personopplysningsloven, skal opphøre eller stille vilkår som må oppfylles for at behandlingen skal være i samsvar med loven, jf. § 46. Ved pålegg etter nærmere angitte bestemmelser kan Datatilsynet fastsette en tvangsmulkt som løper for hver dag som går etter utløpet av den fristen som er satt for oppfylling av pålegget, inntil pålegget er oppfylt, jf. § 47. Den som forsettlig eller grovt uaktsomt bryter nærmere angitte bestemmelser i personopplysningsloven, straffes med bøter og/eller fengsel inntil ett år. Ved særdeles skjerpene omstendigheter kan fengsel inntil tre år idømmes. Medvirkning straffes på samme måte, jf. lovens § 48.

Den behandlingsansvarlige kan pålegges å erstatte skade som er oppstått som følge av at personopplysninger er behandlet i strid med bestemmelser i eller i medhold av loven, med mindre det godtgjøres at skaden ikke skyldes feil eller forsømmelse på den behandlingsansvarliges side. Erstatningen skal svare til det økonomiske tapet den skadelidte er påført som følge av den ulovlige behandlingen. Den behandlingsansvarlige kan også pålegges å betale erstatning for skade av ikke-økonomisk art (oppreisning) som synes rimelig, jf. personopplysningsloven § 49.

Personvernemnda avgjør klager over Datatilsynets avgjørelser, jf. personopplysningsloven § 42 fjerde ledd. Nemnda er et uavhengig forvaltningsorgan administrativt underordnet Kongen og departementet, jf. § 43.

3 Internasjonal regulering

De færreste Europeiske land har særskilt lovregulering av kameraovervåking. I den grad kameraovervåkingen vurderes som en elektronisk behandling av personopplysninger, faller overvåkingen imidlertid inn under EU-direktivets alminnelige bestemmelser, og er således omfattet av landenes personvernlovgivning. Dette vil for eksempel være tilfellet når opptakene lagres ved bruk av elektroniske hjelpemidler. Dersom opptakene enten lagres manuelt uten å inngå i et personregister, eller ikke lagres i det hele tatt, antas de ikke å være omfattet av direktivet.

Bare Sverige, Danmark og til en viss grad Frankrike har separat heldekkende lovgivning for kameraovervåking. Island har, i likhet med Norge, inntatt et par paragrafer om kameraovervakning i loven som tilsvare personopplysningsloven. I samtlige land, med unntak av Sverige, er det datatilsynsmyndigheten som står for tilsyn med etterlevelse av regelverket.

Selv om personvernlovgivningen i hele EØS-området er basert EUs personverndirektiv, som skal forstås på samme vis i alle EØS-landene, har det utviklet seg en noe ulik praksis når det gjelder kameraovervåking gjennom dommer, forskrifter, dekreter og en og annen deldekkende lov.

3.1 Artikkel 29-gruppen

Gruppen er nedsatt ved Europa-Parlamentets og Rådets direktiv 95/46/EF av 24. oktober 1995, som henviser til direktivets artikkel 29 og artikkel 30, nr. 1, litra a), og artikkel 30, nr. 3, som henviser til gruppens forretningsorden, særlig artikkel 12 og 14. Gruppen skal i korte trekk beskytte fysiske personer i forbindelse med behandling av personopplysninger, og omtales som artikkel 29-gruppen.

En av gruppens formål er å se til at personverndirektivet tolkes på samme måte i alle EU/EØS-land. Når det gjelder kameraovervåking vedtok gruppen den 11. februar 2004 en uttalelse om behandling av personopplysninger ved slik overvåking.

Bakgrunnen for uttalelsen var at offentlige og private foretak i Europa i de senere år, i stigende grad, har gjort bruk av forskjellige systemer for billedopptak. Dette har medført en livlig debatt både på fellesskapsnivå og i de enkelte medlemsstater om de betingelser og begrensninger, som skal gjelde for installasjon av utstyr til kameraovervåking, og om den nødvendige beskyttelse av de registrerte.

Man har i de seneste år, blant annet sett en teknologisk utvikling, herunder digitaliseringen og den kraftige reduksjon av utstyrets størrelse, økt anvendelsesmulighetene av utstyr til bilde- og lydopptak, blant annet i forbindelse med anvendelse av intranett og Internett. Borgerne har selv kunnet konstatere den omsegripende anvendelse av kameraovervåkingsteknikker. Det vises også til en stigende tendens til sammenkobling av kameraovervåkingssystemer.

3.2 Artikkel 29-gruppens uttalelse om kameraovervåking

INTERNATIONALE RETLIGE INSTRUMENTER

a) Den Europæiske Konvention om Beskyttelse af Menneskerettigheder og Grundlæggende Frihedsrettigheder

Beskyttelsen af privatlivets fred er sikret i Den Europæiske Menneskerettighedskonventions artikel 8.

b) Europarådets konvention nr. 108/1981 om beskyttelse af det enkelte menneske i forbindelse med databehandling af personoplysninger

Denne konventions anvendelsesområde er ikke ligesom direktiv 95/46/EF begrænset til aktiviteterne under den første søjle (se nedenfor). Videoovervågningsaktiviteter, der medfører behandling af personoplysninger, er således omfattet af konventionen. Det rådgivende udvalg, som er nedsat i medfør af konventionen, har erklæret, at lyd- (tale) og billeddata skal betragtes som personoplysninger, hvis de indeholder oplysninger om en person ved at gøre vedkommende identifiserbar, selv indirekte.

Europarådet er i øjeblikket ved at færdiggøre en række vejledende principper for beskyttelsen af fysiske personer med hensyn til innsamling og behandling af data i forbindelse med videoovervåkning. Disse principper skal yderligere specificere de garantier, der gjelder registrerede, og som er fastsat i Europarådets retlige instrumenter.

c) Den Europæiske Unions Charter om Grundlæggende Rettigheder

Den Europæiske Unions Charter om Grundlæggende Rettigheder indeholder i artikel 7 bestemmelser om respekt for privatliv og familieliv, hjemmet samt kommunikation og i artikel 8 om beskyttelse af personoplysninger.

3. OVERVÅGNING I HENHOLD TIL DIREKTIV 95/46/EF

Det er udtrykkeligt fremhævet i direktiv 95/46/EF (i det efterfølgende benævnt "direktivet"), at behandlingen af de personoplysninger, der er indeholdt i lyd- og billeddata, er af en særlig art, og der henvises til disse flere steder i direktivet. Direktivet sikrer beskyttelse af privatlivets fred og den mere omfattende beskyttelse af fysiske personers personoplysninger i overensstemmelse med de grundlæggende rettigheder og frihedsrettigheder (artikel 1, stk. 1).

En betydelig del af de oplysninger, der indsamles ved videoovervågning, vedrører identificerede og/eller identificerbare personer, som er blevet filmet, mens de befandt sig i offentlige og/eller offentligt tilgængelige områder. Personer, der midlertidigt befinder sig i sådanne områder, må forvente en mindre grad af beskyttelse af privatlivets fred, men ikke fuldstændig at miste samtlige rettigheder og frihedsrettigheder, som gælder for deres private sfære. Der skal også tages højde for fysiske personers ret til personlig bevægelsesfrihed i det land, de lovligt opholder sig i, hvilket er sikret i artikel 2 i 4. tillægsprotokol til Den Europæiske Menneskerettighedskonventionen.

Denne bevægelsesfrihed kan kun være genstand for de begrænsninger, der er nødvendige i et demokratisk samfund og står i forhold til gennemførelsen af specifikke målsætninger. Registrerede har ret til at udøve deres bevægelsesfrihed uden at være udsat for uforholdsmæssige psykologiske begrænsninger af deres bevægelighed og adfærd samt uden at være genstand for en detaljeret overvågning, der foretages for at følge deres færden og/eller udløse "alarmer" på grundlag af software, der automatisk og uden menneskelig indgriben "fortolker" fysiske personers eventuelt mistænkelige adfærd, som følge af flere enheders overdrevne brug af videoovervågning i en række offentlige og/eller offentligt tilgængelige områder.

Det er fremhævet i betragtningerne til direktivet, at behandlingen af lyd- og billeddata om fysiske personer er meget specifik og følsom. Disse betragtninger og de relevante artikler i direktivet gør - ud over nedenstående betragtninger med hensyn til anvendelsesområdet - det klart,

a) at direktivet i princippet finder anvendelse på dette område ved også at tage hensyn til betydningen af udviklingen inden for de teknikker, der anvendes til at optage, bearbejde eller på anden vis anvende specifikke kategorier af personoplysninger, der indsamles på denne måde (se betragtning 14),

b) at principperne for beskyttelse i direktivet finder anvendelse på enhver oplysning - herunder lyd- og billeddata - om en identificeret eller identificerbar person ved at tage højde for alle de midler, som med rimelighed må kunne forventes at blive anvendt af den registeransvarlige eller af en anden person for at identificere den pågældende (se artikel 2, litra a)) og betragtning 26.

Ud over ovennævnte specifikke henvisninger har direktivet helt tydeligt sin fulde virkning inden for rammerne af sine individuelle bestemmelser, der især vedrører:

1) *Datakvalitet*: Billeder skal behandles loyalt og lovligt til udtrykkeligt angivne og legitime formål. Billeder skal anvendes i overensstemmelse med princippet om, at oplysninger skal

være tilstrækkelige, relevante og proportionelle, og de må ikke yderligere behandles på en måde, der er uforenelig med disse formål. De må kun opbevares i en begrænset periode osv. (se artikel 6).

2) *Kriterier for legitim behandling af oplysninger*: Det er med udgangspunkt i disse kriterier nødvendigt, at behandlingen af personoplysninger ved hjælp af videoovervågning foregår på grundlag af mindst én af betingelserne i artikel 7: udtrykkeligt samtykke, opfyldelse af en kontrakt, overholdelse af en retlig forpligtelse, beskyttelse af den registreredes vitale interesser, udførelsen af en opgave i samfundets interesse eller inden for rammerne af offentlig myndighedsudøvelse, interesseafvejning.

3) Behandlingen af *særlige kategorier af oplysninger*, der er underlagt de sikkerhedsforanstaltninger, som gælder enten følsomme oplysninger eller oplysninger vedrørende overtrædelser inden for rammerne af videoovervågning (se artikel 8).

4) *Oplysningspligt* over for de registrerede (se artikel 10 og 11).

5) *De registreredes rettigheder*, især retten til indsigt eller retten til at gøre indsigelse mod behandlingen af vægtige legitime grunde (se artikel 12 og 14, litra a)).

6) Garantier i forbindelse med *edb-behandlede individuelle afgørelser* (se artikel 15).

7) *Behandlingssikkerhed* (se artikel 17).

8) *Anmeldelse af behandlinger* (se artikel 18 og 19).

9) *Forudgående kontrol* af behandlinger, som kan indebære særlige risici for de registreredes rettigheder og frihedsrettigheder (se artikel 20).

10) *Overførsel af oplysninger til tredjelande* (se artikel 25 ff.). Specificiteten og følsomheden ved behandling af lyd- og billeddata anerkendes endeligt i direktivets sidste artikel, hvor Kommissionen forpligter sig til navnlig at undersøge direktivets anvendelse på dette område og til at forelægge passende forslag, der måtte være nødvendige i betragtning af udviklingen inden for informationsteknologien og informationssamfundet (se artikel 33).

4. NATIONALE BESTEMMELSER OM VIDEOOVERVÅGNING

Der er allerede i en række medlemsstater blevet foretaget casestudier vedrørende videoovervågning, der finder sted på grundlag af forfatningsmæssige bestemmelser, specifik lovgivning eller til opfyldelse af forskrifter eller andre beslutninger fra de kompetente offentlige myndigheder.

Enkelte lande har også specifikke bestemmelser, der finder anvendelse, uanset om videoovervågningen medfører behandling af personoplysninger. Installationen og anvendelsen af CCTV-udstyr (lukkede tv-netværk) og lignende overvågningsudstyr skal i henhold til disse bestemmelser forhåndsgodkendes af en offentlig myndighed, der helt eller delvis kan være repræsenteret af den nationale databeskyttelsesmyndighed. Sådanne bestemmelser kan variere afhængig af, om det foretagende, der er ansvarlig for det relevante udstyrs drift, er af offentlig eller privat art.

I andre lande er videoovervågning ikke i øjeblikket underlagt særlige lovbestemmelser, men databeskyttelsesmyndighederne har dog bestræbt sig på at sikre en passende anvendelse af de generelle databeskyttelsesbestemmelser, bl.a. ved hjælp af udtalelser, retningslinjer eller adfærdskodekser, som f.eks. allerede er blevet vedtaget i Det Forenede Kongerige, eller som er under udarbejdelse i Italien.

Belgien

Databeskyttelsesmyndighedens udtalelser, særlig udtalelse nr. 34/99 af 13. december 1999 om behandling af billeder, herunder ved hjælp af videoovervågningssystemer, og udtalelse nr.

3/2000 af 10. januar 2000 om anvendelse af videoovervågningssystemer i indgangspartiet på lejlighedskomplekser.

Danmark

Lovbekendtgørelse nr. 76 af 1. februar 2000 om forbud mod tv-overvågning mv. I henhold til denne lov må private ikke foretage videoovervågning af gader, veje, pladser eller lignende områder, som benyttes til almindelig færdsel. Der gælder dog visse undtagelser fra dette forbud. Datatilsynets udtalelse af 3. juni 2002 om videoovervågning i et stort indkøbscenter og om liveudsendelse fra en pub på Internet. Datatilsynets udtalelse af 1. juli 2003 om, at videoovervågning, der foretages i privatdrevne offentlige transportmidler, skal stå i rimeligt forhold til formålet og være i overensstemmelse med den danske databeskyttelseslovgivning. Datatilsynets udtalelser af 13. november 2003 om visse begrænsninger af den videoovervågning, der foretages af offentlige myndigheder.

Finland

Finland har ingen specifik lovgivning om videoovervågning, men der findes en række bestemmelser om videoovervågning og anden teknisk overvågning, observation eller kontrol i en lang række love. Der stilles regelmæssigt spørgsmål om videoovervågning og aflytning, og der har været en række sager. Databeskyttelsesombudsmanden har f.eks. afgivet en udtalelse om registrering af telefonsamtaler i forbindelse med kundebetjening og på arbejdspladsen (sagsnr. 1061/45/2000 og 425/45/2000).

Det finske kontor har udgivet en brochure om beskyttelse af privatlivets fred i forbindelse med videoovervågning

Frankrig

Lov nr. 78-17 af 6. januar 1978 om behandling, registrering og frihedsrettigheder (CNIL).

Databeskyttelsesmyndighedens anbefaling nr. 94-056 af 21. juni 1994.

Databeskyttelsesmyndighedens vejledning om videoovervågning på arbejdspladsen:

<http://www.cnil.fr/thematic/index.htm>; om andre emner (f.eks. webkameraer). Særlov om videoovervågning af offentlige områder til beskyttelse af den offentlige orden: lov nr. 95-73 af 21. januar 1995 om sikkerhed (som ændret ved bekendtgørelse 2000-916 af 19. september 2000). Dekret nr. 96-926 af 17. oktober 1996 og cirkulære af 22. oktober 1996 om gennemførelse af lov nr. 95-73.

Grækenland

1) Skrivelse nr. 390 af 28. januar 2000 om installation af et lukket tv-netværk i Athens undergrundsbane.

2) Forordning nr. 1122 af 26 september 2000 om lukkede tv-netværk.

3) Beslutning nr. 84/2002 om lukkede tv-netværk i hoteller.

Tyskland

Afsnit 6 b i forbundsloven af 2001. Afsnit 25 i loven om grænsekontrol. Der findes yderligere bestemmelser om politiets videoovervågning i delstaternes politivedtægter. Forbundsdagen behandler i øjeblikket et lovforslag om forbud mod hemmelig videoovervågning.

Irland

Databeskyttelseslov 1998 og 2003. Casestudie nr. 14/1996 (anvendelse af CCTV).

Italien

Afsnit 134 i loven om beskyttelse af personoplysninger (lovdekret nr. 196 af 30. juni 2003 (om vedtagelse af en adfærdskodeks). Databeskyttelsesmyndighedens (*Garante*) afgørelse nr. 2 af 10. april 2002 (om vedtagelse af adfærdskodekser), 28. september 2001 (biometriteknikker og teknikker til ansigtsgenkendelse, der anvendes af banker) og af 29. november 2000 (de såkaldte "ti bud om videoovervågning"). Præsidentdekret nr. 250 af 22. juni 1999 (om regulering af køretøjers adgang til bycentre og områder med begrænset kørsel). Dekret nr. 433 af 14. november 1992 og lov nr. 4/1993 (om museer og statens biblioteker og arkiver). Lovdekret nr. 45 af 4. februar 2000 (passagerskibe på nationale ruter). Afsnit 4 i lov nr. 300 af 20. maj 1970 (den såkaldte "vedtægt for arbejdstagere").

Luxembourg

Artikel 10 og 11 i lov af 2. august 2002 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.

Nederlandene

Databeskyttelsesmyndighedens rapport af 1997 indeholder retningslinjer for videoovervågning, særlig med hensyn til beskyttelsen af fysiske personer og af ejendom på offentlige områder. Der vil i 2004 blive offentliggjort en opdatering af retningslinjerne fra 1997. Der foretages en undersøgelse af anvendelsen af videoovervågning i alle nederlandske kommuner i 2003. Straffeloven vil pr. 1. januar 2004 blive ændret, således at der sker en udvidelse af anvendelsesområdet for den lovovertrædelse, der består i at tage billeder af offentligt tilgængelige steder uden på forhånd at underrette de berørte personer. Regeringen foreslår at ændre loven om lokalforvaltning, der giver kommunalbestyrelserne og borgmestrene udtrykkelig tilladelse til under visse betingelser (f.eks. krav om regelmæssigt at evaluere overvågningens virkning) og til visse offentlige formål at anvende videoovervågningssystemer på offentlige steder.

Portugal

Lovdekret nr. 231/98 af 22. juli 1998 (private sikkerhedsforanstaltninger og systemer til egen beskyttelse). Lov nr. 38/98 af 4. august 1998 (foranstaltninger, der skal træffes i tilfælde af vold i forbindelse med sportsbegivenheder). Lovdekret nr. 263/01 af 28. september 2001 (dansesteder). Lovdekret nr. 94/2002 af 12. april 2002 (sportsbegivenheder).

Spanien

Forfatningslov (*ley organica*) nr. 4/1997 (videoovervågning foretaget af vagtselskaber i offentlige områder). Kongeligt dekret (*Real Decreto*) nr. 596/1999 om gennemførelse af lov nr. 4/1997.

Sverige

Videoovervågning reguleres specifikt i lov nr. 1998:150 om almindelig videoovervågning og i lov nr. 1995:1506 om hemmelig videoovervågning (i forbindelse med efterforskningen i kriminalsager)². Almindelig videoovervågning kræver i princippet en tilladelse fra de kommunale myndigheder. Dog kræves der ingen tilladelse til overvågning af f.eks.

² I Sverige kræver almindelig videoovervågning i princippet en tilladelse fra de kommunale myndigheder, selv om der findes en række undtagelser, f.eks. overvågning af postkontorer, banker og butikker. Hemmelig videoovervågning kræver en dommerkendelse. En afgørelse fra de kommunale myndigheder i henhold til loven om almindelig videoovervågning kan ankes til justitsministeren for at beskytte offentlige interesser.

Videoovervågning ved hjælp af digitalkameraer er blevet anset for at udgøre en behandling af personoplysninger i henhold til den svenske lov om personoplysninger, og denne form for overvågning har derfor været omfattet af databeskyttelsesmyndighedens kontrol. Et undersøgelsesudvalg er i øjeblikket ved at undersøge anvendelsen af videoovervågning med henblik på forebyggelse af kriminelle handlinger. Udvalget skal f.eks. foretage en

postkontorer, banker og butikker. Hemmelig videoovervågning kræver en dommerkendelse. En afgørelse fra de kommunale myndigheder i henhold til loven om almindelig videoovervågning kan ankes til justitsministeren.

Videoovervågning ved hjælp af digitalteknik anses for at udgøre en behandling af personoplysninger, og denne form for overvågning er derfor omfattet af databeskyttelsesmyndighedens kontrol, når den ikke er specifikt reguleret i loven om almindelig videoovervågning.

Det Forenede Kongerige

Kodeks for brug af CCTV av 2000 (*CCTV Code of practice 2000*) fra den britiske databeskyttelsesmyndighed (*Information Commissioner*), i øjeblikket under revision.

Der er ligeledes vedtaget vigtige supplerende lovbestemmelser i Island (afsnit 4, lov nr. 77/2000), Norge (afsnit VII i lov nr. 31 af 14. april 2000), Schweiz (henstilling fra den føderale databeskyttelsesmyndighed) og Ungarn (databeskyttelsesmyndighedens henstilling af 20. december 2000).

5. OMRÅDER, HVOR DIREKTIV 95/46/EF IKKE ELLER KUN DELVIST FINDER ANVENDELSE

Direktivet finder ikke anvendelse på behandling af lyd- og billeddata til formål, der vedrører den offentlige sikkerhed, forsvaret, statens sikkerhed og statens aktiviteter på det strafferetlige område og/eller i forbindelse med enhver anden aktivitet, der ikke er omfattet af fællesskabsretten. En lang række medlemsstater har imidlertid ved gennemførelsen af direktiv 95/46/EF inddraget disse områder på en generel måde, dog sammen med specifikke undtagelser.

A) I visse lande er de behandlinger, der udføres til ovennævnte formål, i alle tilfælde underlagt garantier i overensstemmelse med Europarådets konvention nr. 108/1981 og de relevante anbefalinger fra Europarådet samt visse nationale bestemmelser (se artikel 3, stk. 2, og betragtning 16 i direktiv 95/46/EF). Denne kategori af behandlinger vil ikke blive behandlet på detaljeret vis i dette dokument, fordi de er meget specifikke og er underlagt særlige bestemmelser, der også vedrører efterforskningsrelaterede aktiviteter, som udføres af politiet og domstolene af hensyn til statens sikkerhed¹⁰, og som kan omfatte "skjult" videoovervågning, dvs. uden at de berørte personer på stedet informeres om de pågældende overvågning.

Gruppen ønsker dog at understrege, at videoovervågning, der udføres i medfør af konkrete krav til den offentlige sikkerhed eller med henblik på afsløring, forebyggelse eller kontrol af kriminelle handlinger, ligesom en række andre behandlinger af personoplysninger, der ligeledes falder uden for direktivets anvendelsesområde, skal være i overensstemmelse med kravene i artikel 8 i Den Europæiske Menneskerettighedskonvention og både være omfattet af særlige bestemmelser, som offentligheden har kendskab til, samt vedrøre og stå i forhold til forebyggelsen af *konkrete* risici og *specifikke* overtrædelser – f.eks. på steder, der er udsat for sådanne risici, eller i forbindelse med offentlige begivenheder, hvor sådanne overtrædelser

vurdering af loven om almindelig videoovervågning for at se, om eventuelle ændringer er nødvendige. Undersøgelsesudvalget skal ligeledes foretage en vurdering af anvendelsesområdet for den svenske lov om personoplysninger med hensyn til videoovervågning og et eventuelt behov for særlig lovgivning om behandling af personoplysninger i forbindelse med videoovervågning.

med rimelighed kan forventes at finde sted. Der skal tages højde for virkningerne af videoovervågning - f.eks. at lovovertrædelser begås andre steder - og det skal altid tydeligt angives, hvem der er den registeransvarlige, således at de registrerede har mulighed for at udøve deres rettigheder. Sidstnævnte krav skyldes også den omstændighed, at videoovervågning i stigende grad gennemføres i fællesskab af politi og andre offentlige myndigheder (f.eks. lokale myndigheder) og/eller private foretagender (banker, idrætsforeninger, transportselskaber), således at der kan opstå tvivl om den enkeltes rolle og ansvar med hensyn til de opgaver, der skal udføres¹².

B) For det andet finder direktivet ikke anvendelse på behandlinger, der foretages en fysisk person i forbindelse med rent personlige eller familiemæssige aktiviteter (se artikel 3, stk. 2, og betragtning 12). Mens ovennævnte bestemmelser kan være relevante, hvis der f.eks. foretages videoovervågning med henblik på afstandskontrol af, hvad der foregår i ens hjem - f.eks. for at forebygge tyveri eller i forbindelse med styring af den såkaldte e-familie - er dette ikke tilfældet, hvis videoovervågningsudstyret installeres uden for eller i nærheden af den private ejendom med henblik på ejendomsbeskyttelse og/eller for at garantere sikkerheden. Det kan i sidstnævnte tilfælde for det første være, at udstyret ikke er installeret af de enkelte ejere for at overvåge de døre, som giver adgang til deres bolig, men af flere ejere i henhold til en aftale eller af en grundejerforening eller et ejerlejlighedskompleks for at overvåge flere adgange og områder i bebyggelsen, hvormed direktivet finder anvendelse på de relevante aktiviteter.

Når udstyret anvendes til fordel for en enkelt familie og til at overvåge en enkelt dør, repos, parkering osv., er den omstændighed, at direktivet ikke finder anvendelse på grund af den udelukkende personlige anvendelse og tredjemands manglende adgang til de pågældende oplysninger, ikke ensbetydende med, at den ansvarlige for udstyret er fritaget fra at overholde naboernes og andre forbipasserende personers legitime rettigheder og interesser. I EU-medlemsstaterne er disse rettigheder og interesser - uanset de gældende databeskyttelsesprincipper - beskyttet i henhold til de generelle (civilretlige) bestemmelser om beskyttelse af personlige rettigheder, billeddata om en selv, familieliv og privatliv, f.eks. hvis vinklen, hvormed et kamera er monteret uden for døren til en lejlighed, gør det muligt på systematisk vis at registrere kunder til en lægekonsultation og/eller et advokatfirma beliggende på samme etage, således at disse firmaers tavshedspligt tilsidesættes³. Der skal udvises særlig opmærksomhed omkring videoudstyrets orientering, behovet for at informere og anbringe meddelelser og den rettidige sletning af billeddata - der skal finde sted inden for nogle få timer - hvis der ikke er sket indbrud eller overtrædelser.

C) Endelig fastsættes det i direktivets artikel 9, at medlemsstaterne med hensyn til behandlinger, der udelukkende finder sted i journalistisk øjemed eller med henblik på kunstnerisk eller litterær virksomhed, navnlig på det audiovisuelle område, skal fastsætte fritagelser eller undtagelser fra visse af direktivets bestemmelser (se betragtning 17). Der skal kun fastsættes undtagelser, for så vidt som de er nødvendige for at forene retten til privatlivets

³ Et godt eksempel på denne risiko er de aktiviteter, der udføres af nogle kommuner i Italien med henblik på ved hjælp af videoudstyr at overvåge offentlige steder, hvor de prostituerede opholder sig om natten. En række kommuner har tidligere gjort gældende, at de havde kompetence - hvilket er tvivlsomt - til at træffe foranstaltninger til at forebygge dette fænomen, mens andre kommuner vedtog vedtægter, der alene forbød de prostitueredes kunder at parkere deres biler og/eller køre i disse områder og truede med at sende billeder til deres hjemmeadresse, hvis de overtrådte denne vedtægt. Den italienske myndighed har vedtaget en beslutning med henblik på at klarlægge de passende foranstaltninger for at rejse tiltale for overtrædelse af de pågældende bestemmelser.

fred med reglerne for ytringsfrihed⁴. Man skal i denne forbindelse være særlig omhyggelig ved installationen af webkameraer og/eller onlinekameraer for at undgå en mangelfuld beskyttelse af fysiske personer, der er genstand for videoovervågning til formål som reklame og/eller fremme af turismen⁵.

6. VIDEOOVERVÅGNING OG BEHANDLING AF PERSONOPLYSNINGER

Gruppen finder det i lyset af de forskellige situationer som anført ovenfor nødvendigt at påpege, at direktiv 95/46/EF finder anvendelse på behandlingen af personoplysninger, herunder behandlingen af lyd- og billeddata ved hjælp af CCTV eller andet videoovervågningsudstyr, der helt eller delvis foretages ved hjælp af elektroniske midler, og på en ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Lyd- og billeddata, der vedrører identificerede eller identificerbare fysiske personer, skal betragtes som personoplysninger,

a) selv om billederne anvendes i et lukket kredsløb, og selv om de ikke associeres med mere detaljerede oplysninger om de berørte personer,

b) selv om de ikke vedrører fysiske personer, hvis ansigter er blevet filmet, til trods for, at de indeholder andre oplysninger, f.eks. nummerplader eller PIN-numre, som kræves i forbindelse med overvågningen af automatiske pengeautomater, uanset det medie, der anvendes til behandlingen (f.eks. faste og/eller mobile videosystemer i form af bærbare videomodtagere, farver og/eller sort-hvid billeder), den anvendte teknik (kabel eller fiberoptik), typen af udstyr (stationært, roterende eller mobilt), billedoptagelsesformen (kontinuerligt i modsætning til diskontinuerligt, f.eks. hvis der kun sker billedoptagelse ved overtrædelse af en hastighedsbegrænsning, hvilket adskiller sig fra randomiserede og periodevise videooptagelser), og de anvendte kommunikationsværktøjer (f.eks. tilslutningen til en "central" og/eller videregivelsen af billeder til fjerntliggende terminaler osv.).

Identificerbarhed i direktivets betydning kan også være resultatet af, at de pågældende oplysninger sammenholdes med oplysninger, som tredjemand er i besiddelse af, eller i det enkelte tilfælde ved anvendelse af specifikke teknikker og/eller anordninger. En af de første foranstaltninger, som den registeransvarlige skal træffe, er at kontrollere, om videoovervågningen medfører behandling af personoplysninger, hvis den vedrører identificerbare personer. Hvis dette er tilfældet, finder direktivet anvendelse uanset eventuelle nationale bestemmelser, der desuden kræver en tilladelse af hensyn til den offentlige sikkerhed.

Dette gælder f.eks. udstyr, der er anbragt ved indgangen til eller i en bank, og som gør det muligt at identificere kunderne. Til gengæld finder direktivet under visse omstændigheder hverken anvendelse på luftovervågningsbilleder, der ikke kan forstørres til noget "brugbart" resultat eller ikke indeholder data om fysiske personer (f.eks. billeder, der indsamles for at identificere vandforekomster eller lossepladser), eller på udstyr, der i fejende bevægelser tager billeder af motorvejstrafikken.

7. DEN REGISTERANSVARLIGES PLIGTER, SÆRLIGT PLIGTEN TIL AT TRÆFFE PASSENDE FORANSTALTNINGER

⁴ Se gruppens henstilling nr. 1/97 om databeskyttelseslovgivningen og medierne.

⁵ Et skjult webkamera, der var installeret i nærheden af trapperne til en undergrundsstation i Milano, viste intime billeder af forbipasserende kvinder direkte på Internet til formål, der angiveligt var forbundet med journalistiske aktiviteter. Den nationale databeskyttelsesmyndighed kunne ikke gribe ind, fordi det ikke var muligt at identificere de berørte personer.

A) Behandlingens lovlighed

Den registeransvarlige skal - ligeledes med udgangspunkt i kravet om, at behandlingen skal være lovlig (jf. direktivets artikel 6, litra a)) - på forhånd kontrollere, om overvågningen opfylder de generelle og specifikke bestemmelser, der gælder på dette område, herunder love, forordninger og adfærdskodekser af retlig relevans. Disse bestemmelser kan også være blevet fastsat i forbindelse med hensynet til den offentlige sikkerhed og med andre hensyn end beskyttelsen af personoplysninger, f.eks. behovet for at opnå adhoc-tilladelser fra særlige offentlige myndigheder og følge deres instrukser.

Alle passende foranstaltninger skal træffes for at sikre, at videoovervågning er i overensstemmelse med databeskyttelsesprincipperne, og der bør ikke på upassende vis henvises til beskyttelsen af privatlivets fred⁶. Der skal i denne henseende også tages højde for bedste praksis, som måtte være fastsat i retningslinjer fra tilsynsmyndighederne, samt andre selvreguleringsinstrumenter.

Det er ligeledes nødvendigt at gennemgå de resterende nationale lovbestemmelser - herunder forfatningsmæssige principper og lovbestemmelser på det civilretlige og det strafferetlige område - med hensyn til især de bestemmelser, der finder anvendelse på "retten til billeddata"⁷ eller beskyttelsen af ens egen bopæl; og der skal tages højde for den relevante retspraksis, hvor det kan være fastslået, at andre lokaliteter end dem, der er omfattet af ens bopæl, herunder hotelværelser, kontorlokaler, toiletter, garderober, indendørs telefonbokse osv., skal betragtes som private lokaliteter.

Når udstyret installeres af private firmaer eller offentlige organer, herunder især lokale myndigheder, med henvisning til hensynet til sikkerheden eller for at afsløre, forebygge eller kontrollere lovovertrædelser, skal der ved fastsættelsen af og informeringen om de pågældende formål tages særligt hensyn til de opgaver, som på lovlig vis kan udføres af den registeransvarlige - idet visse offentlige opgaver kun kan udføres på lovlig vis af specifikke ikke-offentlige organer, herunder især retshåndhævende instanser.

Dette spørgsmål har været rejst specifikt i forbindelse med en række lokale myndigheder, der ikke har direkte kompetence med hensyn til visse aspekter af den offentlige orden og den offentlige sikkerhed, men som alligevel udfører supplerende overvågningsaktiviteter. På samme måde har overvågning, der ofte foretages med henvisning til kriminalitetskontrol, i virkeligheden til formål at indsamle bevismateriale i tilfælde af, at der bliver begået en lovovertrædelse.

B) Formålenes specificitet, specifikation og lovlighed

Den registeransvarlige skal sikre, at de formål, der søges opfyldt, hverken er uklare eller tvetydige, således at der også kan fastsættes præcise kriterier for vurderingen af, om behandlingens formål er forenelige med de gældende regler (se direktivets artikel 6, litra b)). Disse præciseringer er også nødvendige for at angive formålene både i den information, der gives de registrerede og i den relevante anmeldelse, og i forbindelse med den forudgående kontrol, der om muligt foretages af behandlingen i medfør af direktivets artikel 20.

⁶ En bank og en lokal politistation gav med henvisning til beskyttelsen af privatlivets fred for nylig afslag til en kunde, der havde anmodet om, at man fra de billeder, som var blevet optaget af et kamera, der også filmede en pengeautomat, udtog billederne af en tyv, som efter at have stjålet kundens bankkort, havde anvendt kortet til på ulovlig vis at hæve penge i pengeautomaten.

⁷ Denne rettighed kræver i Frankrig og Belgien "forudgående samtykke".

Det skal tydeligt angives, at de billeder, som indsamles, ikke må anvendes til andre formål, særlig med hensyn til de eksisterende reproduktionsteknikker, f.eks. ved udtrykkeligt at forbyde kopiering. De relevante formål skal fremgå af et dokument, hvor der også skal være et resumé af andre vigtige bestemmelser om beskyttelse af privatlivets fred, bl.a. sådanne vigtige aspekter som dokumentation for det tidspunkt, hvor billederne slettes, eventuelle anmodninger om egenaccess fra de registrerede og/eller lovlig anvendelse af oplysningerne.

C) Kriterier for, hvornår en behandling kan betragtes som lovlig

Den registeransvarlige skal sikre, at videoovervågningen ikke alene overholder de specifikke bestemmelser, hvortil der henvises i afsnit A), men også mindst ét af de kriterier, der gør behandlingen lovlig i henhold til direktivets artikel 7 - hvad specifikt angår beskyttelsen af personoplysninger.

Undtagen i de mindre hyppige tilfælde, hvor en retlig forpligtelse skal overholdes (der har været henvist til aktiviteterne på et kasino), eller hvor behandlingen er nødvendig for at beskytte vitale interesser (f.eks. til distanceovervågning af patienter i genopvågningslokaler), sker det ofte, at den registeransvarlige anmodes om at udføre en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse ved at opfylde visse særlige bestemmelser (f.eks. at konstatere trafikforseelser eller voldelig adfærd i offentlige transportmidler i områder med høj kriminalitet), jf. direktivets artikel 7, litra e); alternativt kan den registeransvarlige forfølge en legitim interesse, der ikke tilsidesættes af den registreredes grundlæggende rettigheder og frihedsrettigheder (se direktivets artikel 7, litra f)).

I begge tilfælde, dog især i sidstnævnte, kræver de pågældende behandlings følsomme karakter en omhyggelig vurdering af omfanget af den registeransvarliges opgaver, beføjelser og legitime interesser. Denne analyse skal foretages uden at være overfladisk og uden på ubegrundet vis at udvide omfanget af sådanne opgaver og beføjelser.

Man skal især med hensyn til afvejningen af de forskellige interesser - også ved at høre de berørte parter på forhånd - være særlig opmærksom på muligheden for, at en interesse, som fortjener at blive beskyttet, kan være uforenelig med enten udstyrets installation eller med visse dataforvaringsordninger eller andre behandlinger⁸.

Endelig skal den registreredes samtykke være utvetydigt og baseret på tydelig information. Samtykket skal gives separat og specifikt i forbindelse med overvågningen af de lokaliteter, hvor en person lever sit privatliv⁹. Behandlingens lovlighed skal også vurderes i forhold til direktivets bestemmelser om specifikke garantier for oplysninger om lovovertrædelser (direktivets artikel 8, stk. 5)¹⁰. Der kan på grundlag af den forudgående vurdering af behandlingen i forbindelse med den forudgående kontrolmekanisme træffes yderligere foranstaltninger, hvis videoovervågningen indebærer særlige risici for fysiske personers

⁸ Det er i henhold til afsnit 6b i den nye tyske databeskyttelseslov, der trådte i kraft den 23. maj 2001, tilladt at overvåge offentligt tilgængelige områder ved hjælp af optiske og elektroniske anordninger, hvis der f.eks. ikke er nogen grund til at tro, at den registreredes interesser, som skal beskyttes, går forud herfor.

⁹ Man skal i tilfælde af installationen af videoovervågningsudstyr i fællesskab (bofællesskaber osv.) være opmærksom på, om der foreligger en reel mulighed for at give et gyldigt samtykke i den betydning, hvormed dette begreb anvendes i artikel 2, litra h), i direktiv 95/46/EF ("enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilliger i, at personoplysninger, der vedrører den pågældende selv, gøres til genstand for behandling").

¹⁰ Der kan her henvises til paragraf 8 i den portugisiske lov nr. 67/98 med hensyn til oplysninger om personer, der er mistænkt for deltagelse i ulovlige og/eller kriminelle aktiviteter.

rettigheder og frihedsrettigheder (se artikel 20 i direktiv 95/46/EF). Behandlinger ved hjælp af videoovervågning må kun foretages med hjemmel i udtrykkelige lovbestemmelser, hvis de foretages af offentlige organer.

D) Proportionalitet i brugen af videoovervågning

Princippet om, at oplysninger skal være egnede og stå i forhold til de formål, der søges opfyldt, betyder for det første, at CCTV og lignende videoovervågningsudstyr kun må anvendes som et supplement: De må således kun anvendes til formål, der virkelig berettiger anvendelsen af sådanne systemer.

I henhold til proportionalitetsprincippet kan disse systemer anvendes, hvis andre fysiske og/eller generelle forebyggelses-, beskyttelses- og/eller sikkerhedsforanstaltninger, der ikke medfører billedoptagelse (f.eks. anvendelse af armerede døre til at forebygge vandalisme, installation af automatiske porte og adgangstilladelsesanordninger, fælles alarmsystemer, bedre og kraftigere gadebelysning om natten osv.), tydeligt viser sig at være utilstrækkelige og/eller uegnede med hensyn til ovennævnte legitime formål.

Det samme princip finder også anvendelse på valget af passende teknologi, kriteriet for den konkrete anvendelse af udstyret og de nærmere databehandlingsspecifikationer vedrørende bl.a. adgang og forvaringsperiode.

Man skal bl.a. undgå, at en offentlig myndighed installerer videoovervågningsudstyr i forbindelse med mindre overtrædelser, f.eks. for at håndhæve rygeforbudet i skoler eller på andre offentlige steder eller forbudet mod at smide cigaretskod og andet affald på offentlige steder.

Det er med andre ord nødvendigt på en sag-til-sag-basis at anvende *princippet om egntethed* i forhold til de formål, der søges opfyldt, hvilket medfører en slags *dataminimeringspligt* for den registeransvarlige.

Mens et videoovervågnings- og alarmeringssystem, der står i forhold til de fastsatte mål, kan betragtes som lovlig, hvis der har været flere voldsepisoder i nærheden af et stadion, eller hvis der gentagne gange sker overfald i busser i afsidesliggende områder eller i nærheden af stoppesteder, gælder dette ikke et system, der enten har til formål at forebygge verbale overgreb mod buschauffører eller at køretøjerne bliver svinet til (som beskrevet i en anmeldelse til databeskyttelsesmyndigheden), at identificere personer, der er skyldige i mindre administrative overtrædelser (f.eks. at efterlade skraldeposer ved siden af skraldespande og/eller i områder, hvor der ikke må henkastes affald), eller at afsløre personer, der begår tyveri i svømmehaller.

Vurderingen af, hvorvidt foranstaltningerne er proportionelle, skal foretages efter endnu strengere kriterier, når det gælder steder, der ikke er offentligt tilgængelige. Det kan i denne henseende være nyttigt at udveksle information og erfaring mellem de kompetente myndigheder i forskellige medlemsstater¹¹.

Ovenstående betragtninger finder i særdeleshed anvendelse på den mer og mer udbredte anvendelse af videoovervågning til selvforsvar og ejendomsbeskyttelse, særligt i nærheden af offentlige bygninger og kontorer og de omkringliggende områder. Denne type anvendelse kræver en mere overordnet vurdering af de indirekte virkninger af en massiv anvendelse af

¹¹ Dette ville også give en bedre mulighed for at harmonisere de gældende bestemmelser og de administrative beslutninger, der ofte er meget divergerende, f.eks. i forbindelse med spillehaller.

videoovervågning, det vil sige, om installationen af en række anordninger virkeligt virker forebyggende, eller om potentielle lovovertrædere ikke bare vælger andre områder eller aktiviteter.

E) Videoovervågningsaktiviteterne skal være proportionelle

Princippet om, at oplysningerne skal være egnede, relevante og proportionelle medfører, at der, efter en konstatering af, at behandlingen er lovlig, skal foretages en omhyggelig vurdering af, *hvorvidt de foranstaltninger, der gælder databehandlingen, er proportionelle*. Der skal først og fremmest tages højde for *optagelsesforanstaltningerne*, særlig med hensyn til

- a) kameravinklen i forhold til formålet¹² - hvis f.eks. overvågningen finder sted på et offentligt sted, skal kameraet sidde i en vinkel, der ikke gør det muligt at se detaljer og/eller somatiske træk, som ikke er relevante i forhold til formålene, eller områder af private nærliggende lokaliteter, særligt hvis udstyret gør det muligt at zoome ind,
- b) typen af udstyr, der anvendes til at filme, f.eks. om det er stationært eller mobilt,
- c) de aktuelle monteringsforhold, dvs. placering af kameraer, anvendelse af faste og/eller bevægelige kameraer osv.
- d) muligheden for at forstørre billeder og/eller zoome billeder ind på optagelsestidspunktet eller efterfølgende, dvs. af lagrede billeder, og muligheden for at sløre eller slette enkelte billeder,
- e) billedfastfrysningssfunktioner,
- f) tilslutning til en central med henblik på afgivelse af akustisk og/eller visuel alarm,
- g) foranstaltningerne, der træffes som følge af videoovervågningen, dvs. lukning af adgange, alarmering af vagtpersonale osv.

For det andet er det nødvendigt at tage højde for den *beslutning, der skal træffes vedrørende forvaring af billeder og forvaringsperioden* - idet sidstnævnte periode skal være begrænset og i overensstemmelse med de særlige forhold, der gør sig gældende i den pågældende situation. Mens det i enkelte tilfælde kan være tilstrækkeligt med et system, der kun tillader visning i et lukket kredsløb af billeder, der ikke optages, f.eks. ved overvågning af kasseapparaterne i et supermarked, kan det i andre tilfælde være berettiget, f.eks. for at beskytte private lokaliteter, at optage billeder, der efterfølgende slettes automatisk efter nogle få timer, senest ved dagens afslutning og under alle omstændigheder ved ugens afslutning. Denne regel vil naturligvis blive fraveget, hvis der er afgivet alarm, eller hvis der er blevet fremsat en anmodning, som kræver særlig opmærksomhed, idet der i sådanne sager vil være en berettiget anledning til i en kortere periode at afvente en eventuel beslutning fra politiet eller en domstol.

For at nævne et andet eksempel skulle et system, der havde til formål at afsløre uautoriseret kørsel med biler i bycentrum eller i områder med begrænset kørsel, kun optage billeder i det tilfælde, at der blev begået en overtrædelse. Der skal ligeledes tages behørigt hensyn til proportionalitetsprincippet, når det anses for nødvendigt med en kortere forvaringsperiode for

¹² Den italienske databeskyttelsesmyndighed har f.eks. truffet to afgørelser, hvoraf det fremgår, at der skal træffes særlige foranstaltninger med hensyn til kameravinklen. En institution inden for sundhedsvæsenet, der agtede at give de pårørende mulighed for på afstand at observere patienter, der lå i koma, var i karantæne og/eller var alvorligt syge på en akutafdeling, blev gjort opmærksom på, at det var nødvendigt at træffe passende foranstaltninger for at undgå samtidig at vise andre patienter. I en anden sag påpegede myndigheden over for politiet, at det i forbindelse med et system, der skulle afsløre overtrædelser af hastighedsbegrænsningerne, kun måtte filme de relevante nummerplader og ikke samtidig kabinen.

billederne, der dog ikke må overskride en uge¹³, f.eks. i tilfælde af videoovervågningsbilleder, der kan anvendes til at identificere personer, der har opholdt sig i en bank forud for et røveri.

Der skal for det tredje tages højde for de *tilfælde, hvor identificeringen af en person optimeres* ved at associere billeder af den pågældendes ansigt med andre oplysninger om den filmede adfærd og/eller de filmede aktiviteter - f.eks. i tilfælde af associering mellem billeder og aktiviteter, der udføres af kunder i en bank på et nemt identificerbart tidspunkt.

Der skal i denne henseende tages højde for den tydelige forskel mellem midlertidig forvaring af videoovervågningsbilleder, der opnås ved hjælp af udstyr, som er anbragt ved indgangen til en bank, og den klart mere indgribende etablering af databaser indeholdende billeder og fingeraftryk, som bankkunderne frivilligt afgiver.

Endelig skal der tages højde for de beslutninger, der skal træffes med hensyn til både den *eventuelle videregivelse af data til tredjemand* - som i princippet ikke skal omfatte enheder, der ikke har nogen tilknytning til de pågældende overvågningsaktiviteter - og deres fuldstændige eller delvise videregivelse til udlandet eller endog online - også i lyset af bestemmelserne vedrørende tilstrækkeligt beskyttelsesniveau, jf. direktivets artikel 25 ff. Kravet om, at billeder skal være relevante og proportionelle, finder tydeligvis også anvendelse på samkørsel af oplysninger, som forskellige ansvarlige for videoovervågningssystemer er i besiddelse af.

Formålet med ovenstående garantier er - også på det operationelle plan - at gennemføre princippet, som de nationale lovbestemmelser i en række lande betegner som princippet om moderation ved anvendelse af personoplysninger, der har til formål i videst muligt omfang at forebygge eller reducere behandlingen af personoplysninger.

Dette princip bør gennemføres inden for alle sektorer ved også at tage hensyn til den kendsgerning, at mange formål i virkeligheden godt kan opnås uden at gøre brug af personoplysninger eller ved at bruge anonymiserede oplysninger, selv om de umiddelbart ser ud til at kræve anvendelse af personoplysninger.

Ovenstående betragtninger finder også anvendelse, når der er et ellers berettiget behov for at optimere en virksomheds ressourcer¹⁴ eller forbedre de tjenester, der ydes brugerne¹⁵.

F) Informering af de registrerede

Kravet om åbenhed og gennemsigtighed ved anvendelse af videoovervågningsudstyr medfører anvendelse af bestemmelsen om passende informering af de registrerede i henhold til direktivets artikel 10 og 11.

De registrerede skal informeres i overensstemmelse med direktivets artikel 10 og 11. De skal være klar over, at der foretages videoovervågning, også selv om denne overvågning vedrører

¹³ Den danske og den svenske databeskyttelsesmyndighed har givet udtryk for, at videoovervågningsbilleder kun må opbevares i en kort periode, og at denne periode ikke må overskride 30 dage.

¹⁴ Dette kan f.eks. være tilfældet, hvis der er behov for at beregne antallet af kasseapparater, som det er passende at have åbent samtidig i et supermarked afhængig af antallet af kunder, der går ind, eller hvis det er nødvendigt at optimere kundernes indkøbsrute i et supermarked.

¹⁵ For at lette adgangen til arbejdspladser og/eller særlige transportmidler, der kræver identitetskontrol, kan det være tilstrækkeligt med identifikationskort med billede, eventuelt på et edb-baseret medie, uden at gøre brug af et system med ansigtsgenkendelse.

offentlige begivenheder og forestillinger eller reklameaktiviteter (webkameraer), og de skal informeres på detaljeret vis om de steder, der overvåges.

Det er ikke nødvendigt at specificere overvågningsudstyrets nøjagtige placering, men der skal være en tydelig angivelse af, hvad der er genstand for overvågning. Disse informationer skal være anbragt i en passende afstand fra de steder, der overvåges - i modsætning til nogle enkelte sager, hvor placeringen af informationstavler i en afstand på 500 meter fra overvågningsområdet blev accepteret - og der skal også tages hensyn til optagelsesforanstaltningerne.

Informationen skal være synlig og kan gives på sammenfattende vis, såfremt den er effektiv. Der kan gøres brug af symboler, som allerede har været anvendt i forbindelse med videoovervågning og information om rygeforbud - som kan variere afhængigt af, om billederne optages eller ej. Formålet med videoovervågningen og den ansvarlige registeransvarlige skal i alle tilfælde specificeres. Informationernes format skal være tilpasset de konkrete placeringsforhold¹⁶.

Der kan kun i specifikke og berettigede tilfælde gøres undtagelser fra kravet om information, jf. direktivets artikel 10, 11 og 13, og en midlertidig undtagelse finder således anvendelse i forbindelse med oplysninger, der indsamles inden for rammerne af undersøgelser, som på lovlig vis foretages af forsvarsadvokater, eller med henblik på at gøre retten til forsvar gældende, når man ved at give den pågældende information risikerer at forhindre opfyldelsen af de specifikke formål.

Endelig skal man være særlig opmærksom på, hvorledes denne information på passende vis kan formidles til blinde.

G) Supplerende krav

Gruppen ønsker med hensyn til sådanne supplerende krav, sikkerhedsforanstaltninger og garantier, som er fastsat i databeskyttelseslovgivningen, og som er sammenfattet i punkt 3) ovenfor – også hvad angår kravet om, at behandlinger af personoplysninger anmeldes til og er underlagt kontrollen af en uvildig myndighed i medfør af direktivets artikel 18, 19 og 28 - at gøre opmærksom på følgende aspekter:

a) Et begrænset antal fysiske personer, der skal specificeres, skal have tilladelse til at se eller anvende eventuelle optagede billeder, men udelukkende med henblik på de formål, som søges opnået med den pågældende videoovervågning, eller med henblik på vedligeholdelse af det relevante udstyr for at kontrollere, at det fungerer korrekt. Dette kan alternativt foregå på basis enten af en registrerets anmodning om indsigt eller en afgørelse fra politiet eller en domstol med henblik på bekæmpelse af kriminalitet. Når videoovervågningen kun har til formål at forebygge, afsløre eller kontrollere lovovertrædelser, kan det i mange tilfælde være en god løsning at anvende to adgangsnøgler, hvoraf den ene opbevares af den registeransvarlige og den anden af politiet, for at sikre, at billederne kun ses af politiet og ikke af uautoriseret personale, uden at dette dog berører den registreredes legitime ret til indsigt, som kan gøres gældende i den korte billedforvaringsperiode.

b) Der skal træffes passende sikkerhedsforanstaltninger for at undgå situationer som beskrevet i direktivets artikel 17, herunder spredning af oplysninger, som kan være nyttige til at beskytte den registreredes, tredjemands eller den registeransvarliges rettigheder, også med henblik på

¹⁶ Såkaldt « lagdelt » fremgangsmåde.

at forebygge manipulation, ændring eller tilintetgørelse af data og andre tilknyttede elementer, der kan tjene som bevismateriale.

c) Kvaliteten af de billeder, der optages, har ligeledes afgørende betydning, især hvis det samme optagelsesmedie anvendes gentagne gange, hvilket medfører en risiko for, at tidligere billeder ikke slettes fuldstændigt.

d) Endelig er det afgørende, at de operatører, der udfører de pågældende videoovervågningsaktiviteter, har modtaget en passende uddannelse og er bekendt med de foranstaltninger, der skal træffes for at opfylde de gældende krav. Det kan ligeledes være nyttigt at uddanne kontrollører og operatører med udgangspunkt i de konkrete risici og de metoder, der kan anvendes til at identificere de filmede personer.

H) De registreredes rettigheder

Det er ikke fordi, at de indsamlede personoplysninger er af en særlig karakter, at de registrerede ikke kan påberåbe sig deres rettigheder i henhold til direktivets artikel 13 og 14, særlig med hensyn til retten til indsigelse mod behandling.

Direktiv 95/46 giver således de registrerede mulighed for til enhver tid at gøre indsigelse mod behandlingen af deres personoplysninger¹⁷ af vægtige legitime grunde, der vedrører de pågældendes særlige situation. De registreredes ret til privatlivsbeskyttelse og den som regel korte forvaringsperiode, der gælder for billeddata, indskrænker anvendelsesområdet for de registreredes ret til indsigt i de personoplysninger, som gør dem identificerbare, men denne ret skal dog beskyttes, særlig hvis der fremsættes en detaljeret anmodning, således at de relevante billeder nemt kan findes frem. Der skal også tages højde for, at tredjemands rettigheder midlertidigt skal beskyttes.

Enhver begrænsning under henvisning til, at det er et stort arbejde at finde de relevante billeder frem, når dette arbejde med hensyn til søgning, udgifter og ressourcer helt klart i betragtning af den korte forvaringsperiode ikke står i forhold til formålet, skal fastsættes i den sekundære lovgivning (se direktivets artikel 13, stk. 1) under hensyntagen til de registreredes ret til forsvar i forbindelse med særlige begivenheder, som måtte have fundet sted i den pågældende periode.

I) Supplerende beskyttelsesforanstaltninger i forbindelse med specifikke behandlinger

Det skal være forbudt at foretage videoovervågning baseret udelukkende på de pågældende personers racemæssige baggrund, religiøse eller politiske overbevisning, fagforeningsmæssigt tilhørsforhold eller seksuelle forhold (direktivets artikel 8).

Uden at ville fastsætte en udtømmende liste over de mangfoldige anvendelser af videoovervågning ønsker gruppen dog at understrege, at det er nødvendigt – i princippet og i givet fald inden for rammerne af den forudgående kontrol af behandlinger som fastsat i direktivets artikel 20 - i højere grad at være opmærksom på visse situationer, hvor billeder vedrørende identificerede eller identificerbare personer indsamles, eftersom disse situationer skal vurderes på sag-til-sag-basis.

¹⁷ Medmindre andet er fastsat i den nationale lovgivning.

Der henvises især til følgende situationer, der bygger på erfaringer og/eller igangværende forsøg:

- a) permanent sammenkobling af videoovervågningssystemer, der styres af forskellige registeransvarlige,
- b) mulig associering af billeddata og biometriske data, herunder fingeraftryk (f.eks. ved indgangen til banker),
- c) anvendelse af stemmeidentifikationssystemer,
- d) oprettelse - i overensstemmelse med proportionalitetsprincippet og i medfør af specifikke bestemmelser - af systemer til indeksering af optagede billeder og/eller systemer til øjeblikkelig automatisk hentning, især ved hjælp af identifikationsdata,
- e) anvendelse af ansigtsgenkendelsessystemer, som ikke er begrænset til at identificerede forklædte personer i transit, f.eks. personer med falsk skæg eller paryk, men som har til formål at opdage mistænkte lovovertrædere, f.eks. systemer, der automatisk identificerer visse personer på grundlag af modeller og/eller standardidentitetsmønstre, der bygger på visse ydre træk (herunder en persons hudfarve, øjne, udstående kindben osv.), eller på en foruddefineret unormal adfærd (pludselige bevægelser, gentagen transit selv med et bestemt interval, måden, hvorpå et køretøj bliver parkeret, osv.). Det er i denne forbindelse nødvendigt, at systemet er menneskestøttet, især i lyset af de mulige fejl, der kan opstå i disse situationer, hvilket ligeledes gælder litra f) nedenfor,
- f) mulighed for automatisk at følge en rute eller et spor og/eller rekonstruere eller forudse en persons adfærd,
- g) edb-støttet beslutningstagning på grundlag af en persons profil eller intelligente analyse- og interventionssystemer uafhængigt af standardalarmer, herunder adgang til et sted uden den nødvendige identifikation eller en brandalarm.

8. VIDEOOVERVÅGNING I ET ANSÆTTelsesFORHOLD

Gruppen har allerede i sin *udtalelse nr. 8/2001 om behandling af personoplysninger i ansættelsesforhold*, der blev vedtaget den 13. september 2001, og sit *arbejdsdokument om overvågningen af elektronisk kommunikation på arbejdspladsen*, der blev vedtaget den 29. maj 2002, i mere generelle vendinger gjort opmærksom på nogle enkelte principper, der har til formål at sikre de registreredes rettigheder, frihed og værdighed i et ansættelsesforhold.

Det er ud over betragtningerne i ovennævnte dokumenter og i det omfang, at de finder anvendelse på videoovervågning, passende at pointere, at videoovervågningssystemer, der har til direkte formål på afstand at kontrollere kvaliteten og mængden af det arbejde, der udføres, hvilket således medfører behandling af personoplysninger, generelt skal være forbudt. Det forholder sig dog anderledes med videoovervågningssystemer, der med forbehold af passende garantier, anvendes til at opfylde visse erhvervsmæssige beskyttelseskrav, og som - selv indirekte - medfører distanceovervågning¹⁸.

Erfaringerne har desuden vist, at overvågningen ikke skal omfatte lokaliteter, der enten er forbeholdt de ansattes privatliv eller ikke er beregnet til nogen erhvervsaktivitet, herunder toiletter, brusebade, omklædningsrum og fritidsrum, at billeddata, der udelukkende indsamles

¹⁸ Ud over betragtningerne i dette dokument skal der i disse situationer også tages specifikt højde for, at det er nødvendigt at overholde rettigheder, der er fastsat i kollektive aftaler, hvilket til tider bygger på kollektive oplysninger til de ansatte og/eller deres respektive fagforeninger, dvs. ud over de oplysninger, der skal gives på individuel basis i henhold til databeskyttelseslovgivningen. Der skal i andre situationer indhentes forudgående tilladelse fra de ansattes repræsentanter eller fagforeninger til installation af udstyr, også med hensyn til overvågningsvarighed og andre optagelsesforanstaltninger. Det kan i visse lande være nødvendigt, at myndighederne griber ind, hvis der ikke der ikke opnås enighed mellem parterne.

med henblik på ejendomsbeskyttelse og/eller afsløring, forebyggelse og kontrol af alvorlige overtrædelser, ikke må anvendes til at anklage en ansat for mindre disiplinære overtrædelser, og at de ansatte altid skal have mulighed for at fremsætte modkrav ved hjælp af de indsamlede billeddata.

De ansatte og enhver anden person, der arbejder på stedet, skal informeres. Denne information skal omfatte navnet på den registeransvarlige og formålet med overvågningen samt andre oplysninger, der er nødvendige til at sikre en rimelig behandling i forhold til den registrerede, f.eks. i hvilke tilfælde virksomhedens ledelse vil se optagelserne igennem, opbevarelsesperioden, samt hvornår optagelserne videregives til de retshåndhævende myndigheder. Informering ved hjælp af symboler anses ikke for at være tilstrækkelig i et ansættelsesforhold.

4 Vurdering av dagens situasjon i Norge

Oslo sies, som tidligere nevnt, å være en av de mest kameraovervåkede byene i Europa. Enkelte aktører presser på for å overvåke stadig nye områder. En begrunnelse ligger i kriminalitetsforbygging og en annen er terrorbekjempelse. Vurderingene kjennetegnes imidlertid gjennomgående ved at de er foretatt av private rettssubjekter uten særskilt kunnskap om nytten av slik overvåking. Det vises i den sammenheng til forskning på området som omtalt tidligere i dette dokumentet. Sikkerhetsmyndighetene har for øvrig ikke fremmet anførsler om at det er behov for ytterligere kameraovervåking for å motvirke mulighetene for terroranslag i Norge.

I den grad dagens situasjon ikke fremstår som ideell, kan det være grunn til å anta at regelverket utgjør et ikke uvesentlig element i dette

4.1 Utdrag av noen av Datatilsynet avgjørelser:

Overvåking på kollektivtransportmidler

NSB 2004/894

Sporsveisbussene 2004/915

Datatilsynet har godtatt at det kan benyttes kamera i sjåførområdet og mot inngangspartiene. Dette for å ivareta sjåførens og de reisendes sikkerhet.

Det er uenighet om de reisende på busser og togsett også skal kunne kameraovervåkes på passasjerområdet/ i kupeen. Personvernemnda vil forhåpentligvis ta stilling til spørsmålet i løpet av 2006.

Overvåking av svømmeanlegg

Grottebadet 2003/1497

10 kameraer med formål å overvåke bassenget kombinert med badevaktfunksjon. Det ble ved vurderingen av tiltaket lagt vesentlig vekt på argumentet om ivaretagelse av liv og helse. Datatilsynet har akseptert at det kan være nødvendig med kameraovervåking for å ivareta de badendes sikkerhet i et badeanlegg.

Overvåking av venterom på legevakt

Florø sykehus 2005/78

Tilsynet aksepterte overvåkingen. Det ble vektlagt at overvåkingen kun skulle foretas for å sikre pasientenes liv eller helse mens de oppholder seg i venterommet, at området ikke er

bemannet med vakt, og at det kun gjelder monitorering, ikke lagring av bilder. Det ble også vektlagt at bildene kun skal være tilgjengelige for vakthavende personell.

Toaletter

Steen & Strøm Tønsberg 2002/2228

Overvåking av toalettets fellesareal foran "båsene" for å forhindre hærverk ble ikke akseptert. Virksomheten har også benyttet vektere, men det ble anført at dette ikke var tilstrekkelig. Den økonomiske interessen i å begrense hærverk ble ikke ansett å overstige den enkeltes krav på integritetsvern.

Overvåking av eksamenslokaler

2005/82 Biltilsynet Tønsberg

Overvåking av kandidater som avlegger teoriprøve for førerkort. Datatilsynet fant at det ikke forelå noen berettiget interesse. Tilsynets praksis er at kameraovervåking kun kan settes i gang for å ivareta hensynet til liv og helse, samt hensynet til forebygging av straffbare handlinger. Manglende personellressurser anses følgelig ikke som tungtveiende nok i praksis. Datatilsynet uttaler at man er skeptisk til en potensiell utvikling der menneskelige ressurser erstattes av overvåkingskameraer.

Utesteder (restauranter, barer, nattklubber o.l.)

Hotell Plaza 2002/401 (behandlet i Personvernemnda)

Dette er steder hvor publikum normalt har en ekstra forventning om diskresjon. De opplysningene som registreres vil kunne være svært følsomme for den enkelte, selv om de ikke er sensitive i lovens forstand. Samtidig vil virksomheten ha en berettiget interesse i å ivareta de ansattes helse og sikkerhet, særlig mot alkoholpåvirkede gjester. Det må foretas en konkret vurdering. Praksis viser at hensynet til publikums integritetsvern ofte vil veie tyngst, slik at kameraovervåking ikke er tillatt.

CSS Norway AS

2002/1018

Kameraovervåking med et overvåkingsutstyr som aktiveres kun etter spesielt definerte tungtveiende behov (f. eks truende situasjoner) vil allikevel kunne være tillatt.
(Datatilsynets svar på en generell henvendelse)

Arbeidsplass

Leatherman /Pina Colada Oslo AS i Byporten

2003/1126

I butikken er det installert et WEB-kamera, hvor kjedens ledelse kan logge seg på sentralt og følge de ansattes daglige arbeid. Tilsynet fattet i 2003 et vedtak med pålegg mot *Leatherman* om opphør av overvåkingen. Butikken har nå navnet *Pina Colada*. Det er imidlertid de samme eierne, og WEB-kameraovervåkingen er opprettholdt.

DnB NOR

2005/36

I november 2003 ble det utlevert et opptak fra en ansatt i DnB Nor Bank ASA til ISS Norge AS, som var ansvarlig for renholdet av bankens lokaler. Formålet med utleveringen var å fastslå og dokumentere manglende leveranse med hensyn til vask av banklokalet. Den enkelte ISS-ansatte var identifiserbar på opptaket. Det forelå ikke gyldig samtykke fra den avbildede til utlevering av opptaket, og heller ingen lovhjemlet adgang til utlevering.

Den norske Eterfabrikk
2005/1194

Politi og ulike sikkerhetsselskaper har utpekt virksomheten som særlig utsatt for anslag utenfra. Overvåking av produksjonsrom hvor det på kampanjebasis produseres metadon. To ansatte oppholder seg i dette rommet, men hvilke to varierer. Det skjer både opptak og overvåking i sanntid, og et spørsmål er om direktøren skal ha en tilgang til bildene i sanntid kontinuerlig eller bare ved en alarmsituasjon.

Baste Fosen

Kommunal overvåking
2004/1809

Kameraovervåking i Bryne sentrum. Installasjon av tre kameraer, to i Bryne sentrum og ett på Bryne stasjon. Overvåkingen skjer i samarbeid med politiet og Jernbaneverket. Formålet er å forebygge kriminalitet og sikre dokumentasjon til bruk i straffesaker. Kommunen har opplyst at det er om lag 40 voldssaker i området i løpet av ett år.

4.2 Noen problemer ved gjeldende regulering

Reglene om fjernsynsovervåking er i dag skilt ut i et eget kapittel for å sikre bedre oversiktighet på et praktisk viktig område, jf. Ot. prp 92, side 130. Reguleringen i personopplysningslovens kapittel VII, kan imidlertid fremstå som noe uklar. Dette skyldes dels blandingen av spesifikke bestemmelser (f. eks §§ 39 og 40), med generelle bestemmelser (f.eks § 38), dels på grunn av henvisningen til lovens alminnelige bestemmelser (f.eks §§ 8 og 9). Også skillet mellom reguleringsformene i henholdsvis lov og forskrift kan fremstå som en pedagogisk utfordring, primært da hvilke bestemmelser som er valgt inntatt i loven og hvilke i forskriften.

En mulighet for å gjøre dette klarere kan være at formen for overvåking bare reguleres ett sted, eksempelvis i et eget kapittel eller i forskrift. I den sammenheng kan det vurderes å tilføye en setning i personopplysningslovens § 3 (saklig virkeområde) om at kameraovervåking reguleres særskilt.

4.2.1 Skjønnsmessige vurderinger

En årsak til kameratettheten i Norge kan være hvordan det rettslige grunnlag for behandlingen (overvåkingen) er regulert. Personopplysningslovens § 37 viser i dagens utforming til §§ 8 og 9. Det mest praktiske behandlingsgrunnlaget er § 8, f. Bestemmelsen er meget skjønnsmessig utformet, og medfører ofte fortolkningsproblemer. Av den grunn ligger det en problematikk i at fjernsynsovervåking i dag kun er meldepliktig, og at det er den behandlingsansvarlige selv som i første omgang må foreta en objektiv vurdering av de interessene som § 8, f henviser til. Det er ikke unaturlig å anta at denne vurderingen i praksis vil kunne bli subjektiv, all den tid den behandlingsansvarlige har en egeninteresse i overvåkingen.

Et annet problem med det vurderingstema § 8, bokstav f, henviser til, er at det ikke er spesielt klart hva som ligger i vilkårene ”berettiget interesse” og ”den registrertes personvern”. Dette er i og for seg vanlig lovgivningsteknikk, men manglende konkretisering på dette praktisk viktige området kan fremstå som uheldig. Datatilsynets praksis fremstår i dag som hovedrettskilden i forhold til vurderingen av § 8 f, noe som er problematisk når den behandlingsansvarlige selv skal fortolke og anvende bestemmelsen ”i første omgang”.

Skjønnsmessige vurderingstema setter også begrensninger mht. straffesanksjoner.

Det bør vurderes om det er hensiktsmessig å spesifisere bestemmelsene i større grad, særlig i forhold til det rettslige grunlaget for fjernsynsovervåking. Spesifisering er i tråd med intensjonen om oversiktighet, men lovteknisk vil det være en utfordring å ivareta de ulike formål og de store forskjellene i behandlingsansvarliges virkeområde og størrelse. Særlig regulering vil antagelig være mest hensiktsmessig fremkommer i forskrift (enten egen forskrift eller med eget uttømmende kapittel i eksisterende personopplysningsforskrift).

Behovet for uttømmende særregulering inntatt ett sted, vil antagelig kunne bli enda større dersom kommunene får overført kompetanse på området, se for øvrig Justisdepartementets høringsbrev av 07.03.2005.

4.2.2 Behandlingsansvar

Etter personopplysningsloven er det den behandlingsansvarlige, dvs overvåkeren, som har det juridiske ansvaret for å påse at lovens regler overholdes. Leverandører av utstyret som anvendes, har i så måte intet ansvar for å påse at overvåkeren benytter det på en lovlig måte. Etter det Datatilsynet kjenner til, finnes det heller ingen godkjenningsordninger for leverandører eller utstyr.

Selv om produsenter og leverandører av slikt utstyr ikke kan pålegges plikter etter personopplysningsloven, kan det likevel være en fordel om disse øker sin kunnskap om regelverket rundt kameraovervåking. På den måten kan de bidra til å påvirke sine kunder og opplyse dem om regelverket rundt overvåkingen. Samtidig kan de legge opp til tekniske løsninger som gjør at personvernet ivaretas på en best mulig måte ut fra forholdene. Det må forutsettes at de fleste aktørene på markedet ønsker å opptre seriøst, og bransjen har også signalisert at de ønsker å heve sin kompetanse på området.

5 Forslag til endringer

Det kan være behov for noe skjerpet kontroll med kameraovervåking, særlig synes det å være behov for et strengere regime på områder der det ikke finnes noe alternative områder å oppholde seg. Omfanget av kameraovervåking øker jevnt og dukker opp i stadig nye sammenhenger. Diskusjonen om overvåking i kollektivtransportmidler er ett av flere eksempler på dette. Kameraovervåking oppfattes i mange sammenhenger som en sikkerhet mot kriminalitet. At det også utgjør en trussel mot personvernet er ikke like fremtredende i folks bevissthet.

Vissheten om at man overvåkes i stadig flere situasjoner i løpet av en vanlig dag, kan i seg selv oppleves som belastende og inngripende. Utgangspunktet må være at hvis vi ikke har gjort noe galt, så skal vi heller ikke oppleve den last det er å vite at andre har tilgang på en video som beskriver våre handlinger, i en gitt situasjon, visuelt.

5.1 Teknisk utvikling

Det tekniske utviklingen har vært akselererende de siste årene. Det har skjedd en betydelig kvalitetsheving av opptakene, samtidig som prisene på utstyret har falt drastisk. Kvalitetshevingen gjelder både dag -og nattfilming, og har gitt muligheter for meget gode

optiske zoomingsmuligheter. Det kan også installeres automatisk zoom og alarm av objekt ved bevegelse. Hevingen av bildekvaliteten har også gjort ansiktsgjenkjenning/biometri lettere tilgjengelig og bedre å bruke. Mulighetene for lydopptak i tilknytning til det ordinære billedkvaliteten har også blitt bedre.

Digital lagring av opptakene krever andre løsninger for at sletting av opptakene skal være reell. Systemene må innrettes slik at "slettede" data ikke kan hentes frem igjen. I praksis må lagringsplassen overskrives.

5.2 Fra fjernsynsovervåking til kameraovervåking

Termen fjernsynsovervåking som benyttes i dagens personopplysningslov fremstår som "gammeldags" og ikke inkluderende nok. Kameraovervåking er et mer dekkende begrep. Det bør heller ikke være krav om at kameraet skal være fastmontert, da det avgjørende må være formålet med overvåkingen og hvor inngripende denne er. Et eksempel kan være flyttbart web-kamera.

Begrepet bør tydelig omfatte for eksempel forsikringsselskaper som måtte ønske å foreta bevissikring (såkalt videobevis), og overvåking ved hjelp av ordinært håndholdt (digitalt) fotoapparat. Forsikringsbransjen har gjentatte ganger fremmet ønske om å utøve skjult overvåking av forsikringstakere de mistenker for forsikringssvindel knyttet til uførhet og lignende. Måten dette ønskes gjennomført på er at representanter for selskapet, i det skjulte, fotfølger de mistenkte og filmer/tar bilder av disse hvis de utfører handlinger de har oppgitt at de ikke kan klare.

5.3 Behandlingsgrunnlag

Det bør vurderes særskilt regulering av det praktisk viktigste behandlingsgrunnlaget på området (§ 8, f), der det fremkommer mer uttømmende hvilke interesser som skal vernes (liv, helse, kriminalitetsforebygging). En slik reguleringsform er valgt i den svenske loven om allmenn kameraovervåking (1998-04-02), jf. § 6.

Videre bør det vurderes ytterligere presisering av det strengere kravet om "særskilt behov" for overvåking av områder der en begrenset krets ferdes. De samme hensyn gjør seg gjeldene her. I denne sammenheng vil det kanskje også være naturlig å se nærmere på hvor integritetstrusselen faktisk er størst. Kan det være naturlig med andre skillelinjer enn offentlig sted og der en begrenset krets jevnlig ferdes? Bør det tenkes i retning av områder der forventningen om ikke å bli overvåket er størst, så som offentlig rom begrenset til friluft, offentlig vei, badestrender, skog og mark, annens eiendom? I tillegg til særskilt regulering av arbeidsplass.

Uansett kan det være naturlig med en presisering av at overvåking av områder, der forventningen om diskresjon normalt er høy, ikke skal forekomme.

Presisering av nødvendighetskravet kan fremkomme i samme bestemmelse. Gode grunner taler for å kalle bestemmelsen noe annet enn "vilkår for å behandle personopplysninger" eller "behandlingsgrunnlag". Bestemmelsen kan utformes på en slik måte at det tydelig fremkommer at kameraovervåking som hovedregel er ulovlig, og at det er overvåkingen som krever rettslige grunnlag, ikke retten til å være fri fra overvåking. Viser igjen til nevnte svenske lovs § 6.

5.4 Proporsjonalitet

Kravet til proporsjonalitet er et grunnleggende prinsipp knyttet til menneskerettighetene. Kravet kan utledes i tre kriterier:

- Formålet med tiltaket må være tilstrekkelig viktig til å berettigje avvik fra en grunnleggende rettighet
- Tiltaket må være egnet til å nå dette formålet
- Tiltaket må være nødvendig for å nå formålet

Prinsippet er av stor viktighet også når det gjelder kameraovervåking, og innebærer at det også må legges til grunn:

- at det overveies om det ønskede formål kan nås med mindre inngripende midler enn kameraovervåking og registrering,
- at overvåking skal gjennomføres på en måte som virker minst mulig integritetskrenkende for den alminnelige borger,
- at kameraovervåking av områder hvor det er adgang for alminnelig ferdsel, herunder eksempelvis vei- og parkeringsarealer, unnlates,
- at opptak slettes innen en kort periode og
- særlig for så vidt angår opptak som inneholder opplysninger om straffbare forhold, må det være begrenset til kortvarig oppbevaring med henblikk på politianmeldelse, som må gjøres snarest mulig. Opptakene skal avleveres til politiet i forbindelse med anmeldelsen og slettes fra egne systemer umiddelbart deretter.

Antallet kameraer, vinkling og hvor disse er plassert er også av betydning i proporsjonalitetsvurderingen. I Datatilsynets avgjørelser om kameraovervåking i kollektivtransporten, var proporsjonalitetsprinsippet en viktig faktor for begrensninger i overvåkingen.

Det stilles krav til "særskilt behov" ved overvåking der en begrenset krets av personer ferdes. "Butikk –og fellesområdene" i de fleste butikker, kjøpesentre, stormagasiner etc. anses ikke som områder der begrenset krets av personer ferdes. Det gjør imidlertid pauserom, garderober med mer. Skillet kan også sies å ha grunnlag i proporsjonalitetsvurderinger.

Viktigheten av å ivareta proporsjonalitetshensynet kommer særlig på spissen når man ser det totale omfanget av kameraovervåkingen i sammenheng.

Kvaliteten på deler av kameraene er så dårlig at de er til liten hjelp. Gjelder særlig gamle analoge systemer, eksempelvis opptakene under ranet av Munch-museet i 2004.

5.5 Sondre mellom opptak og monitorering

Det bør presiseres at bestemmelsene gjelder både monitorering og opptak. Men likevel bør det kanskje også sondres mellom de to overvåkingsformer i mange sammenhenger, fordi personvernetrusselen vil være noe forskjellig, jf. proporsjonalitetsprinsippet. Det kan imidlertid stilles spørsmål ved om "bare" monitorering vil være aktuelt i fremtiden, når overvåkingen stort sett vil foretas ved hjelp av digitale løsninger.

5.6 Skillet mellom analoge og digitale system

Gjeldende lovgivning (jf. § 37, jf. § 3) har i praksis blitt oppfattet å skille mellom analog og digital kameraovervåking. Dette er basert på en vurdering av gjenfinningskriteriet. Et slikt skille er imidlertid ikke praktisk. Korte slettefrister (jf. forskriftens § 8-4) bidrar til at gjenfinningskriteriet ofte vil være oppfylt også for analoge systemer.

Dagens teknologi legger videre til rette for at en konvertering fra analoge til digitale opptak med letthet kan gjøres, og at skillet mellom disse teknologiene i hovedsak begrenses til hvilken bearbeiding som kan gjøres samtidig (realtime). Analoge systemer har også kapasitet for enkel bearbeiding, klassisk bevegelsesdeteksjon har i lang tid vært realisert også i analoge systemer.

Det foreslås derfor at et slikt skille ikke viderefører. Gjeldende regulering, § 37, fremstår i dag som uklar, og analoge opptak er langt på vei i ferd med å bli erstattet av digitale systemer. Av det totale salget i 2004 utgjorde de analoge systemene bare 1%.

Det faktum at de fleste opptak i dag gjøres digitalt, og at de analoge lett kan digitaliseres, må tas med i vurderingen av hvilket inngrep fjernsynsovervåking representerer i personvernet. Det nevnes her løsninger for systematisering og analyse av billedopptak. I tillegg må spredningsfaren (spredingslettetheten) tas med i en totalvurdering.

5.7 Melde- og konsesjonsplikt

Det bør fremkomme klarere at hovedregelen er meldeplikt. Lovens nåværende utforming pålegger, med enkelte unntak i §§ 36-37, konsesjonsplikt der det registreres sensitive personopplysninger. Det er imidlertid et område Datatilsynet har utstedt et begrenset antall konsesjoner. Det kan være naturlig at eventuell konsesjonsplikt for overvåkingstiltak som registrerer sensitive opplysninger, kommer klarere til uttrykk. Det er ikke tilstrekkelig med unntaket etter § 37, 2. ledd, 2. pkt., hvor § 2, nr. 8 bokstav b unntas.

Meldesystemet har i dagens utforming en begrenset funksjon. Dette har ikke bare sammenheng med at det antagelig er en meget stor underrapportering fra de behandlingsansvarlige. Det kan tenkes at kameraovervåking bør underlegges en særskilt meldeordning, hvor for eksempel antallet kameraer og om disse er plassert på ulike geografiske steder kan fremgå. Det vil gi Datatilsynet en bedre oversikt over den totale fjernsynsovervåkingen i samfunnet, og således være bedre i samsvar med direktivets intensjoner.

En annen mulighet er at eventuell overvåking registreres i andre offentlige registre, hvor virksomhetene allerede er registrert. En slik løsning vil kunne ivareta Datatilsynets behov for oversikt, samtidig som de næringsdrivende vil kunne sende ett skjema mindre til offentlige myndigheter. Det såkalte GAB-registeret (grunneiendommer, adresse- og bygningsregisteret) kan være et alternativ. Registrering knyttet til eiendom kan på den annen side vise seg kompliserende, da eiendomretten og behandleransvaret ikke nødvendigvis vil være sammenfallende.

Et mer strikt regime for meldinger kan være en kontrollmekanisme. Eventuelt vil innføring av en form for lisensavgift også kunne ha en begrensende funksjon. Overvåking vil ved en slik løsning gjøres til en økonomisk kostnad, som kan vurderes mot antatt nytteverdi.

Det kan også tenkes en løsning med innføring av krav om en særskilt form for "internkontroll" som må gjennomføres før overvåkingen kan påbegynnes. Behandlingsansvarlige kan på denne måten pålegges å gjennomgå en intern prosess som i større grad vil kunne sikre at overvåkingen skjer i samsvar med regelverket.

Videre kan det vurderes om det bør innføres konsesjonsplikt, eller andre særlige godkjenningssløsninger, dersom biometrisk gjenkjenning eller bearbeiding ønskes tatt i bruk. Tilsvarende kan vurderes for lydopptak i forbindelse med kameraovervåking, i den grad lydopptak ikke vil være i strid med straffeloven § 145a. På den annen side vil virkningene av slik plikt kanskje være begrenset, all den tid Datatilsynet uansett har muligheter til å prøve behandlingsansvarliges saklighetsvurdering. For øvrig skal det legges en strengere vurderingsnorm til grunn desto sterkere personvern hensyn som gjør seg gjeldende i forbindelse med den aktuelle overvåkingen. Datatilsynet kan samtidig sette de vilkårene som er nødvendige for at lovens krav skal være oppfylt.

Datatilsynet bør imidlertid følge utviklingen nøye og evaluere behovet for konsesjonsplikt.

5.8 Sikring av billedopptak

Det stilles ikke detaljerte krav om hvordan sikringen skal utføres, men at den skal være forholdsmessig, jf. personopplysningsloven § 13. Det vil si at de sikkerhetstiltak som iverksettes for en overvåkingssentral normalt vil være strengere enn de tiltak som iverksettes for et enkeltstående anlegg.

Dagens regulering av informasjonssikkerhet skjer etter den generelle sikkerhetsbestemmelsen i personopplysningslovens § 13, enten ved at denne gjelder etter § 37, eller at den gjøres gjeldende etter personopplysningsforskriftens § 8-2.

Slik reguleringen fremstår i dag ender man uansett opp i den generelle informasjonssikkerhetsbestemmeslen i loven. Etter Datatilsynets syn, bør denne til en hver tid gjelde. Det er her et vurderingskriterie om informasjonssikkerhet er nødvendig, hvilket det for lovens definisjon av fjernsynsovervåking, vil være. Eventuell særregulering bør legges på forskriftsnivå. Det bemerkes at den systematiske fremgangsmåte etter personopplysningsforskriftens 2. kapittel klart er relevant for større, nettverksbaserte overvåkningssystemer, og for datatbehandlere (vaktentraler) som behandler overvåkningsdata fra flere behandlingsansvarlige.

Det er imidlertid klart at mindre, isolerte systemer trenger særregulering, eventuelt klar veiledning for å tilfredstille regelverket for informasjonssikkerhet. Dette eksemplifiseres her ved utdrag fra veiledningsmateriale:

Oppbevaring av informasjonen må være sikker. Opptak på filmruller, videobånd, CD-plater eller lignende oppbevares normalt i et låst skap der tilgangen er styrt av den sikkerhetsansvarlige. Opptakene er konfidensielle, og kun de som har behov for det skal ha tilgang til dem.

Sikring av systemer for digital kameraovervåking

1. De samme forventningene til sikring gjelder for digitale kameraovervåkingssystemer, men her er det ytterligere utfordringer. Tilgangen til opptakene må sikres både fra datamaskinen de er lagret på og fra eventuelt tilknyttede nettverk, overføringen av

bilder mellom kamera og sentralt utstyr må sikres, og kravene til sletting må være ivarettatt av løsningen. Teknologien gjør det enkelt å misbruke denne typen opptak ved å for eksempel legge bilder ut på nett eller sende opptakene via e-post. Det er derfor her svært viktig at tilgangen er begrenset til de daglig ansvarlige for å forminske mulighetene for misbruk.

2. Informasjonssystemet skal sikres på bakgrunn av en vurdering foretatt av den behandlingsansvarlige. Datatilsynet kan overprøve vurderingen.
3. Systemet må ivareta slettekravet. Det er viktig at slettingen er reell, noe som innebærer at data overskrives. Dette gjelder også ved utfasing av utstyr.
4. Kun autorisert personell skal ha tilgang på tjenesten. Tilgang må sikres, og bruken av dette skal loggføres. Tilgangen til bildeopptak bør sikres bedre enn brukernavn og passord dersom det blir gitt tilgang til disse utenfor eget nettverk.
5. Dersom tjenesten gjøres tilgjengelig over nettverk utenfor den ansvarliges kontroll bør kryptering benyttes for å sikre dataene. Dette gjelder både mellom kamera og sentralt utstyr, og mellom sentralt utstyr og brukeren.

5.9 Web-kamera

Begrepet WEB-kamera spenner fra enkle innretninger beregnet for private formål til profesjonelle installasjoner lagt til rette for publikums tilgang over Internett. Eksempelvis nevnes her privat kamera til bruk sammen med PC for å føre videosamtaler, og kamera tilgjengelig over Internett for å gi publikum en oversikt over Aker Brygge i Oslo.

Hvorvidt et kamera kommer inn under loven eller ikke avhenger av bruken av det, hvoviddt det benevnes som WEB-kamera eller ikke er irrelevant. Vurderingskriteriene er her privat bruk, og hvorvidt enkeltperson kan identifiseres. Med denne bakgrunn er det ikke hensiktsmessig å omtale WEB-kamera konkret.

Bruken av disse fortjener imidlertid en vurdering, da kvaliteten og mulighetene disse gir medfører at de faller inn under lovens virkeområde, selv om dette nødvendigvis er intensjonene for de som tar slike kamera i bruk.

Eksempelvis er web-kamera er plassert på en rekke byggeplasser, og alle kan følge byggeprosessen til enhver tid. Mange aviser har kamera plassert sentrale steder i Norge, som muliggjør at publikum kan følge vær -og bybilde, eller en badestrand. I den grad overvåking innebærer at bildene blir tilgjengelige på Internett, har Datatilsynet stilt krav om det ikke skal være mulig å kjenne igjen enkeltpersoner, eller at det innhentes samtykke fra hver enkelt.

Datatilsynet har også eksempler hvor slike kamera har blitt benyttet til klare overvåkningsformål. Dette både i sikret form og usikret(tilgjengelig for enhver), samt at episoder hvor dette har vært benyttet både som skjult overvåking, og som direkte overvåking av ansattes oppførsel.

5.10 Forskjell mellom offentlig og privat overvåking – og overvåkingssentraler

I all hovedsak er det (mindre) private aktører som bedriver kameraovervåking. Overvåkingen er fysisk begrenset til et område, med et begrenset antall personer, noe som igjen innebærer mindre risiko for sammenstilling og misbruk. Det er imidlertid en tendens til at private selskaper i større grad tilbyr løsninger med overvåkingssentraler. Dette kan være internt på et kjøpesenter eller eksternt hos et vaktelskap. På denne måten kontrollerer en liten gruppe personer områder hvor mange tusen mennesker ferdes til enhver tid, og i en geografisk utstrekning på mange kvadratkilometer. Personverntrusselen blir på denne måten større enn når flere små aktører overvåker hvert sitt begrensede område.

Overvåkningspotensialet slike sentraler (vaktelskaper) har fått bygget opp, overgår det man ville ha akseptert for eksempelvis politiet. Det er også grunn til å stille spørsmål om hvor bevisst disse sentralene er i forholdet mellom rollen behandlingsansvarlig og databehandler.

Videre ser vi en utvikling hvor offentlige myndigheter i stadig større grad mener å ha behov for å overvåke borgerne innen større eller mindre geografiske enheter. Politiet i Oslo har eksempelvis installert et kamera på Oslo sentralstasjon med god oppløsning og meget stor rekkevidde. Tiltaket innebærer et misbruks –og overvåkningspotensiale langt ut over det tradisjonelle. Videre er det også stadig flere kommuner som ønsker å overvåke det offentlige rom for å forebygge hærverk og "bråk". Det synes som om en stor andel av norske kommuner allerede har slike overvåkingsløsninger.

5.11 Biometri/gjenkjenningsteknologi/digital bearbeiding

Moderne overvåkingssystemer som benytter ulike former for digital bearbeiding har en klar grensedragning mot biometri. Grensedragning er ikke klar, og det fremstår som nødvendig å avklare når man går utenfor "ordinær" fjernsynsovervåking etter regelverkets definisjoner, og over på annen behandling av personopplysninger som krever et eget behandlingsgrunnlag.

Datatilsynet har gitt uttrykk for at digital bearbeiding av opptakene, med formål å gjenkjenne personer eller gjenstander (som kjøretøy), i utgangspunktet ikke faller inn under lovens definisjon av fjernsynsovervåking. Særskilt grunnlag eller tillatelse kreves derfor for dette. Det er imidlertid denne muligheten som fremstår som det mest personverntruende elementet ved utviklingen.

Tilknytningen til mange digitale systemer som har dette potensialet er lett tilgjengelig. Et eksempel på hvilke muligheter som ligger i dette: "Kjøpesenteret har implementert en elektronisk vektor (E-vektor), i kameraovervåkingssystemet. E-vektoren sier fra til sine menneskelige kollegaer dersom mistenkelige personer sortert etter hudfarge, bærere av skolesekk og tidligere bekjenskaper med vaktelskapet eller lignende, går i nærheten av kosmetikkhyllene"

Bearbeiding av data kan gjøre at behandlingen av personopplysningene får et bredere omfang enn kameraovervåking.

- a. "Alarm" funksjoner ved aktivitet - som for analoge
- b. Stigmatiserende bearbeiding - Skolesekk i kosmetikkhylla / etnisk filter
- c. Gjenkjenningsteknologi. Søk etter tidligere uønskede kunder / vaktelskapets OBS-liste
- d. Kunden er ansvarlig for det vaktelskapet gjør

På Keflavik flyplass i Island er ansiktsgjenkjenningsteknologier i bruk.

Det bør vurderes om konsesjonsplikt er nødvendig for denne type bearbeiding av opplysninger fremskaffet ved kameraovervåking. Grensedragningen må ses i sammenheng av håndtering av biometri generelt i lovrevisjonen

5.12 Lydopptak

En tilleggsfunksjon ved mange overvåkingsløsninger som leveres i dag er lydopptak. I den grad muligheten faktisk benyttes, vil det imidlertid kunne rammes av forbud mot romavlytting i straffeloven 145a.

Norske banker og postkontor har i en årrekke foretatt lydopptak i tilknytning til kameraovervåkingen. Lydopptak skal imidlertid være begrenset til alarmsituasjoner. I hvilken grad dette eventuelt er i strid med straffeloven § 145a, har etter det Datatilsynet forstår ikke tidligere blitt problematisert. Det har heller ikke vært rettet spesielt fokus mot spørsmålet om varsling.

Lydopptak i tilknytning til ordinært bildcopptak endrer overvåkingens karakter. Det er ikke tvilsomt at personvernulempen øker betydelig ved at det også gjøres lydopptak. Utviklingen med at det i stadig større utstrekning tilbys, og selges, overvåkingssystemer med mulighet for lydopptak, gjør at dette bør utredes særskilt, herunder forholdet til straffeloven § 145a. Det fremstår i denne sammenheng som bemerkelsesverdig dersom private aktører skal ha vesentlig større adgang til å overvåke enn politiet.

5.13 Informasjon/varsling

Etter personopplysningsloven § 40 følger et absolutt krav om å varsle fjernsynsovervåking på offentlig sted eller sted hvor en begrenset krets av personer ferdes jevnlig. Loven oppstiller et forbud mot skjult overvåking. Ved skilting eller på annen måte skal det gå tydelig frem at stedet blir overvåket og hvem som er behandlingsansvarlig.

Det er Datatilsynets inntrykk, blant annet gjennom tilsynsvirksomhet, at varslingen generelt sett ikke er bra nok. Informasjon kan være vanskelig å få øye på, blant annet fordi den kan være vanskelig å skille fra ordinær reklame for vaktelskapene Securitas og Falck. For øvrig fremgår det sjelden av informasjonen hvem som er behandlingsansvarlig, og det er lett å få inntrykk av at det er vaktelskapet som er ansvarlig. Ofte er det også vanskelig å forstå hvilket kamera som tilhører hvilken virksomhet.

Det er viktig at befolkningen er klar over at de blir overvåket, og at det informeres om hvem som er ansvarlig for tiltaket. Uten slik informasjon blir den enkeltes mulighet til å benytte de øvrige rettighetene etter personopplysningsloven i stor grad illusorisk.

Varslingsbestemmelsen fremstår i seg selv som tilfredsstillende. Det kan imidlertid stilles spørsmål ved om den er egnet til å fange opp utviklingstrendene. Av varslingen bør det også fremgå hvor sterk overvåkingen er, herunder om det bare utføres monitorering, biometri (ansiktsgjenkjenning), lydopptak med mer. Det kan også tenkes løsninger med en form for lampe som lyser på kameraet når opptak foretas.

Ved at det informeres om hvor sterk overvåkingen er kan det tenkes løsninger med bruk av standardsymboler. Problemet med det er imidlertid at det for mange vil kunne enda

vanskeligere å forstå hva symbolene representerer, særlig hvis det benyttes flere (eks. monitorering, opptak, lyd, ansiktsgjenkjenning osv.). Slike symboler kan også tenkes benyttet sammen med tekst.

Bransjen vil her kunne gjøre et viktig opplysning/informasjonsarbeid ved kjøp/salg av utstyr.

5.14 Særlig bestemmelse om innsynsrett og utlevering

Utgangspunktet om innsynsrett etter personopplysningsloven § 18 nyanseres noe i personopplysningsforskriften § 8-5. Det er i alle tilfeller en forutsetning at det foretas opptak. For billedopptak som omfattes av personopplysningsloven § 37 annet ledd, dvs. opptak hvor det er mulig å finne igjen opplysninger om en bestemt person, gjelder innsynsretten etter § 18. I andre tilfeller kan den som det er gjort billedopptak av, kreve innsyn i billedopptakene hvor vedkommende er avbildet, dersom billedopptakene oppbevares ut over 7 dager.

Når det gjelder utlevering er det regulert i personopplysningsloven § 39. Utleveringsadgangen til andre enn behandlingsansvarlige er begrenset til situasjoner der den avbildede samtykker eller utleveringsadgangen følger av lov. Billedopptak kan likevel utleveres til politiet under nærmere angitte forutsetninger.

Innsyn i analoge opptak er et lite praktisk alternativ. Dette særlig fordi det forutsettes at den som gis innsyn, ikke skal gis innsyn i opptak av andre personer. Det er lettere, men ikke uproblematisk, å begrense utleveringen/innsynet til aktuelle personer ved bruk av digitale systemer.

Av konkrete eksempler hvor utlevering har skjedd, kan nevnes en kiosk-eier som utleverte opptak av en person, som feilaktig ble oppgitt å være Lotto-millionær, til TV2. Også politiet har utlevert opptak. Politiet laget i 2004 en niminutters videofilm bestående av opptak rundt den såkalte Plata. Filmen ble vist i lukkede fora, men også overlevert til NRK. En kortversjon av filmen ble vist av NRK, der en del av de avbildede personene var "sladdet". Imidlertid kunne flere av dem gjenkjennes. Både politimester Gjengedal og kringkastingssjef Bernander ble anmeldt grunnet visningen. Begge sakene ble imidlertid henlagt av Riksadvokaten den 31.10.2005, idet intet straffbart forhold var ansett bevist.

Personopplysningslovens §§ 39 og 40 bør videreføres inn i ny forskriftsregulering av kameraovervåking. Det samme bør eksisterende bestemmelser i forskriftens §§ 8-3 og 8-4.

5.15 Personvernforenne muligheter i digitale systemer

Digitale systemer er klart mest utbredt. Funksjonaliteten er stor, kan tilpasses og justeres på mange vis.

For det første : Dette innebærer at kameraene/systemene m/software i større grad enn tidligere kan "spisses" mot det aktuelle formålet :

- Områder som er uinteressante for formålet kan maskeres
- Tidsbestemt bruk kan benyttes mer aktivt
 - o aktiveres kun til bestemte tider
 - o analyse kan begrenses til å kun skje etter at et sikkerhetsbrudd er konstatert (black box- tilnærming)
 - o systematisk ivaretagelse av sletting (eksempelvis når betaling er utført)

For det andre : Bruk av digitale systemer har den ”fordel” at det kan legges igjen spor i form av sikkerhetslogger i programmene. Dette bør muligens få konsekvenser for Datatilsynets tilsyn med bruk av kameraovervåking. Tilsynet bør/kan i større grad benytte disse sporene/loggene for å sjekke om overvåkingen og spesielt håndteringen av opptakene er lovlig.

- når ble det foretatt opptak ?
- hvem har tilgang og hvem har faktisk vært inne og sett ?
- etc

Taxi, ”låsbare systemer”

5.16 Andre overvåkingsformer

Den teknologiske utviklingen medfører som kjent at det også kan være mulig å overvåke personer på annen måte enn gjennom ordinært billedopptak. Det kan derfor reises spørsmål om det er naturlig å regulere nærmere også andre overvåkingsformer som for eksempel ulike former for lydopptak, registrering gjennom sensorer osv. sammen med billedopptak. I den grad annen overvåking vil utgjøre en elektronisk behandling, vil den omfattes av de alminnelige reglene i loven. Dette vil for eksempel gjelde overvåking gjennom lydopptak der opptakene lagres på en slik måte at det er mulig å identifisere enkeltpersoner. Det vil imidlertid også kunne være regulert i straffeloven § 145a.

Det er vanskelig å ha fullstendig oversikt over hva det vil innebære å utvide bestemmelsene om kameraovervåking som ikke er elektronisk behandling til også å omfatte andre overvåkingsformer. Andre overvåkingsformer vil muligens nødvendiggjøre andre former for lovregulering enn det personopplysningsloven legger opp til for kameraovervåkingsens vedkommende.

Som et konkret eksempel i denne sammenhengen nevnes det at fjernsynsovervåking i moderne systemer kan implementeres i en integrert løsning sammen med adgangskontroll.

5.17 Reaksjoner fra tilsynsmyndigheten

Mangel på reaksjoner fra tilsynsmyndighet og klare lovkrav kan virke begrensende på motivasjonen for regeletterlevelse. I personopplysningslovens system ligger mye skjønnsbaserte vurderinger som overlates til den behandlingsansvarlige. Muligheten for enkeltmennesket til å forutberegne sin rettsstilling begrenses ved denne reguleringsformen, noe som igjen, av rettsikkerhetshensyn, begrenser tilsynsmyndighetens reaksjonsmuligheter. Det kan derfor være hensiktsmessig å vurdere muligheten for mindre skjønnsmessige regler, og for at også overtredelser av andre bestemmelser enn §§ 39 og 40 bør være straffesanksjonerte.

5.18 Andre aktører

Det er positivt at bransjen selv ønsker å øke sitt kunnskapsnivå, og på den måten bidra til at lover og regler overholdes i større grad. Tilsynet har som nevnt ikke myndighet til å pålegge leverandører og produsenter noen plikter, men oppfordrer likevel bransjen til – i samarbeid med Datatilsynet - å utarbeide retningslinjer på området. Aktørene vil da, med sin økte kompetanse, kunne hjelpe kundene/ de behandlingsansvarlige til å utføre overvåkingen på en

lovlig måte, og på måter som anses som minst mulig personvernkretnkende. Dette vil ikke minst være viktig med tanke på den raske utviklingen av nye produkter og ny teknologi på området noe som kan vise seg å være en utfordring for personvernet.

Det kan også nevnes at artikkel 29-gruppen understreker viktigheten av at medlemsstatene fastsetter retningslinjer vedrørende produsenters, tjenestetilbyderes, distributørers og forskeres aktiviteter for å kunne utvikle software og tekniske løsninger som er i tråd med gruppens anbefalte prinsipper om kameraovervåking. (Uttalelse nr 4/2004 om behandling av personopplysninger i forbindelse med videoovervåking).

Bransjeorganisasjoner, blant annet Nelfo, har uttrykt at de er interessert i å samarbeide med Datatilsynet for å utarbeide retningslinjer på området. Slikt samarbeid er i gang.

Kan tenkes at det innføres et lettere regime for overvåkere som har benyttet ”godkjente” leverandører.

- Bør det tas skritt for å fremme ordningen med personvernombud og bransjevise atferdsnormer?
- Typegodkjenning (Veritas)?
- Delegasjon til kommunen
- Lisens eller andre registreringsordninger

5.19 Andre tendenser i utviklingen

- Større grad av overvåking i private hjem, som også er arbeidsplass for andre, eks. hjemmehjelp. Døgnkontinuerlig for å følge med sykt familiemedlem, som også får ekstern pleie fra kommunen noen timer i døgnet. Er det å anse som rent personlig eller privat formål og dermed unntatt fra lovens saklige virkeområde, jf. § 3.
- Nanny cams
- Flytting av minibank og postkontor til butikker. Reiser nye problemstillinger. De gamle skillelinjene ikke lenger like naturlig utgangspunkt for eksempel reglene for sletting. Kontantbeløpene i postsystemet vil antagelig være mindre, men risiko for ran med mer vil antagelig være større fordi sikkerhetsregimet er dårligere.

Bør det klargjøres nærmere hva personovervåking er?

- For kontroll
- For bistand/utrykning
- Ekstra øye
- Hva er integritetskretnkende

Vedlegg: 1

Dagens kapittel VII - Fjernsynsovervåking

For å gjøre reglene om fjernsynsovervåking så oversiktlige som mulig har er det valgt å samle dem i et eget kapittel. § 37 gir en oversikt over hvilke behandlingsregler som kommer til anvendelse for ulike typer fjernsynsovervåking. §§ 38-41 oppstiller enkelte særregler som supplerer de øvrige reglene i loven for fjernsynsovervåkingens vedkommende. Det følger av reglene i kapittel 8 at Datatilsynet skal føre tilsyn med at reglene følges og bli pålagt i den utstrekning det er nødvendig.

§ 36. Definisjon

Med fjernsynsovervåking menes vedvarende eller regelmessig gjentatt personovervåking ved hjelp av fjernbetjent eller automatisk virkende fjernsynskamera fotografiapparat eller lignende apparat.

Til § 36 Definisjon

Definisjonen tilsvarende gjeldende definisjon i personregisterloven § 37 a og er også i samsvar med utvalgets forslag til § 4 tredje ledd.

§ 37. Virkeområde

Reglene i §§ 38-41 gjelder for all fjernsynsovervåking. Det samme gjelder § 8, § 9, § 11, § 31 og § 32. Fjernsynsovervåking som har som formål å avdekke opplysninger som nevnt i § 2 nr 8 bokstav b, er likevel tillatt, selv om vilkårene i § 9 første ledd ikke er oppfylt. Når billedopptak fra fjernsynsovervåking lagres på en måte som gjør det mulig å finne igjen opplysninger om en bestemt person, jf. § 3 første ledd, gjelder også lovens øvrige bestemmelser. Konsesjonsplikten etter § 33 gjelder likevel ikke for slik fjernsynsovervåking som har som formål å avdekke opplysninger som nevnt i § 2 nr 8 bokstav b.

Til § 37 Virkeområde

De særlige reglene i §§ 38-41 gjelder for alle former for fjernsynsovervåking, også for den overvåkingen som ikke er å anse som elektronisk behandling i henhold til § 3 og som derfor ikke omfattes av lovforslagets alminnelige regler, jf *første ledd* og punkt 8.5 i proposisjonen. Det samme gjør bestemmelsene i §§ 8, 9, 11, 31 og 32 i lovforslaget.

Henvisningen til §§ 8 og 9 om vilkår for å behandle personopplysninger og § 11 om grunnkrav til behandlingen innebærer bl a at overvåkingen på samme måte som i dag må være saklig begrunnet i den behandlingsansvarliges virksomhet, jf § 11 første ledd bokstav b. I tillegg stilles nå andre uttrykkelige krav til overvåkingen. Overvåkingen må grunnes på samtykke eller være nødvendig for å ivareta de interessene som er nærmere definert i §§ 8 eller 9. Formålet med fjernsynsovervåkingen må angis uttrykkelig i meldingen til Datatilsynet, og opptak som samles inn ved overvåkingen kan ikke benyttes til formål som er uforenlige med det opprinnelige formålet, jf § 11 første ledd bokstavene b og c og § 32. Av § 11 følger det at billedopptakene ikke kan lagres lenger enn det som er nødvendig ut fra formålet med behandlingen, jf første ledd bokstav e.

Fjernsynsovervåking vil være meldepliktig etter § 31 uten hensyn til om den resulterer i billedopptak, jf punkt 8.5. Innmeldte overvåkinger skal inntas i den offentlige fortegnelsen som Datatilsynet skal utferdige over meldepliktige behandlinger, jf § 42 tredje ledd nr 1. Datatilsynet har kompetanse til å stanse og gi pålegg overfor fjernsynsovervåking som foregår

i strid med lovens regler og vil også kunne ilegge tvangsmulkt dersom ikke påleggene overholdes, jf §§ 46 og 47. Den som ikke overholder pålegg gitt av Datatilsynet kan straffes, jf § 48 første ledd bokstav d. En behandlingsansvarlig som fjernsynsovervåker i strid med loven vil også kunne ilegges erstatningsansvar, jf § 49 i lovforslaget.

Fjernsynsovervåking og billedopptak der opptakene lagres manuelt som del av et personregister eller elektronisk på en måte som gjør det mulig å søke seg frem til enkeltpersoner, er behandling av personopplysninger i henhold til § 3 i lovforslaget, med den følge at også de øvrige bestemmelsene i loven får anvendelse, jf *annet ledd*.

§ 38. Grunnkrav til overvåking

Fjernsynsovervåking av sted hvor en begrenset krets av personer ferdes jevnlig, er bare tillatt dersom det ut fra virksomheten er et særskilt behov for overvåkingen.

Til § 38 Grunnkrav til overvåking

Bestemmelsen supplerer regelen om grunnkrav i § 11, og viderefører det kvalifiserte kravet for fjernsynsovervåking som følger av personregisterloven § 37 a første ledd annet punktum og som gjelder f eks for arbeidsplasser, jf også § 7 tredje ledd i utvalgets forslag.

§ 39. Utlevering av billedopptak gjort ved fjernsynsovervåking

Personopplysninger som er innsamlet ved billedopptak gjort ved fjernsynsovervåking, kan bare utleveres til andre enn den behandlingsansvarlige dersom den som er avbildet samtykker eller utleveringsadgangen følger av lov. Billedopptak kan likevel utleveres til politiet ved etterforskning av straffbare handlinger eller ulykker hvis ikke lovbestemt taushetsplikt er til hinder.

Til § 39 Utlevering av billedopptak gjort ved fjernsynsovervåking

Bestemmelsen viderefører pregl § 37 b første ledd. Departementet ser i motsetning til utvalget behov for å beholde en særlig regel om utlevering av billedopptak som er gjort ved fjernsynsovervåking.

§ 40. Varsel om at overvåking finner sted

Ved fjernsynsovervåking på offentlig sted eller sted hvor en begrenset krets av personer ferdes jevnlig, skal det ved skilting eller på annen måte gjøres tydelig oppmerksom på at stedet blir overvåket og hvem som er behandlingsansvarlig.

Til § 40 Varsel om at overvåking finner sted

De alminnelige reglene om varsling i lovforslaget passer dårlig på fjernsynsovervåking. Det vil som regel ikke være kontakt mellom den behandlingsansvarlige og de registrerte, og den behandlingsansvarlige vil ikke kjenne de registrertes identitet. Dette gjør at regelen om individuelt varsel ikke kan gjennomføres. Bestemmelsen viderefører varslingsplikten i straffeloven § 390 b, jf også utvalgets forslag til § 24. Departementet har imidlertid utvidet varslingsplikten, slik at den i tillegg til offentlig sted gjelder områder der en begrenset krets av personer ferdes jevnlig, i stedet for arbeidssted slik strl § 390 b nå lyder. Bakgrunnen er bl a at Datatilsynet gjennom sin praksis har erfart at det kan være behov for varsling på steder som det ikke uten videre er naturlig å betegne som offentlig sted eller arbeidsplass. Slik bestemmelsen utformes i departementets lovforslag, vil det også kreves varsling for overvåking f eks av parkeringsplasser i borettslag og foreningslokaler. Det vil i tillegg innebære en forenkling å knytte varslingsplikten til de samme steder der det stilles særlig

strengt krav til overvåking etter § 38 i lovforslaget. Begrepet «offentlig sted» skal forstås på samme måte som i straffeloven § 390 b.

§ 41. Forskrifter

Kongen kan gi forskrifter med nærmere bestemmelser om fjernsynsovervåking og billedopptak i forbindelse med slik overvåking, herunder om sikring, bruk og sletting av billedopptak gjort ved fjernsynsovervåking og om innsynsrett for den som er overvåket i de deler av billedopptakene hvor han eller hun er avbildet. Det kan også gis forskrift om at billedopptak kan utleveres utover det som følger av § 39.

Til § 41 Forskrifter

På samme måte som etter personregisterloven bør det åpnes for å gi nærmere regler ved forskrift, f.eks. om sikring av fjernsynsopptak, bruk av billedopptak som gjøres ved fjernsynsopptak og sletting av slike opptak.

Forskriften kapittel 8. Fjernsynsovervåking

§ 8-1. Virkeområde

Kapittelet her gjelder for fjernsynsovervåking, jf. personopplysningsloven § 36.

§ 8-2. Sikring av billedopptak

Billedopptakene skal sikres i henhold til personopplysningsloven § 13 om informasjonssikkerhet og bestemmelsene i kapittel 2 i forskriften her.

§ 8-3. Politiets bruk av billedopptak

Personopplysningsloven § 11 første ledd bokstav c er ikke til hinder for at politiet bruker billedopptak det er i besittelse av, i forbindelse med forebygging av straffbare handlinger, i forbindelse med oppklaring av ulykker eller i saker om ettersøking av forsvunne personer.

§ 8-4. Sletting av billedopptak

Billedopptak skal slettes når det ikke lenger er saklig grunn for oppbevaring, jf. personopplysningsloven § 28.

Billedopptak skal senest slettes 7 dager etter at opptakene er gjort. Sletteplikten etter forrige punktum gjelder likevel ikke dersom det er sannsynlig at billedopptaket vil bli utlevert til politiet i forbindelse med etterforskning av straffbare handlinger eller ulykker. I slike tilfeller kan billedopptakene oppbevares inntil 30 dager.

Billedopptak gjort i post- og banklokaler skal slettes senest tre måneder etter at opptakene er gjort.

Sletteplikten etter andre og tredje ledd gjelder ikke for billedopptak som politiet er i besittelse av, for billedopptak som kan være av betydning for rikets eller dets alliertes sikkerhet, forholdet til fremmede makter og andre vitale nasjonale sikkerhetsinteresser, eller hvor den som er avbildet samtykker i at billedopptakene oppbevares lenger.

Dersom sletteplikten etter første ledd oppstår for billedopptak som er utlevert til politiet fra andre, kan politiet tilbakelevere opptaket til vedkommende, som snarest skal slette det dersom fristen etter andre og tredje ledd er gått ut.

Dersom det foreligger et særlig behov for oppbevaring i lengre tid enn fastsatt i andre og tredje ledd, kan Datatilsynet gjøre unntak fra disse bestemmelsene.

§ 8-5. Innsynsrett

For billedopptak som omfattes av personopplysningsloven § 37 annet ledd, gjelder reglene om innsynsrett etter personopplysningsloven § 18. I andre tilfelle kan den som det er

gjort billedopptak av, kreve innsyn i de deler av billedopptakene hvor vedkommende er avbildet, dersom billedopptakene oppbevares utover 7 dager.

Innsynsrett etter første ledd annet punktum gjelder ikke i billedopptak som politiet er i besittelse av, eller billedopptak som kan være av betydning for rikets eller dets alliertes sikkerhet, andre vitale nasjonale sikkerhetsinteresser og forholdet til fremmede makter.

Justis- og politidepartementet
Lovavdelingen
Att: Knut Erik Sæther
Postboks 8005 Dep
0030 Oslo

Deres ref

Vår ref
09/00735-1

Dato
19. mai 2009

Supplerende kommentarer til Notat fra Datatilsynet i forbindelse med forestående revisjon av personopplysningslovens bestemmelser om fjernsynsovervåking fra 2005

Datatilsynet viser til tidligere oversendte notat om kameraovervåking fra 2005. Da notatet ligger tilbake i tid har Datatilsynet ønsket å feste noen kommentarer til temaet basert på våre erfaringer de siste årene. Det opprinnelige notatet mener vi fortsatt dekker temaet godt.

Kommentarene supplerer notatet og vi har søkt å trekke frem utviklingstrekk og erfaringer som vi har sett den seneste tiden.

1. Overblikk

Kameraovervåkingsutstyr blir billigere og billigere. Utbredelsen av kameraovervåking har blitt langt større, og det er ingen tegn til at denne utviklingen skal stanse nå. Over telefon og e-post mottar Datatilsynet en stor mengde spørsmål om kameraovervåking.

For bare ti til femten år siden så man kameraovervåking forholdsvis sjeldent, oftest ved ransutsatte virksomheter. Overvåkingen var i stor grad forbundet med tungtveiende sikkerhetsbehov, eller behov for å sikre fysiske verdier. Denne begrensningen er forlengst et tilbaketrukket stadium, og aktører tar i bruk kameraovervåking til å ivareta andre behov og ønsker.

Tradisjonelt så vi at verdisikring var en drivkraft for bruk av kameraovervåking. Dersom dette blir et vurderingskriterium i fremtiden er det antagelig viktig å definere at det ikke omfatter enhver verdi. Kanskje skal den knyttes opp til andre formålsbetraktninger som eksempelvis viktigheten for samfunnet at verdiene sikres.

Dagens situasjon er at kameraovervåking generelt skjer ved masseinnsamling av personopplysninger i håp om at dette vil ha en preventiv virkning på ulovlig eller uønsket adferd, gjerne utført av et lite mindretall. Resultatet er at den store overvekt av innsamlede og lagrede personopplysninger ikke viser annet en personers lovlige og dagligdagse handlinger.

Saksbehandlingen, kontrollene og henvendelsene til Datatilsynet viser at det er vanskelig å få øye på bransjer hvor kameraovervåking ikke benyttes. Man kan heller ikke konkludere med at en virksomhet har tatt i bruk kameraovervåking bare ved å se på hvilken type virksomhet det

er. Det er i dag like vanlig at kiosken har kameraovervåking, som at gullsmedbutikken har det.

Stadig flere formål blir trukket frem for å begrunne kameraovervåking. Et eksempel fra en restaurant i Trondheim kan belyse denne observasjonen. Restaurantens hovedbegrunnelse for overvåkingen var muligheten for å kunne følge med på behovet for å rydde bord eller å betjene kundene. Overvåkingen gjorde at servitøren skulle slippe å gå ut i lokalet for å se. Datatilsynet har også fått henvendelser fra virksomheter som ønsker å bruke kameraovervåking for å se om det er kunder i lokalet, samt fra personer som ønsker å ha ubemannede løsninger av ulike slag.

Når terskelen for å igangsette kameraovervåking fjerner seg stadig mer fra de mest basale behov som sikkerhet og trygghet, blir grensedragningen en utfordring: Finnes det formål og begrunnelser som må anses som så svake at overvåking ikke bør være tillatt? Skal det finnes noen grense? Om man ikke er villig til å trekke denne grensen, er alternativet at kameraovervåking i prinsippet kan brukes til hva som helst, og kan finnes hvor som helst, så lenge personvernulempene er små nok.

Kameraovervåking er ikke lenger avgrenset til en profesjonell eller offentlig sfære som i forretninger, banker eller på kjøpesentre.

Datatilsynet mottar forholdsvis mange henvendelser fra privatpersoner som ønsker å igangsette kameraovervåking, for eksempel av egen eiendom og egne verdier. I en del tilfeller er det også andre motiver, som overvåking av leietagere eller naboer. Datatilsynet mottar også mange henvendelser fra privatpersoner som reagerer på andre privatpersoners overvåking. Ofte gjelder disse situasjonene nabokrangler, gjensidig mistillit og beskyldninger. Det synes å være en tendens til at "dummy-kameraer" (kameraer som kun ser ut som ekte overvåkingskameraer) er mye i bruk i slike situasjoner.

Samtidig skjer det også en annen form for løsrivelse fra det "profesjonelle", i form av "gjør-det-selv-løsninger", gjerne basert på bruk av web-kamerateknologi. Dette gjelder både i private sammenhenger, i butikker og på arbeidsplasser. Det er ofte svært dårlig konfidensialitetssikring for slike løsninger.

De kameraovervåkingsanlegg tilsynet i hovedsak ser når vi kontrollerer er fremdeles forholdsvis tradisjonelle: faste kameraer, koblet til en billedopptaksenhet, gjerne med monitor. Imidlertid har det de siste årene vært en overgang fra analog til digital lagring. Digital lagring gjør det enklere å bruke eller kopiere opptak til andre formål enn opptaket hadde da det ble startet.

Det er vanlig å ha en opptaksenhet som kun gjør opptak når det er bevegelse innenfor det feltet kameraet fanger opp, noe som gjør det enklere å finne tilbake til hendelser.

På noen felter fører teknologien til en mer inngripende situasjon, for eksempel ved overføring av bilder over Internett. Skjer dette på en arbeidsplass, vil sjefen kunne overvåke arbeidsplassen når som helst, og fra hvor som helst, så lenge det er tilgang til Internett.

Datatilsynet har også merket seg at styrbare kameraer med zoomfunksjon ikke er uvanlig. Utstyret gir muligheter for en oppsøkende og nærgående overvåking i langt større grad enn faste kameravinkler og vanlige oversiktsbilder vil kunne gi. Dette kan føre med seg betydelig større

personvernulemper og Datatilsynet mener denne typen kameraovervåking må sees på og skal kanskje ikke alminneliggjøres.

2. Et regelverk tilpasset målgruppen

Hensynet til lettfattelighet må veie tungt i arbeid med regelverk for kameraovervåking. Gruppen som trenger å forstå lovens krav er stor; den er voksende og innenfor et bredt spekter av bransjer.

Erfaringsmessig viser Datatilsynets kontroller lav kunnskap om regelverket blant de som benytter kameraovervåking. Selv om Datatilsynet erfarer at reglene brytes ofte, er krav til melding til Datatilsynet og krav om skilting ofte kjent. Også at det er strenge krav for utlevering til andre synes å være godt kjent. Mer ukjent synes kravene til behandlingsgrunnlag og grunnkrav for behandling av personopplysninger (personopplysningslovens §§ 8, 9 og 11) – bestemmelser som er svært viktig for personvernet, og som også gjelder for kameraovervåkingstilfellene.

Situasjon fordrer et fokus på hvordan regelverket kan utformes slik at de som skal lese og etterleve det, forstår lovens krav. Regelverket bør utformes slik at det treffes beslutninger som medfører minst mulig inngripen i personvernet, og unngå inngripen som ikke er nødvendig eller nyttig.

Datatilsynet vil peke på tre grupper som vi ser er sentrale. Den ene gruppen er behandlingsansvarlige og de som medvirker til beslutninger om å igangsette kameraovervåking hos den ansvarlige. Videre er selgere og montører av kameraovervåking en viktig målgruppe. Men også vanlige samfunnsmedlemmer er berørt, og vil i egenskap av ansatt, nabo, borger lure på hvor grensene går for en akseptabel overvåking, hva vedkommende må finne seg i og hvilke rettigheter vedkommende har i sammenheng med kameraovervåking.

Regelverket bør være mest mulig lettfattelig, og regelverket bør også stå mest mulig samlet på et sted.

Det er et betydelig forbedringspotensial innefor begge disse feltene. Når det gjelder et mest mulig samlet regelverk, er det en ulempe at behandlingsgrunnlag og grunnkrav til behandling av personopplysninger ikke er å finne innenfor lovens særregulering av kameraovervåking.

3. Krav til rettslig grunnlag bør tilpasses og settes inn i særreguleringen

Et naturlig utgangspunkt er at kameraovervåking reguleres i et eget kapittel i loven, slik det også er i dag. Tilsynet mener at et slikt kapittel i større grad enn i dag bør gi uttømmende lovbestemmelser for kameraovervåking *innenfor* selve kapittelet. Det bør i minst mulig grad vises til lovens alminnelige bestemmelser.

Personopplysningslovens §§ 8, 9 og 11 eller de hensyn disse bestemmelsene er satt til å ivareta, bør vurderes tatt inn i et eget kapittel om fjernsynsovervåking. Antagelig bør bestemmelsene omformuleres i tråd med konteksten – eksklusivt rettet mot kameraovervåking. Det bør vurderes hvorvidt begrepet proporsjonalitet skal gjøres eksplisitt i

sammenheng med grunnkravene. Aktuelle behandlingsgrunnlag for kameraovervåking vil være begrenset, etter Datatilsynets vurdering.

I notatet fra 2005 gjøres det også rede for muligheten for å tydeliggjøre hvilke hensyn som skal vektlegges i en vurdering av en akseptabel overvåking. Det er tilsynets oppfatning at en slik formulering bør vurderes. En åpenbar fordel er å tydeliggjøre hvilke formål som anses som relevante for bruk av kameraovervåking. En annen fordel med en slik formulering er at den, direkte eller indirekte, poengterer forskjellen mellom tungveiende hensyn, eksempelvis liv og helse, og hensyn som er av en mindre tungveiende karakter.

Å benytte kameraovervåking for å forebygge kriminalitet har i mange tilfeller blitt sett som legitimt formål. Forskning på dette feltet gir ikke de konklusjoner som mange tror og håper på. En formulering som utdyper personopplysningslovens § 8 f bør derfor være forsiktig i sammenheng med kriminalitetsforebyggelse. Om formuleringen setter krav til at overvåkingen reelt må kunne forventes å forhindre kriminalitet, vil formuleringen bli vanskelig å forholde seg til.

Det gis et eksempel for å illustrere rådende situasjon, og hvilket behov som eksisterer for å bringe bestemmelser om formålsangivelse og formålsrelevans inn sammen med regelverket spesielt for kameraovervåking:

I 2008 sendte Datatilsynet en rekke varsler om kontroll av kameraovervåking. I brevet ble det vist til lovens § 11, og bedt om at det i forbindelse med kontrollen ble overlevert *”en nedtegnelse av formålet med fjernsynsovervåkingen. Datatilsynet ønsker å motta dette som et eget skriv som kan tas med videre i saksbehandlingen.”* Kun et meget lite antall av de spurte la frem en nedtegnelse av formålet på kontrollen. Foranledningen for anskaffelse av kameraovervåking var klart, men et avgrenset og tydelig formål med den pågående behandling av personopplysninger var en mangelvare.

Sammen med grunnkrav bør det vurderes en formulering som setter krav til en skriftlig nedfelt formålsangivelse.

Et klart definert formål er viktig for selve utformingen av overvåkingen. Et lite spesifisert formål vil kunne gi en langt mer omfattende og inngripende overvåking. Også den daglige drift behøver et skriftlig nedfelt formål. Konkrete hendelser vil føre til spørsmål om bruk av overvåkingen, noe som må vurderes etter formålet med innsamlingen. Den registrerte må kunne vite med sikkerhet hva opplysningene samles inn for, hva de kan brukes til og hvor lenge de oppbevares.

4. Informasjonssikkerhet og internkontroll

Det må trolig gjøres noen kompromisser i forhold et prinsipp om at særreguleringen skal være mest mulig uttømmende. Personopplysningslovens bestemmelser for informasjonssikkerhet i dagens § 13, med utfyllende forskriftsbestemmelser, må også gjelde for kameraovervåking så langt de passer. Det vil neppe være naturlig at disse kopieres i særreguleringen.

I tillegg bør også personopplysningslovens § 14 om internkontroll gjelde for kameraovervåking, noe som ikke fremkommer av dagens § 37 i loven.

5. Personopplysningslovens § 37 bør gjennomgås

Dagens § 37 i personopplysningsloven bør gjennomgås. Grensen er uklar mellom den overvåking som kun er omfattet av første ledd og den overvåking som også er omfattet av bestemmelsens andre ledd. I tråd med at digitale løsninger er blitt det vanlige, må man stille spørsmål ved om det er tjenelig å trekke et slikt skille. Om det skal gjøres, vil det være mer naturlig å ta utgangspunkt i skillet mellom den kameraovervåking som skjer med opptak og den overvåking som ikke har opptak - monitorering.

6. Rett til innsyn

Lovens kapittel VII har ingen særskilte bestemmelser om innsynsrett for kameraovervåking; disse finnes i forskriftens kapittel 8. Det bør vurderes om rett til innsyn i opptak skal nedfelles i loven, da dette er et viktig personvernprinsipp.

Hovedbestemmelsen om sletting slik den nå står i forskriftens § 8-4 bør vurderes flyttet til loven

7. Opptak og sletting

Slettefristen bør vurderes strammet opp eksempelvis til *”så snart som mulig, og senest innen 7 dager”*. Da får man gitt klart uttrykk for at det er et selvstendig ansvar å slette opptakene så raskt som mulig. Per i dag er det en meget utbredt misforståelse at slettefristen er 7 dager, uavhengig av om det er nødvendig å lagre opptakene så lenge eller ikke. Dette tilsvarer maksimal tillatt lagringstid. Erfaring viser at mange virksomheter som i dag lagrer opptak i 7 dager ikke har behov for så lang lagring. Lagringstiden er ofte heller ikke et resultat av en vurdering.

Et annet viktig spørsmål er om opptak er berettiget og nødvendig hele døgnet - hele uken. I mange tilfeller er det klare risikotider, eksempelvis kveld, natt og helger. Det er tilsynets vurdering at personvernkonsekvenser kan reduseres vesentlig ved en mer kritisk vurdering av når opptak er nødvendig. For de som foretar opptak, er tidsavgrensning dessverre lite utbredt.

Regelverket kan i større grad enn i dag kreve at det skal være bevisste valg med referanse til nødvendighet som ligger bak en beslutning om overvåkning.

Slik informasjon vil være nyttig for Datatilsynet ved kontroller. Begrunnelsen vil også være av verdi internt, eksempelvis som informasjon til ansatte, drøfting med ansattes representanter og ved revisjoner av den praksis som virksomheten har.

Et annet virkemiddel og vurderingstema som kan redusere mengden med lagrede personopplysninger er at opptak skjer med intervaller, eksempelvis ved at opptak kun skjer fra ett og ett kamera av gangen. Selv om den totale mengden opptak vil kunne reduseres, og med den også en reduksjon i mengden lagrede personopplysninger, må man likevel sette spørsmål ved hvor betydningsfullt dette er for personvernet. Så lenge den som befinner seg under

kameraene ikke kan vite seg fri for overvåking, spiller det kanskje mindre rolle om opptak skjer hele tiden eller kun en brøkdel av tiden.

8. Varsling og informasjon

Personopplysningslovens nåværende § 40 om varsling setter kun krav til en begrenset informasjonsmengde til publikum. Datatilsynet har i konkrete saker sett at dette er problematisk. Det gjelder både informasjonsmengden på skilter og mangel av informasjon ut over skilter. Datatilsynet ser det som tjenelig at det vurderes krav til informasjon, skilter og annen informasjon, i en og samme bestemmelse.

En bakgrunn for personopplysningslovens § 40 er at lovens alminnelige regler for informasjon er vanskelige å praktisere i forbindelse med kameraovervåking. Men opplysningsmengden i personopplysningslovens § 40 vil være urimelig liten for særlig berørte grupper.

Det bør videre vurderes en bestemmelse som stiller minstekrav til varsling gjennom skilter; - informasjon som skal nå alle berørte. I tillegg bør det være et krav om ytterligere informasjon etter mønster av personopplysningslovens § 19 til særlig berørte grupper så langt dette med rimelighet lar seg gjøre. Det er mulig å sette dette i tett relasjon til personopplysningslovens § 38 og formuleringen "begrenset krets". Normalt vil det være denne kretsen som har størst behov for informasjonen.

Typiske eksempler på slike grupper kan være ansatte på kameraovervåkede arbeidsplasser, beboere i borettslag med kameraovervåking og elever og deres foresatte (i den grad kameraovervåkingen i det hele tatt skal aksepteres mens elevene er på skolen i skoletiden).

Det kan være tjenelig å vurdere om tradisjonelle skilter bør ha mer informasjon enn hva personopplysningslovens § 40 krever. Standardisering av skilter bør vurderes. Felles utforming av skilter, eventuelt også med bruk av standardsymboler, kan gjøre det lettere å merke seg informasjonen når man går inn i et overvåket område. I tillegg til de momenter som er nevnt i rapporten fra 2005, bør tidsavgrenset overvåking nevnes. I denne type situasjoner er utdypende informasjon særlig viktig.

Hvis skilter ikke oppgir når (tidspunkter eller situasjon) det foretas kameraovervåking, vil den som tar utgangspunkt i skiltene tro at kameraovervåkingene er aktiv hele tiden.. Skiltene kan derfor bli misvisende. Man vil kunne tro at man er overvåket også når det ikke er tilfellet. Ett eksempel kan være områder rundt et fotballstadion som kun er overvåket under kampavvikling.

Det er ikke bare en verdi å være informert om kameraovervåking. Det er også en verdi å vite seg fri for kameraovervåking når det er tilfellet. Et relevant eksempel er kameraovervåking av skoler. Den informasjon (skilter og/ eller annet) som elever har må ikke lede dem til å tro at de er kameraovervåket i skoletiden; en overvåking som normalt vil være i strid med loven.

Selv om mange typer informasjonen kan være både relevante og ønskelige, må det utvises en forsiktighet med for mye informasjon på selve varslingskiltene. Den viktigste informasjonen – at området er overvåket og av hvem – må ikke drukne i detaljer.

Etter tilsynets vurdering, bør tidsavgrensning stå på skiltene. Det samme gjelder også kontaktopplysninger for henvendelser vedrørende kameraovervåkingen.

9. Lyd sammen med overvåkingsbilder

Kombinasjonen av overvåkingsbilder og lyd vil i mange tilfeller kunne være svært inngripende og krenkende. Hver for seg, gir lyd og bilder en stor mengde informasjon. At eksempelvis to kameraovervåkede mennesker kan føre en samtale hvor innholdet blir mellom dem, er av stor verdi. Lyd og bilde sammen gjør situasjonen tilnærmet helt transparent, informasjonen som samles inn står i liten grad tilbake for hva som kan oppfattes ved å være fysisk til stede i situasjonen. Det bør stilles spørsmål ved om ikke lyd alene er mer inngripende enn bilde alene. I valget mellom at en overvåker, eksempelvis arbeidsgiver, kan høre det du sier eller se det du gjør, antar Datatilsynet at de fleste vil oppfatte lydoverføring eller lydopptak som mest inngripende.

Et annet forhold er at kameravinkelen gjør det mulig å holde noe utenfor. En slik avgrensning av mikrofoners evne til å selektivt fange opp lyd, er neppe realistisk. Lyd vil kunne fanges opp ut over hva som skjer innenfor billedrammen.

Det er derfor viktig at den enkle muligheten som finnes for lydoverføring og opptak som finnes i sammenheng med kameraovervåkingsteknologi, ikke blir benyttet. Det ville medført et uforsvarlig inngrep i personvernet. Temaet er også tatt opp i rapporten fra 2005.

Det kan tenkes enkelte steder og situasjoner hvor lyd likevel kan være berettiget, kanskje i sammenheng med tidsmessig isolerte alarmsituasjoner hvor liv og helse står på spill. Men en vanlig utbredelse bør dette ikke få.

Det bør vurderes om det skal innføres et generelt forbud mot kameraovervåking med lyd, og eventuelt med enkelte positivt angitte unntak. Et annet alternativ kan være å oppliste krav til når lydoverføring og/ eller opptak kan skje i sammenheng med kameraovervåking. Det er tilsynet vurdering at disse kravene i så fall må være svært strenge.

10. Konesesjonsplikt

Slik Datatilsynet ser det, er konsesjonsplikt for kameraovervåking ikke ønskelig, rent generelt.

Det bør vurderes om Datatilsynet likevel kan beslutte at konkrete tilfeller av kameraovervåking, eller spesielle former for kameraovervåking, skal være konsesjonspliktig.

11. Forskriftshjemler

Datatilsynet mener det er tjenelig at det også finnes bestemmelser for kameraovervåking på forskriftsnivå, også her innenfor et eget kapittel. Hovedbestemmelsene bør stå i loven, mens unntak og presiseringer henvises til forskriften.

For den som skal lese loven, eksempelvis en som vurderer om hun skal igangsette kameraovervåking, ville det vært enklest om alle bestemmelser var samlet på ett sted (enten forskrift eller lov). Men muligheten for gi nærmere forskriftsbestemmelser har en stor verdi.

Anledning for en mer dynamisk utvikling av regelverket enn lovendringer er viktig på et felt hvor utvikling skjer raskt. Det gjelder både med tanke på ny teknologi, og ny og annerledes bruk av kameraovervåking (formål og situasjon overvåkingen skjer i). Forskrifthjemmel er i denne sammenheng en mulighet for å kunne følge med i utviklingen.

Det må legges til at teknologiske nyvinninger ikke nødvendigvis medfører en større inngripen i personvernet. Det er fullt mulig å se for seg at ny teknologi også vil kunne gjøre behandlingen av personopplysninger mer eksklusivt avgrenset til hva som er formålet, og med en god evne til å sjalte vekk irrelevante opplysninger – både fra innsamling og fra lagring.

Innenfor dagens lovbestemmelser sondres det kun mellom overvåking av steder hvor en begrenset krets av personer ferdes jevnlig og offentlig sted.

Ut over dette, må man med dagens situasjon ta utgangspunkt i forvaltningspraksis for en nærmere avklaring av hvor grensene går for en overvåking i tråd med loven.

Det kan vurderes om det er ønskelig å oppstille et sterkere vern på andre steder enn der hvor ”en begrenset krets av personer ferdes jevnlig”, jf personopplysningslovens § 38. Dette kan gjøres ved en utvidelse i personopplysningslovens § 38.

Et synspunkt er at det kan settes spesielle krav til overvåking av nærmere definerte *situasjoner, steder eller funksjoner*. Et annet utgangspunkt kan være å sette særlige krav knyttet til kameraovervåking av *grupper* som behøver et særlig vern. Ett eksempel kan være skoleelever eller overvåking innenfor rammen av opplæringsinstitusjoner. Et annet eksempel kan være beboere eller innlagte på sykehus, sykehjem, bo- eller rehabiliteringsinstitusjoner.

Andre muligheter kan være å sette særlige begrensninger for, eller forbud mot, overvåking av steder hvor folk forventer en stor grad av diskresjon, eller steder hvor det forventes en form for frihet som ikke lar seg forene med overvåking. Denne type spesifikasjoner behøver ikke å ha en tilknytning til noen spesiell gruppe eller krets, man kun ta utgangspunkt i stedets egenart og funksjon. Mulige eksempler kan være parker, friområder eller restauranter.

Spesifikke reguleringer for overvåking med utgangspunkt i spesielle bransjer/ virksomheter, grupper, eller med utgangspunkt i stedets funksjon, kan være

- at overvåking kun vil være tillat til snevert definert og tungveiende formål
- begrensning i lagringstid eller anledning til foreta opptak
- at enkelte former for overvåking ikke kan foretas med hjemmel i interesseavveining, men fordrer samtykke fra den det gjelder
- begrensning i hva som kan overvåkes
- begrensning i når det kan overvåkes
- særlige krav til sikkerhet eller rutiner

Det er ønskelig å få høringsinstansenes vurdering av hvilke forskrifthjemler som loven bør ha i sammenheng med kameraovervåking, og om dagens forskrifthjemmel bør utvides i tråd med de hensyn som står beskrevet ovenfor.

12. Villedende informasjon og anordninger

Datatilsynet får stadig flere henvendelser fra personer som opplever sitt personvern krenket av overvåkingskameraer som ved nærmere ettersyn viser seg å være etterligninger, ikke ordentlige overvåkingskameraer. Bruk av slike dummy-kameraer reiser vanskelige, prinsipielle spørsmål.

Det samme gjelder utplassering av varslingsskilter uten at det foregår kameraovervåking. Det ser også ut til å være vanlig å la ødelagte kameraovervåkingsanlegg bli værende sammen med varslingsskilter. Resultatet er det samme; folk ledes til å tro at de er gjenstand for reel kameraovervåking.

Mange av sakene omhandler dummy-kameraer i nabolag og boligområder, men Datatilsynet ser også dummy-kameraer i bruk hos profesjonelle aktører, både utendørs og innendørs. I mange tilfeller er dummy-kameraene plassert slik at de ville representert en ulovlig overvåking dersom kameraene var ekte.

Datatilsynet oppfatter at mange tror at bruk av dummykameraer skåner den enkelte i høyere grad enn reell overvåking vil gjøre: Folk gis "bare" en følelse av å bli overvåket. Datatilsynet ser store problemer med en slik tilnærming. Det må stilles spørsmål ved om samfunnet er tjent med at borgernes handlinger blir forsøkt manipulert, eller for den saks skyld "forbedret", gjennom tilsynelatende overvåking.

Selv om det verken innsamles, lagres eller tilgjengeliggjøres personopplysninger, vil dummy-kameraer true sentrale personvernprinsipper. Ryddig og sannferdig informasjon er bærende elementer i personvernregelverket. Borgeren er avhengig av å kunne ha tillit til hva han blir presentert for, det være seg informasjon i en samtykkeerklæring, informasjon på varselskilter eller synlige overvåkingskameraer. Usannheter og tilbakeholdelse av informasjon svekker en viktig ressurs, nemlig tillit.

Datatilsynet har i konkrete saker anbefalt eier å fjerne dummy-kameraer, men det kan ikke pålegges. Denne situasjonen er i en del tilfeller svært lite tilfredsstillende. Så lenge eier ikke er villig til å etterkomme en anbefaling, vil den tilsynelatende overvåkingen fortsette, og med den også forvirring og opplevelse av å bli overvåket.

13. Web-kamera og nettpublisering – grensedragning for begrepet personopplysninger

Over tid har det vært en rekke henvendelser hvor personer reagerer negativt på bruk av web-kamera som gir oversiktsbilder publisert på Internett. Sakene er ofte vanskelige. Det kan være knyttet en følelse av krenkelse til det at en privat sfære, om enn fra langt hold og med til dels dårlig billedkvalitet, blir vist på Internett for en hel verden. Problematikken er også nevnt i notatet fra 2005.

Hvor grensen skal gå, avhenger av en vurdering av hva som må være å betrakte som personopplysninger. Særlig når bildene viser privat bebyggelse, er det svært vanskelig å trekke en klar grense.

Dagens praksis har i stor grad vært knyttet til gjenkjennbarhet for personer på bildene. Heller ikke dette er et enkelt kriterium. Et åpenbart spørsmål er gjenkjennelig *for hvem*, og i en

situasjon hvor personen befinner på et sted hvor ikke hvem som helst befinner seg. En synlig skikkelse på byen torg kan være hvem som helst. Det stiller seg annerledes med en skikkelse innefor et hagegjerde.

Samme problematikk kan være aktuell innenfor byggeplasser. Formålet med nettpublisering av bilder i denne sammenheng kan være å vise hvordan et bygg reiser seg, eksempelvis slik at kjøpere av leiligheter kan se hvordan arbeidet med deres fremtidige bolig skrider frem. For dem som vet hvem som jobber på stedet, og hvem som jobber med hva, kan det være mulig å følge den enkelte arbeider. For de ikke har denne kunnskapen vil det kanskje være umulig å identifisere de som er på bildene.

En annen problematikk er bevegelige web-kameraer, eksempelvis forhåndsprogrammert til å ta bilder fra ulike vinkler. Bildene som tas, og som publiseres på Internett, kan være uproblematisk. Men for naboer rundt et slikt kamera, kan situasjonen oppfattes som uholdbar.

Det kan antas at kameraet relativt enkelt kan styres med vinkel, høyde og zoom fra et brukergrensesnitt, og det eksisterer ikke full tillit til at kameraets potensial ikke nyttes ut over hva som kan ses på Internett. Naboer kan ønske en etterprøvbar eller synlig sikring mot at det styrbare kameraet ikke kan overvåke deres hus og hage.

Personopplysningslovens forholdet til ytringsfriheten reguleres i lovens § 7. Også for behandlinger av personopplysninger som faller inn under denne bestemmelsen gjelder personopplysningslovens kapittel VII om fjernsynsovervåking. Svært mange av aktørene som publiserer oversiktbilder fra web-kameraer er aviser på Internett.

Høringsinstansenes vurdering av dette temaet i sammenheng med revisjon av regelverket er ønskelig.

14. Overvåking av privat eiendom og kameraovervåking til "private formål"

Kameraovervåking av eget hus og eiendom har blitt forholdsvis vanlig. Naboer som reagerer på andre naboers overvåking resulterer i en rekke henvendelser til Datatilsynet. Bakgrunnen er gjerne antagelser om at overvåkingen går ut over kameraeierens eiendom. Situasjonen er ofte preget av nabokrangel og gjensidig mistillit. Ord står ofte mot ord. Sakene er vanskelige, langvarige og arbeidskrevende. Det er også et spørsmål om den kameraovervåking som skjer i det hele tatt faller inn under lovens bestemmelser.

Justisdepartementets lovavdeling gav i 2001 en tolkningsuttalelse om fjernsynsovervåking og private formål, jf unntak fra lovens bestemmelser etter § 3 (departementets referanse: 01/08493 ES KES/bj). Datatilsynet har lagt denne til grunn for sin praksis på det aktuelle feltet.

Problematikken er ikke bare relevant ved kameraovervåking over eiendomsgrenser, eller antagelser om dette. Det er også aktuelt inne på kameraovervåkes egen eiendom, eksempelvis i relasjon til leietagere eller personer med en vei- eller ferdselsrett over eiendommen.

Det kan vurderes om denne type overvåking bør klargjøres i lovtekst.

Kameraovervåking inne i private hjem i forbindelse med utøst alarm, og med billedoverføring til vaktentral, eksisterer i dag som et tilbud fra sikkerhetsbransjen. Denne type overvåking reiser flere spørsmål. Ett tema er hvorvidt dette er en overvåking som kan betraktes som "private formål" og unntatt personopplysningslovens virkeområde, jf. personopplysningslovens § 3 andre ledd. Et annet spørsmål er knyttet til ansvarsforhold; om sikkerhetsselskapet er å betrakte som behandlingsansvarlig eller om selskapet foretar en behandling av personopplysninger på vegne av privatpersonen som kjøper tjenesten.

15. Sletting av billedopptak i politiets besittelse

Det er ikke uvanlig at politiet sikrer seg opptak i forbindelse med etterforskning. Datatilsynet er opptatt av hva som skjer med opptaket videre. Det bør vurderes å se om det er behov for et sekundært regelsett i tillegg til straffeprosessuelle regler for oppbevaring av opptaket som bevis.

16. Kameraovervåking , gjenkjennelsesteknologi og digital bearbeiding

Blant de spørsmål som bør reises, er hvordan lovverket best mulig kan ivareta personvernet i møte med ny teknologi. Ikke bare må det forventes at overvåkingskameraer vil bli både billigere og bedre i tiden fremover.

Et tema er gjenkjenningsteknologi, noe som vil kunne ha en klar grense mot biometri.

Utviklingen av teknologien kan i fremtiden kobles sammen slik at en kamerasystem kan følge en person basert på ansiktsgjenkjennelse og analyse av bevegelsesmønster.

Kameraovervåking sammen med biometri og digital bearbeiding behandles også i punkt 5.11 i Notat fra Datatilsynet i forbindelse med forestående revisjon av personopplysningslovens bestemmelser om fjernsynsovervåking fra 2005.

Med hilsen



Kim Ellertsen
avdelingsdirektør