RETTSLIGE SPØRSMÅL KNYTTET TIL INNSAMLING OG BRUK AV DIGITALE BEVIS

Line Coll,

i samarbeid med Dag Wiese Schartum, AFIN, UiO

På oppdrag fra Norsk Regnesentral

Oktober 2004

Forord

Den økende utbredelsen av datasystemer i samfunnet leder til at digitale bevis blir stadig viktigere. Prosjektet DESDIFOR (Defining Standards in Digital Forensics) dreier seg om å lage et forslag til en standard for hvordan man proaktivt kan legge sine datasystemer og organisasjon tilrette for å samle inn og oppbevare digitale bevis i overensstemmelse med Norsk lovgivning. I dette prosjektet samarbeider NR med AFIN. Utredningen "Rettslige spørsmål knyttet til innsamling og bruk av digitale bevis" er et viktig bidrag i prosjektet DESDIFOR og vi vil med dette takke for rapporten og for et godt og nyttig samarbeid.

Ingvar Tjøstheim og Jerker Danielsson
NR

Innledning

Innsamling og bruk av digitale bevis reiser en rekke spørsmål av juridisk, etisk og samfunnsmessig art. I forhold til digital informasjon brukt som bevis har det særlig vært fokusert på spørsmålene knyttet til bruk av såkalt overskuddsinformasjon og til bruk av opplysninger til andre formål enn de opprinnelig ble samlet inn for. Slik bruk av informasjon har også en side til det som har blitt kalt "storebrorsamfunnet", hvor skrekkscenarioet er en sterk og overordnet (stats)makt som ser og vet alt om borgerne. For å sikre fundamentale rettssikkerhetsprinsipper og for å ivareta viktige personrettslige prinsipper, er det derfor svært viktig å ha klare grenser og regler for innsamling og bruk av personopplysninger. Dette hensynet blir særlig viktig der de innsamlede opplysningene skal benyttes som bevis i en straffesak.

I denne utredningen vil det bli gitt en fremstilling av reglene for innsamling av opplysninger med formålet å bevise en straffbar handling. Oppmerksomheten vil bli rettet mot opplysninger i elektronisk form, det vil si opplysninger som vil fremkomme som "digitale bevis". Den største delen av utredningen vil gjelde rettsregler vedrørende innsamling og bruk av personopplysninger. Dette fordi de aller fleste opplysninger som kan brukes som bevis vil være knyttet til fysiske personer på en slik måte at de faller innenfor definisjonen av "personopplysning". For behandling av slike opplysninger gjelder personopplysningsloven,[1] og reglene som følger av loven vil være avgjørende for i hvilken grad slike opplysninger lovlig kan samles inn som bevis av private virksomheter og privatpersoner. Utredningen vil også omfatte rettsregler for politiets behandling av digitale bevis, noe som primært er regulert i rettspleielovgivningen. Først i utredningen vil det bli redegjort for hva som menes med "digitale bevis", og for prinsippet om fri bevisvurdering i norsk rett.

1. HVA ER DIGITALE BEVIS?

Ordet "bevis" er definert som et middel som benyttes for å godtgjøre en rettslig relevant omstendighet i en sak. I både straffe- og sivilprosessretten skiller man gjerne mellom de personlige bevis, som er parts- og vitneforklaringer og de tinglige bevis, også kalt de reelle bevis, som er åstedet eller gjenstander som er relevante for saken. En særskilt kategori er dokumentbevisene, hvor det som regel er meningsinnholdet i dokumentet som er relevant.[2] Et dokumentbevis kan for eksempel være en avtale, en injurierende avisartikkel, en dagbok eller lignende.[3] Også disketter eller annet digitalt lagret informasjon vil være dokumentbevis.

"Digitale" eller "elektroniske" bevis er relativt nye former for bevismidler. Grensen mellom de nyere digitale bevismidlene og de mer tradisjonelle bevismidlene er flytende. Digitale bevismidler er for eksempel video fra overvåkningskameraer, opplysninger om passering i bomringer, bilder som er knipset i fartsbokser, utskrifter fra adgangslogger eller elektroniske spor lagt igjen på Internett.

Det samlede begrepet "digitale bevis" eller "elektroniske bevis" er et forholdsvis nytt begrep, og omfatter i utgangspunktet svært mange forskjellige former for opplysninger. Begrepet favner i utgangspunktet ethvert digitalt materiale som er samlet inn for å underbygge en

---

[1] Lov om behandling av personopplysninger av 14. april 2000 nr 31.

[2] Jo Hov, Rettergang i sivile saker, 2. utg. 1994, side 387.

[3] Johs. Andenæs, Norsk straffeprosess, Bind I, 3. utgave 2000, side 181.

faktisk omstendighet som antas å være rettslig relevant. Her velger vi å dele materialet inn i to kategorier i samsvar med det "formålsbestemthetsprinsippet" som er nedfelt i personopplysningslovgivningen. Den første kategorien kan kalles direkte innsamling av bevis. Dette er opplysninger som samles inn *med det formål* å underbygge og dokumentere at noen har overtrådt rettsregler som det er knyttet sanksjoner til. Kategorien dekker både det tilfellet at en kriminell (avsluttet eller pågående) handling er avdekket eller klart forventet. For eksempel kan arbeidsgiver ta beslag i en arbeidstakers filer med ulovlig innhold, eller sette opp videokamera for å avdekke det han mistenker er en pågående kriminell aktivitet (tyveri fra lageret).

Begrepet digitale bevis kan også omfatte materiale som samles inn uten å ha innsamling av bevis som formål. For eksempel kan opplysninger om biler som har passert en bestemt bomring senere brukes i etterforskningen av et ran som er blitt begått på et sted der det er bomringer eller annen overvåkning langs aktuelle fluktruter. Dette kan kalles indirekte innsamling av bevis. Formålet med innsamlingen er da primært et annet enn bevisinnsamlingen. Vi antar at denne kategorien er mindre interessant for arbeidet i DESDIFOR.

I strafferetten har begrepet bevis en relativt klar avgrensning og definisjon. Fingeravtrykk, fotspor og DNA er materiale som klart fremstår som bevis i folks bevissthet. Det samme gjelder utskrifter av mobiltelefonlogger og elektroniske spor lagt igjen på Internett. På det privatrettslige området er innholdet av begrepet "bevis" noe mer diffust. Forklaringen kan være at man svært ofte hører om politiets sikring og innhenting av bevis forut for, eller etter at det har skjedd en kriminell handling. Det er da lettere å knytte innhentingen av informasjonen opp til formålet – nemlig å benytte informasjonen til å underbygge en faktisk omstendighet som er rettslig relevant i en sak. Innhenting av bevis på det privatrettslige området får ikke like stor oppmerksomhet i media, men er ikke desto mindre viktig i den enkelte sak. Man kan for eksempel tenke seg at en arbeidsgiver ønsker å sikre seg opplysninger om en ansatt i forbindelse med en mulig arbeidsrettssak, og gjør dette for eksempel ved å innhente opplysninger om den ansattes bevegelser på Internett eller lignende. Informasjonen vil kunne benyttes av arbeidsgiver til å underbygge en faktisk omstendighet som er rettslig relevant i tvisten mellom partene.

Felles for begge kategorier digitale bevis er at opplysningene som innhentes svært ofte vil inneholde personopplysninger.[4] Informasjon fra både anropslogger, informasjon om passering av bomringer og elektroniske spor på Internett vil være eller inneholde personopplysninger. Det er ikke fri adgang til å behandle[5] personopplysninger, verken på det privatrettslige eller det strafferettslige området. Problemstillingene og spørsmålene som reises i fortsettelsen av denne utredningen er dermed primært av personvernrettslig karakter. De mer overordnede personvernrettslige og personvernetiske problemstillingene ved innsamling og bruk av digitale bevis er uansett sentrale både i forhold til strafferetten og i forhold til privatretten. Også de strafferettslige aspektene er imidlertid viktige, særlig i forbindelse med det offentliges innhenting av digitale bevis.

[4] Se personopplysningsloven § 2, nr 1. For en nærmere gjennomgang av begrepet "personopplysninger", se avsnitt 4.1.

[5] Se personopplysningsloven § 2 nr 2. For en nærmere gjennomgang av begrepet "behandling", se avsnitt 5.1.

Hovedvekten i utredningen vil ligge på de situasjonene der det beviste saksforholdet vil bli prøvet av en domstol, men også situasjoner der det ikke er sannsynlig at saksforholdet blir gjenstand for domstolsbehandling, vil bli tatt opp.

2. PRINSIPPET OM FRI BEVISFØRING

Prinsippet om fri bevisfremleggelse er et grunnleggende prinsipp i norsk rett, som gjelder både på strafferettens område og i sivile saker. Prinsippet innebærer at partene som hovedregel fritt kan legge frem de bevisene de ønsker.

En domstol kan imidlertid avvise bevisfremleggelsen (såkalt bevisavskjæring), med hjemmel i de ulovfestede reglene om bevis ervervet på ulovlig eller utilbørlig måte. Ettersom det rettslige utgangspunktet er prinsippet om fri bevisføring, krever slik bevisavskjæring i utgangspunktet en positiv hjemmel. På grunnlag av rettspraksis er det utviklet regler for avskjæring av ulovlig ervervet bevis. Retten kan i særlige tilfeller nekte bevis fremlagt dersom fremleggelse vil medføre en krenkelse av tungtveiende personvern- eller rettssikkerhetshensyn.[6] Bevisavskjæring etter disse reglene forutsetter at det dreier seg om et bevis som er ervervet på ulovlig eller utilbørlig måte, og som etter en bred avveining av så vel de prinsipielle som konkrete hensyn heller ikke bør tillates ført for retten. Slike saker reiser altså to spørsmål; om det dreier seg om et ulovlig eller utilbørlig bevis, og i så fall om beviset likevel skal tillates ført for retten.

I straffeprosessen har en vært opptatt av bevisavskjæring der beviset er ervervet på ulovlig måte. Denne problemstillingen har ikke vært tilsvarende utførlig omhandlet innenfor sivilprosessen, men er likevel sentral også her. Omfanget av privates innhenting av bevis gjennom ulovlige metoder, som for eksempel industrispionasje eller ulovlig telefonavlytting, er ikke klarlagt, men at det foregår er det ikke tvil om. Også i sivilprosessen er det sikkert at bruken av et ulovlig ervervet bevis er avskåret i visse tilfeller og det er en grunnleggende forutsetning for at opplysningene skal kunne legges frem som bevis i retten, at innhenting av bevisene har vært lovlig.

Problemstillingen rundt ulovlig ervervede bevis har to sider.

For det første kan det dreie seg om ulovlig innhentede bevis som åpenbart ikke kan legges frem, ettersom bruken vil innebære en ytterligere rettskrenkelse i forhold til den opplysningene knytter seg til. Et eksempel kan være en situasjon hvor en part ved ulovlig telefonavlytting har fått tak i opplysninger som den annen part ikke plikter å forklare seg om for retten. Her er opplysningene for det første innhentet ulovlig, og for det andre vil en eventuell fremleggelse av opplysningene innebære en ytterligere krenkelse av den andre partens rettigheter.

For det andre kan man stå ovenfor bevis som er fremskaffet på ulovlig måte, men som man ellers ville hatt rett til å benytte. Dette kan for eksempel være opplysninger som er innhentet uten rettslig grunnlag, jf personopplysningsloven § 8 og § 9 og straffeprosessloven § 224, og dermed er behandlet i strid med loven. Dersom man hadde hatt rettslig grunnlag, for eksempel samtykke fra den registrerte eller at det foreligger en anmeldelse, ville opplysningene fritt kunne legges frem for retten. I slike tilfeller kan det være mer nærliggende å tenke seg at man skal tillate at opplysningene blir fremlagt for retten, og at man i stedet reagerer mot den ulovlige innhentingen av bevis på andre måter. Et slikt system vil imidlertid undergrave lovens krav om rettslig grunnlag, og vil også kunne oppmuntre til bruk av ulovlige metoder. Domstolene har derfor valgt å behandle spørsmålet under vurderingen av om det skal foretas bevisavskjæring, og ikke som et særskilt spørsmål på siden av dette.

---

[6] Se avgjørelsene inntatt i Rt 91/616, Rt 97/795 og Rt 01/668.

Et annet spørsmål er hvilken vekt digitale bevis skal ha i bevisbedømmelsen. Norsk rett bygger på prinsippet om fri bevisbedømmelse, som bygger på den oppfatning at dommeren best kan finne frem til sannheten i saken hvis han får bedømme bevisene uten å være bundet av lovregler.[7] Vi har ikke gjennomført forskning for å kartlegge hvilke typer innsigelser og uttrykk for tvil norske domstoler har knyttet til digitale bevis og hvilke generell lærdom vi eventuelt kan trekke av en slik praksis. Manglende kunnskap om rettspraksis, kombinert med prinsippet om fri bevisbedømmelse, gjør det derfor vanskelig å angi noen prosessuelle og/eller empirisk baserte retningslinjer for hvorledes digitale bevis vil kunne bli vektlagt. I tillegg kommer at digitale bevis spenner over et meget vidt felt og at slike bevis – ikke minst – vil befinne seg i ulike bevismessige sammenhenger. Således er det grunn til å tro at intensiteten i prøvingen av digitale bevis vil variere avhengig av om det (nesten) utelukkende er digitale bevis i en sak eller om de digitale bevisene inngår blant en rekke andre bevis. Likevel er det etter vår mening mulig å gi noen generelle råd på basis av generelle rettslige krav. Dette gjelder primært krav til sikker/entydig identifisering av personer (avsnitt 4.5) og krav til opplysningskvalitet og -integritet (avsnitt 4.6).

3. OVERSIKT OVER SENTRAL LOVGIVNING MV VEDRØRENDE PERSONOPPLYSNINGER

3.1 Personopplysningsloven og annen privatrettslig personvernlovgivning

På det privatrettslige området er det først og fremst Lov om behandling av personopplysninger av 14. april 2000 nr. 31 (”personopplysningsloven”) med tilhørende forskrifter[8] som danner det rettslige grunnlaget for behandling av personopplysninger. Loven trådte i kraft 1. januar 2001. Det er denne loven som i utgangspunktet gjelder for alle personers og virksomheters behandling av personopplysninger, herunder opplysninger som kan være aktuelle som digitale bevis. Innenfor bestemte saksområder kan særlovgivning i større eller mindre utstrekning gjelde foran personopplysningsloven. Dette gjelder primært for helseinstitusjoners behandling av helseopplysninger, se helseregisterloven.[9] Andre lover gjelder for bestemte registre, for eksempel folkeregisterloven[10] og strafferegisterloven.[11] Mens helseregisterloven er en ”moderne” personopplysningslov som langt på vei erstatter personopplysningsloven, har slike ”registerlover” en annen oppbygning og innhold, noe som innebærer at personopplysningsloven likevel får forholdsvis stor betydning i samspill med særloven. Annen lovgivning supplerer lovgivning vedrørende personopplysninger og -registre på viktige måter. Dette gjelder særlig regelverk som påbyr sikring av opplysninger.[12] Slik regelverk, og spørsmålet om regelverket er fulgt, kan konkret ha stor betydning for den

---

[7] Johs. Andenæs, Norsk Straffeprosess, Bind I, 3. utg. 2000, side 183.

[8] Forskrift til personopplysningsloven (personopplysningsforskriften) av 15. desember 2000.

[9] Lov om helseregistre og behandling av helesopplysninger av 18. mai 2001 nr 24.

[10] Lov om folkeregistrering av 16. januar 1970 nr 1.

[11] Lov om strafferegistrering av 11. juni 1971 nr 52.

[12] Se for eksempel forskrift til kredittilsynsloven om bruk av informasjons- og kommunikasjonsteknologi (IKT), av 21. mai 2003, lov om elektronisk signatur av 15. juni 2001 nr 81 og forskrift om elektronisk kommunikasjon med og i forvaltningen av 25. juni 2004 nr 988.

konkrete bevisbedømmelsen. For øvrig kommer vi ikke nærmere inn på spørsmål vedrørende særlovgivning, men avgrenser fremstillingen til de alminnelige bestemmelsene om behandling av personopplysninger.

3.2 Personvern i strafferetten og straffeprosessen

På det strafferettslige området oppstilles det en rekke bestemmelser som er av personvernrettslig karakter. Straffeloven § 390 og § 390a er klare personvernrettslige bestemmelser, som verner privatlivets fred. Etter § 390 straffes den som krenker privatlivets fred ved å gi offentlig meddelelse om personlige eller huslige forhold. Bestemmelsen kommer til anvendelse også når behandling av personopplysninger skjer for private og personlige formål. Dette i motsetning til personopplysningsloven, som ikke gjelder behandlinger for rent personlige eller andre private formål. Bestemmelsen i straffeloven § 145a, regulerer ulovlig telefonavlytting, og beskytter dermed den personlige integritet. Det samme gjelder for eksempel for straffeloven § 145 som setter straff for brevbrudd.

Flere av de handlinger som er straffebelagt i straffeloven (brevbrudd, avlytting mv), kan likevel være lovlig for politiet å utføre som ledd i etterforskning og innsamling av bevis. Lovligheten vil imidlertid være avhengig av en rekke vilkår som ikke vil bli nærmere behandlet her. Det er imidlertid bare politiet som kan utføre slike handlinger som ellers rammes av straffeloven, og slike handlinger står med andre ord ikke til disposisjon for private som ønsker å sikre digitale bevis. I forhold til innsamling og bruk av bevis i den konteksten som her drøftes, vil dessuten bestemmelsene i straffeprosessloven §§ 224, 225 og 226 kunne sies å være av personvernrettslig karakter. Bestemmelsene fastsetter når etterforskning kan igangsettes, hvem som skal etterforske og spørsmålet om formålet for og omfanget av etterforskningen. Fordi etterforskningen går ut på å sikre bevis, og disse bevisene vil være opplysninger om personer, kan bestemmelsene indirekte sies å ivareta personvernet til de personer det er aktuelt å etterforske.

3.3 Ulovfestet rett

Lovgivningen på det privatrettslige og strafferettslige området må suppleres av ulovfestet rett, og da spesielt i form av rettsavgjørelser. Særlig interessante i forhold til innsamling og bruk av bevis er gatekjøkkenkjennelsen[13], fotobokskjennelsen[14], e-postdommen[15] og tappetårn-kjennelsen[16]. Disse avgjørelsene er avsagt under den personregisterloven[17] som nå er opphevet og erstattet av personopplysningsloven, men har likevel rettskildemessig verdi. De siste årene er det avsagt en rekke dommer hvor personopplysningsloven er benyttet, og ut i fra den problemstillingen som drøftes her, er det særlig avgjørelser avsagt i tilknytning til privat bruk av e-post i arbeidsforhold som er interessante.

---

[13] Rt 91/616

[14] Rt 90/1008

[15] RG 93/77

[16] Kjennelse fra Agder lagmannsrett fra 5. oktober 1992, publisert i Lov og Data 1993 nr 34, side 8. I denne saken ble bevis hentet fra hemmelig overvåkning ikke tillatt ført som bevis i en arbeidsrettssak.

[17] Personregisterloven av 9. juni 1978 nr 48.

3.4 Internasjonale regler

De norske reglene på personvernområdet suppleres av en rekke internasjonale regler. Det vil favne for vidt i denne utredningen å gjennomgå disse i detalj, og det avgrenses derfor til å nevne de mest sentrale.[18]

Europaparlamentets og rådets direktiv 95/46/EF om beskyttelse av fysiske personer ved behandling av personopplysninger, vedtatt 24. oktober 1995, er den mest sentrale kilden internasjonalt. Personverndirektivet stiller visse minstekrav til nivået på den nasjonale personvernlovgivningen, og har således vært en viktig intern premissleverandør for utforming av regelverk på personvernområdet i Norge. Direktivet er folkerettslig bindende for Norge, men kommer ikke til anvendelse på "statens virksomhet på det strafferettslige område", se direktivets artikkel 3 nr 2.

Et annet sentralt direktiv er direktiv 2002/58/EF av 12. juli 2002, om behandling av personopplysninger og beskyttelse av privatlivets fred i den elektroniske kommunikasjonssektoren. Direktivet omhandler viktige områder innen elektronisk kommunikasjon, som blant annet sikring av data og kommunikasjon, lagring og viderebruk av trafikk- og debiteringsdata, utstedelse av spesifiserte regninger og uønsket markedsføring.

Forut for personverndirektivet ligger blant annet Europarådets konvensjon om personvern (Europarådskonvensjonen), vedtatt 28. januar 1981, som angir en rekke overordnede prinsipper og minimumsstandarder for personvernet, som blant annet legger føringer på utformingen av regelverket.

En siste viktig internasjonal kilde som skal nevnes her er Den Europeiske Menneskerettskonvensjonen fra 1950 (EMK), og da særlig Artikkel 8 om vern for privatliv og familieliv.

De nevnte direktivene og konvensjonene binder Norge og utgjør en ramme for innholdet av norsk lovgivning og rettspraksis. Dette innebærer bl.a. at Norge ikke står fritt når innholdet av personvern skal fastsettes. Dersom en for eksempel skulle ønske å endre på norsk lovgivning for i større grad å legge til rette for privat innsamling av digitale bevis, blir dette ikke bare et internt norsk politisk spørsmål. I tillegg må ønskene om endringer av rettstilstanden vurderes ut i fra Norges internasjonale forpliktelser.

[18] En omfattende oversikt finnes i Schartum og Bygrave "Personvern i informasjonssamfunnet", Fagbokforlaget 2004, s 75 – 99.

4. NÆRMERE OM PERSONOPPLYSNINGSLOVEN

4.1 Noen innledende begrepsavklaringer

Før vi går nærmere inn på de bestemmelsene i personopplysningsloven som har betydning for vurdering av privates innsamling av digitale bevis, er det nødvendig å forklare enkelte av de mest sentrale begrepene i loven.

Loven regulerer behandling av "personopplysninger", og dette begrepet er derfor helt avgjørende for hvilke forhold som reguleres av loven. Personopplysninger er *opplysninger* og *vurderinger* som kan knyttes til en identifiserbar enkeltperson, jf personopplysningsloven § 2 nr 1. Med "opplysninger" forstår man mer statiske former for opplysninger om en person, som for eksempel navn, adresse og alder. Med "vurderinger" forstås mer sammensatt informasjon, ofte basert på en eller flere opplysninger.

For at en opplysning skal regnes som en personopplysning etter loven, må den kunne knyttes til en bestemt person. Tilknytningen kan være både direkte og indirekte. Direkte tilknyttede opplysninger *er* knyttet til personen, for eksempel navn, personnummer og fingeravtrykk. Indirekte tilknyttede opplysninger *kan* knyttes til personen, for eksempel opplysninger om telefonnummer, bostedsadresse, bilregistreringsnummer eller yrkestittel. Det er altså ikke noen vilkår for at loven skal komme til anvendelse at en vet hvilken person det foreligger opplysning om – muligheten for identifisering er nok.

Personopplysningsloven skiller mellom personopplysninger (generelt) og sensitive personopplysninger, og oppstiller strengere krav for behandling av sensitive personopplysninger enn for andre personopplysninger. Sensitive personopplysninger er i loven definert som opplysninger om rasemessig eller etnisk bakgrunn, politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold samt opplysninger om medlemskap i fagforeninger, se § 2 nr 8. Det er i utgangspunktet opplysnings*typen* som er avgjørende for om en opplysning skal anses som sensitiv eller ikke. Dersom behandlingsansvarlige for eksempel setter opp en loggrutine som registrerer opplysningstyper som klart viser straffbare disposisjoner, vil disse loggopplysningene være sensitive. Derimot ikke dersom loggopplysningene kun gjelder uønskede disposisjoner som ikke er straffbare. Selv om opplysningstypen ikke i seg selv er sensitiv, er det grunn til å anse opplysningene som sensitive dersom den behandlingsansvarlige forventer at opplysningsverdiene regelmessig vil uttrykke mistanke om straffbare forhold. En URL-adresser er i seg selv ikke en sensitiv opplysningstype. Likevel kan de bedømmes som sensitive dersom behandlingsansvarlige for eksempel logger adresser med semantiske elementer som antas å vise mistanke om straffbare forhold. Dersom det skal behandles sensitive personopplysninger gjelder det skjerpede krav til rettslig grunnlag for behandlingen. I tillegg kommer det – i utgangspunktet – krav om konsesjon fra Datatilsynet, se straks nedenfor.

Opplysninger om juridiske personer omfattes som hovedregel ikke av den personopplysningsloven.[19] Dette betyr at innsamling av bevis knyttet til juridiske personer, for eksempel skatteunndragelse eller korrupsjon hos en bedrift, i utgangspunktet vil falle utenfor de problemstillingene og spørsmålene som reises her. Dette utgangspunktet må imidlertid nyanseres. Bevis knyttet til juridiske personer vil svært ofte også være opplysninger om

[19] Unntak er gitt for behandling av personopplysninger i kredittopplysningsvirksomhet.

fysiske personer, ettersom det straffbare forholdet rent praktisk må utføres av en eller flere fysiske personer. Politiets eller privates etterforskning av for eksempel korrupsjon vil inneholde en rekke opplysninger knyttet til virksomheten, som omfatter opplysninger om for eksempel daglig leders drift og håndtering av virksomheten og forholdet som etterforskes. Slike opplysninger om enkeltpersoners handlinger mv vil klart være "personopplysninger", derimot ikke regnskapsopplysninger og andre virksomhetsopplysninger som er uten særlig tilknytning til en person. Grensene mellom personopplysninger og virksomhetsopplysninger kan være vanskelig å trekke, og i praksis kan dette føre til at de strengeste normene (vedrørende personopplysninger) blir anvendt på alle opplysninger.[20]

Personopplysningsloven gjelder all "behandling" av personopplysninger, og dette begrepet dekker "alt" en kan tenke seg å gjøre med opplysninger (innsamling, lagring, sletting, retting mv). For å komme inn under loven må behandlingen skje "elektronisk" eller opplysningene må befinne seg i et personregister eller bli samlet inn for å inngå i et slikt register. "Elektronisk" og "digital" må antas å ha det samme meningsinnholdet, og behandling av digitale bevis som kan knyttes til en enkeltperson, omfattes derfor av loven. Det spiller ingen rolle på hvilken måte opplysningene fremkommer. Opplysninger som fremkommer ved skrift, stillbilde, video og ulike typer sensorer er omfattet så lenge opplysningene blir behandlet elektronisk eller er knyttet til et personregister. Derfor vil alle digitale bevis reguleres av samme lov uansett hvorledes opplysningene fremkommer.

Personopplysningsloven pålegger den "behandlingsansvarlige" en rekke plikter ved behandling av personopplysninger. De samme forpliktelsene vil langt på vei også foreligge ved behandling av opplysninger etter straffeprosessloven, selv om de samme begrepene ikke benyttes i strafferetten. "Behandlingsansvarlig" er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes, jf § 2 nr 4.[21] Det er den behandlingsansvarlige som utad står ansvarlig for at grunnlaget for behandlingen av personopplysningene er lovlig og at behandlingen for øvrig skjer i henhold til lovens regler, og som kan saksøkes og pådra seg straffansvar for overtredelse av lovens bestemmelser. Den behandlingsansvarlige vil etter loven normalt være organer eller personer med sivilprosessuell partsevne, det vil si at de kan saksøke og saksøkes. Der behandlingen av opplysningene skjer i regi av en bedrift, vil bedriftens ledelse være behandlingsansvarlig. Innenfor offentlig sektor vil det som hovedregel være det enkelte forvaltningsorgan eller etat, representert ved dens ledelse, som er behandlingsansvarlig. Bare organer og etater som kan saksøkes kan være behandlingsansvarlige. I mange tilfeller vil man også kunne ha delt behandlingsansvar, for eksempel mellom to eller flere bedrifter hvor samtlige har større eller mindre kontroll og innflytelse over behandlingen av personopplysningene.

Dersom private virksomheter eller personer samler inn digitale bevis og selv avgjør hvorledes dette skal skje, vil de anses som "behandlingsansvarlige" og således være pålagt en rekke plikter etter loven. Dersom innsamlingen av bevis er tilrettelagt og skjer etter avtale med

---

[20] Datatilsynet har uttalt at behandling av opplysninger som for eksempel navn og e-postadresse til kontaktpersoner hos ulike virksomheter ikke faller inn under loven. En leverandørs registrering av opplysninger om innkjøpssjef Per Berg hos Bedrift AS vil etter dette ikke omfattes av loven. Begrunnelsen er at det ikke er Per Bergs egne private opplysninger som er interessante for leverandøren, men han som kontaktperson hos en mulig kunde. Hensynet til personvernet gjør seg dermed ikke gjeldende slik som ved markedsføringshenvendelser rettet mot Per Berg selv.

[21] Begrepet "behandlingsansvarlig" tilsvarer i hovedsak begrepet registeransvarlig etter den gamle personregisterloven.

politiet eller andre, vil disse tilretteleggerne/oppdragstakerne kunne ses som behandlingsansvarlige, eventuelt kan en komme til at det foreligger et delt behandlingsansvar. Handler den private på oppdrag fra politiet eller andre, vil den private kun være "databehandler" med langt mer beskjedne plikter etter loven enn det som gjelder for den behandlingsansvarlige. Det er uansett avgjørende at det er klargjort hvem som skal stå som behandlingsansvarlig og (eventuelt) databehandler i forhold til innsamlingen av digitale bevis.

Loven gir "den registrerte" en rekke rettigheter og etablerer plikter for den behandlingsansvarlige overfor registrerte personer. Den registrerte er den som en personopplysning kan knyttes til, jf lovens § 2 nr 6. Særlig gjelder dette registrertes rett til innsyn i opplysninger om ham selv, og plikten den behandlingsansvarlige har til å varsle den registrerte om forestående behandling av opplysninger om den registrerte, se nedenfor.

4.2 Nærmere om personopplysningslovens virkeområde

Loven gjelder i utgangspunktet for all elektronisk behandling av opplysninger, uavhengig av sektor. Det er imidlertid gjort unntak for behandling av personopplysninger som skjer til rent personlige eller private formål, jf § 3, 2. ledd. Loven gjelder for eksempel ikke for en person som samler inn og lagrer opplysninger om sin egen slekt på sin egen pc. Innsamling og behandling ellers av digitale bevis kan aldri komme inn under dette unntaket. Det er også gjort omfattende unntak for behandling av personopplysninger når formålet utelukkende er for kunstnerisk, litterær eller journalistisk formål, herunder opinionsdannende, jf § 7.[22] Innsamling av digitale bevis kan tenkes å komme inn under denne unntaksbestemmelsen. Dette kan for eksempel gjelde dersom en person samler inn digitale bevis for å styrke en åpen argumentasjon mot en person. En forfatter skriver for eksempel om korrupsjon og samler inn opplysninger som kan fungere som digitale bevis som en del av sitt researcharbeid. For at unntaket skal gjelde, må opplysningene imidlertid bare brukes til for eksempel slike journalistiske/opinionsdannende formål. Dersom opplysningene også brukes på annen måte (for eksempel overleveres politiet), gjelder personopplysningsloven fullt ut.

Personopplysninger som behandles i henhold til rettspleielovene (for eksempel domstolloven, straffeprosessloven, tvistemålsloven og tvangsfullbyrdelsesloven), er unntatt fra personopplysningsloven, se personopplysningsforskriften § 1-3. Når digitale bevis overleveres politiet, vil opplysningene derfor løftes ut av personopplysningsloven og inn i straffeprosesslovens og rettspleielovgivningens regime for øvrig. Dette omhandles nærmere nedenfor i avsnitt 5.

Personopplysningsloven gjelder i utgangspunktet kun for behandlingsansvarlige som er etablert i Norge eller som gjør bruk av utstyr som befinner seg i landet, jf § 4. Utenlandske personer og virksomheter som ikke er etablert i Norge men i et EØS-land, kan samle inn digitale bevis på norsk territorium uten å komme inn under loven. I stedet gjelder vedkommende EØS-lands personvernlovgivning. Fordi det ligger et felles direktiv bak alle EØS-lands lovgivning på området, innebærer det likeartet regulering uansett EØS-land.

[22] I så fall er det kun bestemmelsene i lovens §§ 13-15, § 26, §§ 36-41, jf kapittel VIII som kommer til anvendelse.

4.3 Krav til rettslig grunnlag for innsamling av personopplysninger

For at det over hode skal være lovlig for private å behandle personopplysninger som kan være digitale bevis, må de ha et alminnelig rettslig grunnlag for behandlingen, jf pol § 8. For sensitive opplysninger, for eksempel opplysninger om mistanke om straffbare forhold, er det tilleggskrav til rettslig grunnlag i § 9. For slike opplysninger må med andre ord både kravene i § 8 og § 9 være tilfredsstilt. Bestemmelsene er bygget opp over samme lest, og vil derfor bli fellesbehandlet her. Tre typer rettslig grunnlag er felles for de to bestemmelsene:

- Behandling av personopplysninger er hjemlet i lov,
- Behandlingen skjer i samsvar med samtykke fra den registrerte, eller
- Behandlingen må anses å være nødvendig i tråd med lovens alternativer.

Etter § 9 kan alle i tillegg behandle opplysninger som den registrerte selv frivillig har gjort alminnelig kjent. Forutsetningen er imidlertid at det bare er slike opplysninger som blir behandlet. Slike opplysninger kan med andre ord samles inn som bevis, uten lovhjemmel, samtykke eller nødvendig grunn, men vilkårene for at dette skal være et tilstrekkelig grunnlag er for strenge til at dette kan få praktisk verdi. I realiteten kreves det med andre ord lovhjemmel, samtykke eller at behandlingen anses for ”nødvendig”.

På generelt grunnlag er det antatt at det viktigste grunnlaget for behandling av personopplysninger etter § 8 er den registrertes samtykke. Lovteksten og forarbeidene gir imidlertid ikke full klarhet i om i hvilken grad det er anledning til å unnlate å innhente samtykke og i stedet basere behandlingen på ”nødvendighet”. En prinsipiell avgjørelse fra Personvernnemnda gir nærmere anvisning på forholdet mellom samtykke og nødvendighetsbegrunnelse som rettslig grunnlag for å behandle personopplysninger.[23] Saken gjaldt valg mellom samtykke og nødvendighetsgrunn i et helseforskningsprosjekt. Personvernnemnda understreket at selv om samtykke er hovedregelen, innebærer ikke dette at denne regelen ikke kan fravikes. Nødvendighetsbegrunnelsene i pol § 8 f kunne imidlertid etter nemndas mening ikke fritt velges i stedet for samtykke ut i fra rene hensiktsmessighetsbetraktninger. Man måtte i stedet ta hensyn til de konkrete argumentene for å velge nødvendighetsbegrunnelsen, og vurdere hvor tungtveiende disse er i den konkrete sak: ”For at man skal kunne gjøre et avvik fra hovedprinsippet, må det derfor foreligge en begrunnelse. Denne begrunnelsen kan […] ikke bare være en ren hensiktsmessighetsbetraktning, f eks å unngå kostnader, spare tid eller lignende – selv om slike begrunnelser selvsagt også må vurderes konkret i forhold til den enkelte sak.” Personvernnemnda godtok deretter de forskningsmetodiske argumentene for å velge nødvendighetsalternativet i pol § 8 bokstav f, og fant de anførte argumentene vedrørende forskningsmetode tilstrekkelig tungtveiende. Selv om samtykke er det primære rettslige grunnlaget, kan det med andre ord gjøres unntak som er saklig begrunnet ut i fra noe mer enn rent økonomiske og praktiske forhold.

Betydningen av samtykke som rettslig grunnlag for innhenting av bevis, avhenger i stor grad av om innsamlingen skjer proaktivt eller reaktivt. Ved reaktiv innsamling, vil samtykke normalt være forholdsvis lite aktuelt. Ved proaktiv innsamling vil samtykke derimot være praktisk viktig. Dette gjelder i alle fall tilfelle der det ikke foreligger intensjoner om ulovlige/uakseptable handlinger (en ansatt kan for eksempel mangle respekt for internt forbud

[23] Se sak nr. 2004/01 STAMI, http://www.personvernnemda.no/vedtak/2004_1.html.

mot å laste ned musikk på virksomhetens anlegg). Uansett vil det i slike situasjoner sosialt sett være vanskelig å nekte avgivelse av samtykke.

For at samtykket skal være gyldig må det være informert, se pol § 2 nr 7, dvs. den behandlingsansvarlige må informere hva formålet med behandlingen er og hvordan opplysningene skal brukes. Dersom det ved innhenting av samtykke er informert om muligheten for å overlevere materiale som kan være bevis til politiet, er det derfor neppe tvil om at arbeidsgiver har rett til slik overlevering. Mer tvilsomt er spørsmålet dersom det ikke er nevnt noe om denne muligheten. Arbeidsgiver vil i en viss utstrekning kunne definere nye formål. Denne adgangen er imidlertid begrenset, noe vi kommer tilbake til nedenfor. Dersom det ikke er aktuelt å basere behandlingen på den ansattes samtykke, må arbeidsgiver (som behandlingsansvarlig) sikre seg rettslig grunnlag for behandlingen på annet vis, for eksempel ved å identifisere en nødvendig grunn i et av alternativene i personopplysningsloven § 8 bokstavene a – f. Dersom arbeidsgiver ikke sikrer seg rettslig grunnlag for behandlingen som omfatter utlevering av opplysninger til politiet, er utleveringen av personopplysningene ulovlig og han risikerer at opplysningene blir avskåret som bevis. Det er imidlertid flere eksempler fra rettspraksis på at domstolene har tillatt fremleggelse av slike opplysninger, selv om de er innhentet ulovlig – for eksempel fordi behandlingen ikke har hatt det nødvendige rettslige grunnlaget.

Dersom det er fastsatt i lov at behandling av personopplysninger kan finne sted, er dette et mulig rettslig grunnlag for innsamling av bevisene. Slik særlovgivning går foran bestemmelsene i personopplysningsloven, noe som innebær at den lovbestemte behandlingen av personopplysninger kan være lovlig selv om den ikke tilfredsstiller vilkår og krav til behandlinger gitt i eller i medhold av personopplysningsloven.

Hjemmelskravet i personopplysningsloven er relativt, noe som innebærer at det kreves klarere rettslig grunnlag jo større de personvernrettslige konsekvensene av behandlingen vil være for den registrerte. Denne forståelsen underbygges også av Den europeiske menneskerettighetsdomstolens (EMD) praksis i forhold til EMK artikkel 8, annet ledd. I en rekke saker fra EMD, hvor EMK Artikkel 8 har stått sentralt, har domstolen således kommet til at det har forekommet en krenkelse av EMK artikkel 8, fordi lovhjemmelen er for svak.

EMK artikkel 8 lyder som følger:

> ” 1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.
>
> 2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.”

EMD har fastslått at offentlige myndigheters behandling av opplysninger om enkeltindivider uten deres samtykke eller kunnskap, i utgangspunktet vil være å regne for et inngrep i deres rett til privatliv. Et slikt inngrep må da rettferdiggjøres i henhold til annet ledd i artikkel 8, som innebærer at behandlingen må oppfylle flere kumulative kriterier. Det første sett av kriteriene, og det som er relevant her, er at behandlingen må ha et rettslig grunnlag som tilfredsstiller vanlige prosessuelle rettssikkerhetskrav. Lovhjemmelen som påberopes må være tilstrekkelig klar og tilgjengelig for borgerne, slik at de innenfor rimelige grenser kan forutsi konsekvensene av lovhjemmelen. I Kruslin-saken[24], uttalte domstolen at: ”*In short, French*

[24] Sak nr 4/1989/164/220.

law, written and unwritten, does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. This was truer still at the material time, so that Mr Kruslin did not enjoy the minimum degree of protection to which citizens are entitled under the rule of law in a democratic society."

Det er imidlertid usikkert hva artikkel 8 krever av private aktører som behandler opplysninger, ettersom bestemmelsen primært beskytter enkeltindivider mot inngrep fra offentlige myndigheter.

Et meget relevant eksempel på særlovgivning er bestemmelsen i straffeprosessloven § 206. Bestemmelsen innebærer at enhver kan ta beslag i bevis, når den mistenkte treffes eller forfølges på fersk gjerning eller ferske spor.

Som tidligere nevnt, kan en behandlingsansvarlig i visse tilfelle behandle personopplysninger dersom det er "nødvendig" for å ivareta nærmere angitte interesser som følger av lovens § 8 bokstavene a) til f). Bestemmelsen er primært aktuell i situasjoner der det ikke foreligger lovhjemmel eller samtykke fra de aktuelle personene, jf ovenfor. Spørsmålet her er om noen av alternativene i § 8 kan danne rettslig grunnlag for privates innsamling av digitale bevis. Trolig er det bare det siste alternativet i bokstav f som kan være aktuelt. Bestemmelsen er meget åpen og vurderingspreget og kan derfor i konkrete saker tenkes å gi tilstrekkelig rettslig grunnlag. Det er likevel langt fra noen automatikk her. Nedenfor skal vi derfor kort gjennomgå noen hovedpunkter ved anvendelse av bestemmelsen.

Personopplysningsloven § 8 bokstav f) åpner for behandling av opplysninger dersom behandlingen er nødvendig for at den behandlingsansvarlige eller en tredjeperson som opplysningene utleveres til kan ivareta en berettiget interesse. Forutsetningen er at hensynet til den registrertes personvern ikke overstiger denne interessen. Vi står med andre ord overfor en bred interesseavveining. I tilfelle av privates innsamling av digitale bevis, blir spørsmålet for det første om den private (behandlingsansvarlige) har en berettiget interesse i å gjøre dette. Dernest blir spørsmålet om en slik berettiget interesse skal veie mer enn den registrertes interesse i personvern. Det er vanskelig å si noen generelt om denne avveiningen. Likevel kan det imidlertid sies at innsamling og overføring til politiet av digitale bevis mot en person vil innebære en klar og alvorlig personvernkrenkelse. Den "berettigende interessen" som motiverer ønsket om å behandle personopplysningene må derfor være sterk. Desto alvorligere den kriminelle handlingen de digitale bevisene gjelder, desto sterkere må den berettigede interessen anses å være. Dersom den privates innsamling av bevisene kan antas å være nødvendige for å bevise den straffbare handlingen, er dette selvsagt et ytterligere moment som taler for at det foreligger en tilstrekkelig nødvendig grunn i samsvar med personopplysningsloven § 8 bokstav f.

Det er den behandlingsansvarlige selv som i første omgang må vurdere om det foreligger et tilstrekkelig rettslig grunnlag. Datatilsynet kan imidlertid overprøve denne vurderingen, og dette kan enten skje som ledd i konsesjonsbehandling eller i tilknytning til tilsynets kontrollvirksomhet. Datatilsynet kan i slike sammenhenger eventuelt stille vilkår for at behandling av personopplysninger som digitale bevis kan skje.

I dette avsnittet har vi fremholdt at behandling av personopplysninger som digitale bevis må ha et rettslig grunnlag for å være lovlig. Dersom bevis er ulovlig innsamlet vil det kunne bli avskåret av retten. Selv om det ikke er noen automatikk i at retten avskjærer ulovlig innsamlede bevis er det derfor viktig å forsikre seg om eksistensen av et tilstrekkelig rettslig grunnlag. Om rettslig grunnlag foreligger eller ikke, må vurderes konkret i forhold til

personopplysningsloven § 8 og § 9 som gir anvisning på tre typer rettslig grunnlag; samtykke, lovhjemmel og nødvendig grunn slik dette er spesifisert i loven.

4.4 Krav om formålsangivelse

Personopplysningsloven § 11 oppstiller grunnkrav til behandling av personopplysningene. Bestemmelsen stiller både krav til formålsangivelse og til opplysningskvalitet. Formålsangivelsen har direkte betydning for krav til opplysningskvalitet. Formålet har også betydning for avgivelse av samtykke (jf ovenfor), fordi formålet må inngå i den informasjonen som skal gis og som dermed beskriver omfanget av hva det samtykkes til.

Personopplysninger kan bare behandles til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet. Formålet skal være uttrykkelig angitt av den behandlingsansvarlige, og kan ikke være for vidt eller upresist. Ved innsamling av bevis må formålsangivelsen omfatte behandling av personopplysninger som bevismiddel. Innsamling av bevis som skjer for å ivareta den behandlingsansvarliges interesser må alltid anses å være saklig begrunnet i virksomheten. Derimot neppe dersom innsamlingen skjer for å ivareta interesser utenfor virksomheten. Kravet til at formålet må være uttrykkelig angitt innebærer neppe at det direkte må sies at formålet gjelder innsamling av bevis. Det kan være nok at formålet er beskrevet som oppklaring av sikkerhetsbrudd e.l. Uansett må det klart fremgå at det dreier seg om mer enn ivaretakelse av vanlig intern sikkerhet. Formålsangivelsen må med andre ord være slik at det fremstår som en nærliggende mulighet at personopplysninger vil kunne bli overlevert til politiet som digitale bevis.

Hovedregelen er at opplysningene kun kan behandles i samsvar med de opprinnelige formål(ene), det vil si i overensstemmelse med de formålene som er fastsatt før behandlingen av personopplysninger tar til. Opplysningene kan imidlertid behandles til nye formål som blir formulert på et senere tidspunkt. Forutsetningen er at slike nye formål ikke ”*er uforenlig med det opprinnelige formålet med innsamlingen*”. Dersom dette vilkåret ikke kan tilfredsstilles, må det innhentes nytt samtykke fra den registrerte. Spørsmålet om et nytt formål er uforenelig med de opprinnelige formålene eller ikke, må avgjøres ut i fra en vurdering av hvem som kan sies å tjene på at formålet blir realisert. Dersom det opprinnelige formålet er knyttet til ivaretakelsen av de registrertes egne interesser, vil formålet å samle inn digitale bevis mot de samme personer trolig bli ansett å være ”uforenlig”. Utgangspunktet blir motsatt dersom formålet er å føre intern kontroll med at et informasjonssystem blir brukt i samsvar med gjeldende regler, og formålet utvides til også å gjelde bistand til politiets etterforskning av straffbare handlinger. I så fall vil både det opprinnelige og det nye formålet gjelde kontroll av den registrerte, noe som i de fleste tilfelle ikke kan anses å være ”uforenlig”.

4.5 Krav til sikker identifisering

Bevis skal benyttes for å bevise en eller flere personers overtredelser av straffebestemmelser mv. Det sier seg derfor selv at spørsmålet om sikker identifisering er helt avgjørende for hvilke vekt digitale bevis kan ha i den totale bevisbedømmelsen. Personopplysningsloven § 12 regulerer spørsmålet om bruk av ”entydige identifikasjonsmidler”. Bestemmelsen bruker fødselsnummer som eksempel på entydige identifikasjonsmiddel. Mer praktisk i bevissammenheng er imidlertid biometriske identifikasjonsmåter som fingeravtrykk, irisgjenkjenning og lignende. Bestemmelsen legger både begrensninger på slik identifisering og åpner opp for at Datatilsynet kan gi pålegg om entydig identifisering. Bestemmelsen er knapp og forholdsvis lite informativ, og er ikke detaljregulert i personopplysningsforskriften. Det er likevel mulig å formulere noen enkle retningslinjer på grunnlag av bestemmelsen.

Bestemmelsen krever at entydig identifisering kun skal skje dersom det er "saklig behov". Dersom forveksling av identitet kan få alvorlige følger, kan det sies å foreligge et slikt saklig behov. Ved direkte innsamling av digitale bevis, det vil si når formålet med behandlingen av personopplysninger (blant annet) er bevisinnsamling, må kravet til saklig behov alltid sies å være tilfredsstilt. I en slik situasjon har en altså en rett til å bruke entydige identifikasjonsmidler. Fordi det må anses å foreligge en generell aktsomhetsplikt, kan det imidlertid også argumenteres for at det i slike tilfelle også foreligger en plikt til slik identifisering, selv om dette ikke går frem av lovteksten.[25] Dersom formålet med behandlingen klart krever entydig identifisering, vil det med andre ord kunne anses uaktsomt å unnlate å benytte slike identifikasjonsmidler. I slike tilfelle har Datatilsynet en særskilt hjemmel for å gi pålegg om identifiseringsmåten, se § 12 annet ledd.

I tillegg til at det må foreligge saklig behov for bruk av entydig identifikasjonsmidler, må identifiseringsmåten være nødvendig. Dersom en med andre ord kan kombinere to eller flere identifikasjonsteknikker og oppnå like sikkert resultat, kan ikke entydige identifikasjonsmidler benyttes.

Når formålet med behandling av personopplysninger er innsamling av digitale bevis, er det etter dette en oppfordring og lovlig anledning til å sørge for sikker identifisering av aktuelle personer. "Entydige identifikasjonsmidler" som for eksempel biometriske metoder kan benyttes dersom dette er eneste måten å sikre en så lite tvilsom identifisering som mulig. Det må imidlertid legges til at valg av slike metoder vil kunne innebære en intensivert og strengere prøving av det rettslige grunnlaget for behandlingen, jf avsnitt 4.3.

4.6 Krav til informasjonssikkerhet og opplysningskvalitet

For å sikre at lovens bestemmelser etterleves av den behandlingsansvarliges medarbeidere i virksomheten, pålegger personopplysningsloven den behandlingsansvarlige å etablere rutiner for informasjonssikkerhet (personopplysningsloven § 13 og personopplysningsforskriften kapittel 2) og internkontroll (personopplysningsloven § 14 og personopplysningsforskriften kapittel 3).

Sikkerhetsbestemmelsen i § 13 innebærer krav om at den behandlingsansvarlige og eventuelle databehandlere skal iverksette nødvendige planlagte og systematiske tiltak for å oppnå tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet. Tiltakene kan være av organisatorisk og teknisk eller annen art. Informasjonssystemer og sikkerhetstiltak skal dokumenteres, og dokumentasjonen skal være tilgjengelig både for medarbeiderne i behandlingsansvarliges og (eventuelt) databehandlers virksomhet, og for Datatilsynet og Personvernnemnda.[26]

Personopplysningsforskriftens kapittel 2 inneholder detaljerte krav til informasjonssikkerhet for behandling som skjer helt eller delvis elektronisk. Hvilke tiltak som må iverksettes avhenger av en konkret vurdering av hva som er et nødvendig for å oppnå tilfredsstillende sikkerhet, og knytter i forarbeidene opp til standardene BS 7799 "A code of practice for information security management" og NS-5814 "Krav til risikoanalyser". Bestemmelsene

---

[25] Lovens § 12 annet ledd rubriserer identifiseringsspørsmålet som et spørsmål om "kvalitet". Øvrige kvalitetsaspekter er regulert i § 11 bokstavene d og e, der kvalitetskravene defineres i relasjon til formålet. Det er derfor nærliggende at også spørsmålet om kravet til identifisering ses i forhold til formålet.

[26] Personvernnemnda behandler klager på vedtak i Datatilsynet, se personopplysningsloven § 43.

forutsetter at den behandlingsansvarlige er bevisst i forhold til farer og trusler ved virksomhetens informasjonssystemer og konsekvenser av for eksempel brudd på sikkerhetssystemer. I henhold til personopplysningsforskriften § 2-3 er det ”den som har den daglige ledelsen av virksomheten” som har ansvaret for at bestemmelsene følges.

Lovens § 14 pålegger den behandlingsansvarlige å etablere systematiske rutiner for internkontroll. Bestemmelsen innebærer at arbeidet med opplysningskvalitet skal være del av internkontrollrutiner og -tiltak. Dette innebærer at kravet til opplysningskvalitet vil stå i forhold til formålet med behandlingen og alvorlighetsgraden av de mulige krenkelsene av personvern som bristende kvalitet kan medføre. Personopplysningsloven § 11 bokstavene d og e oppstiller krav til at opplysningene er tilstrekkelige, relevante, korrekte, oppdaterte og ikke unødvendig lagret. Disse kvalitetskravene skal vurderes i forhold til *formålet med behandlingen*. Behandling av personopplysninger som har som formål å bli behandlet som digitale bevis, vil typisk innebære mulighet for alvorlige krenkelser noe som vil innebære strenge krav til tilstrekkelighet, korrekthet mv.

Opplysninger som inneholder feil eller ufullstendigheter skal rettes, suppleres eller slettes i tråd med bestemmelsen i § 27. Av samme bestemmelse går det frem at opplysninger som det ikke er adgang til å behandle, for eksempel fordi det mangler rettslig grunnlag (jf avsnitt 4.3), skal slettes. Siden kravene til opplysningskvalitet må antas å være strenge for digitale bevis, vil det også bli stilt strenge krav til rutinene for retting og sletting mv. Dersom formålet med behandlingen ikke lenger tilsier lagring, skal de som hovedregel slettes, jf § 28. Dette innebærer trolig at kopi av bevis som er overlevert politiet normalt ikke kan beholdes hos den behandlingsansvarlige.

Det er grunn til å understreke betydningen av informasjonssikkerhet og opplysningskvalitet for vurderingen av digitale bevis. Fordi formålet med behandlingen er knyttet til mulige alvorlige konsekvenser for personer (som for eksempel straff), må det forventes å bli stilt strenge krav dersom de digitale bevisene skal bli tillagt vekt i bevisbedømmelsen. Særlig er det grunn til å anta at spørsmålet om korrekthet og oppdatering vil være viktigst blant de kravene som stilles i § 11, og at det vil være en klar fordel å stille presise og strenge krav på disse områdene. Loven opererer imidlertid kun med meget enkle krav som er knyttet til ”personopplysning”, og utdypende regler om kvalitet finnes ikke i forskriften. Det kan derfor være behov for å anvende en mer avansert tilnærming, for eksempel slik at en vurderer kvaliteten på data (forholdet til det dataene er ment å representere/beskrive), informasjonen (forholdet til bruksformålet) og spørsmålet om system- eller behandlingskvalitet (jf de utførende delene av data-/informasjonssystemet og forholdet mellom disse). Vi kommer ikke nærmere inn på disse spørsmålene her, men viser generelt til fremstillingen i Schartum og Bygrave ”Personvern i informasjonssamfunnet”, Fagbokforlaget 2004, s 54 - 59 med videre henvisninger.

Når det spesielt gjelder spørsmålet om dataintegritet, er dette klassifisert som et informasjonssikkerhetsspørsmål, som er nærmere regulert i personopplysningsforskriften. Her er det særlig grunn til å forholde seg samvittighetsfullt til § 2-8 om autorisasjon av personell, § 2-10 om fysisk sikring, § 2-13 sikring av integritet, samt § 2-14 som blant annet stiller krav til logging av forsøk på uautorisert bruk. For at digitale bevis skal ha størst mulig grad av autoritet, er det dessuten særlig viktig å etterleve kravene til sikkerhetsledelse, -organisering, -revisjon, avvikshåndtering og de mange kravene i forskriften til dokumentasjon, herunder kravet til registrering av autorisert bruk i § 2-9.

4.7 Melde- og konsesjonsplikt

Personopplysningsloven § 31 etablerer en plikt for den behandlingsansvarlige til å gi melding til Datatilsynet om alle behandlinger av personopplysninger som skjer med elektroniske hjelpemidler eller om opprettelse av manuelt personregister, og som inneholder *sensitive opplysninger*.[27] Meldeplikten gjelder for hvert opplegg for behandling av personopplysninger,[28] noe som i realiteten innebærer at det er nye informasjons-/datasystem som er gjenstand for meldeplikt. Meldingen skal inngis senest 30 dager før behandlingen tar til. Meldingen skal gi Datatilsynet grunnlag for å kontrollere om lovens vilkår for å behandle personopplysninger er oppfylt. Det er gjort mange viktige unntak fra den vide meldeplikten etter loven. Blant annet er aktivitetslogger unntatt fra meldeplikt forutsatt at disse kun benyttes til å administrere systemet eller til å avdekke/oppklare brudd på sikkerheten i systemet. Dersom opplysninger i logger benyttes til å overvåke eller på annen måte kontrollere enkeltpersoner, gjelder unntaket likevel ikke, se forskriften § 7-11.

Etter personopplysningsloven § 33 kreves det som hovedregel konsesjon fra Datatilsynet for å behandle *sensitive* personopplysninger. Generelt er det således grunn til å anta at de fleste opplegg for å samle inn mv opplysninger som skal være fungere som bevis, vil kreve konsesjon (forhåndstillatelse) fra Datatilsynet. Dette gjelder i alle fall når opplysningstypene er må anses å være sensitive, jf definisjonen i pol § 2 nr 8. På samme måte må en trolig bedømme tilfelle der formålet med informasjonsbehandlingen er å innhente opplysnings*verdier* som indikerer ulovlige forhold. I tvilstilfelle må spørsmålet uansett avgjøres i lys av de personverntrusler som kan sies å være knyttet til behandlingen av opplysningene. Alvorlige trusler vil da trekke i retning av å etablere konsesjonsplikt. Den behandlingsansvarlige har selv ansvaret for å avgjøre om det foreligger konsesjonsplikt og for inngivelse av konsesjonssøknad. Dersom det er tvil om det foreligger konsesjonsplikt, kan den behandlingsansvarlige dessuten kreve at Datatilsynet på forhånd avgjør om en behandling vil kreve konsesjon eller ikke, se pol § 33 tredje ledd. Datatilsynet kan uansett gi pålegg om konsesjonsbehandling, jf pol § 46. En som etablerer et system for innsamling av digitale bevis som han anser å være konsesjonsfritt, kan med andre ord senere risikere å bli møtt med et pålegg fra Datatilsynet om konsesjonsbehandling og tilhørende forbud mot eller vilkår for fortsatt behandling mv.

Ved å oppstille konsesjonsplikt gjennomføres en strengere kontroll av hvorvidt den som behandler opplysningene oppfyller de lovbestemte kravene til behandlingen. I tillegg følger det av lovens §§ 34 og 35 at Datatilsynet skal foreta en ulempevurdering hvor hensynet til personvernet veies opp mot de hensyn som tilsier at konsesjon skal gis. Videre skal Datatilsynet vurdere om det skal stilles vilkår i konsesjonen som avhjelper ulempen for den registrerte. Det følger av loven at Datatilsynet kan avslå konsesjonssøknaden, selv om vilkårene i loven isolert sett er oppfylt.

I forskriften til personopplysningsloven er det på visse vilkår gjort unntak fra melde- og konsesjonsplikten for behandling av sensitive personopplysninger, se forskriften kapittel 7 del III og IV. Dette er for eksempel tilfellet med opplysninger i "hvitvaskingsregistre" dersom de kun blir behandlet i tråd med bestemmelsene for slike registre, se forskriftens § 7-22. Behandling av digitale bevis utenfor de pliktene som er etablert i eller i medhold av hvitvaskingsloven, er derimot omfattet av konsesjonsplikten. Slike opplysninger må normalt

---

[27] Se nærmere om hva som regnes som sensitive opplysninger i avsnitt 4.1.

[28] Og ikke hver konkrete bruk av personopplysningene!

anses å være sensitive fordi de i alle fall gjelder mistanke om et straffbart forhold og fordi de ikke kommer inn under forskriftens unntak.

4.8 Informasjon til den registrerte

Begrepet personvern er tradisjonelt blitt brukt som betegnelse på den interesse enkeltindivider har i å føre kontroll med opplysninger som beskriver dem selv. I nyere personvernteori har fokuset i stor grad vært på elektronisk behandling av personopplysninger, og innebærer at man søker å imøtekomme den enkeltes interesse i at personlige opplysninger tilfredsstiller kvalitetskrav og ikke behandles på en utilbørlig måte. Et viktig aspekt av dette er individets rett og mulighet til å ha oversikt og kontroll over behandling av opplysninger om seg selv. For å oppnå dette er den registrerte gitt rett til innsyn i opplysninger om seg selv, samt at den behandlingsansvarlige er pålagt en relativt vid informasjonsplikt overfor den registrerte.

Den registrertes innsynsrett følger av lovens § 18, hvoretter det gis rett til informasjon om behandlinger som utføres av den behandlingsansvarlige. Dette er en innsynsrett som gjelder for enhver, uavhengig av om vedkommende er registrert hos den behandlingsansvarlige (eller en databehandler) eller ikke, såkalt generelt innsyn. I tillegg gir § 18 også rett til individuelt innsyn, det vil si rett til innsyn i konkrete opplysninger som er knyttet til egen person.

Ved siden av den generelle og individuelle innsynsretten, som den registrerte selv kontrollerer, er den behandlingsansvarlige pålagt informasjonsplikt overfor den registrerte. Når det samles inn opplysninger fra den registrerte selv eller fra andre enn den registrerte, må den behandlingsansvarlige etter personopplysningslovens § 19 og § 20 av eget tiltak informere om navn og adresse på den behandlingsansvarlige og dennes eventuelle representant; hvilke opplysninger som samles inn fra andre enn den registrerte; om det er frivillig for den registrerte å gi fra seg opplysningene; formålet med behandlingen; om opplysningene vil bli utlevert og til hvem; og om retten til å kreve innsyn og retting av opplysninger. Informasjonen må gis før behandlingen av opplysningene foretas, så langt det er mulig.

I forhold til behandling av personopplysninger som skal eller kan tenkes å bli benyttet som bevis, er det de særlige *unntakene* fra innsyns- og informasjonsretten som er interessante. Det følger for det første av § 19 at varsling til den registrerte ikke er påkrevd når den registrerte selv allerede kjenner informasjonen som det er pålagt å informere om. Dette unntaket kan for eksempel være aktuelt ved arbeidsgivers innsamling av opplysninger frem til opplysningene eventuelt skal benyttes til et annet formål (indirekte innsamling av bevis).

Det følger av lovens § 20 at den registrerte ikke har krav på varsel dersom innsamlingen eller formidlingen av opplysningene er uttrykkelig fastsatt i lov, varsling er umulig eller uforholdsmessig vanskelig, eller det er på det rene at den registrerte allerede kjenner til informasjonen varselet skal inneholde.

I tillegg følger det av lovens § 23 vide generelle unntak fra retten til informasjon etter § 18, § 22, § 19, § 20 og § 21. Her skal vi bare trekke frem enkelte bestemmelser som må antas å være særlig relevante for spørsmålet om behandling av digitale bevis. Dette gjelder særlig alternativet som gjelder personopplysninger som det er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger, se § 23 bokstav b. Dette alternativet gjelder imidlertid bare aktiviteter som skjer som ledd i

politiets arbeid etter kapittel 18 i straffeprosessloven og andre kontrolletaters virksomhet.[29] Innsyn kan derfor ikke unntas etter dette alternativet dersom det gjelder privates behandling av personopplysninger som skal brukes som bevis.

Innsynsretten gjelder heller ikke dersom opplysningene er omfattet av lovbestemt taushetsplikt for (§ 23, bokstav d). Det er imidlertid grunn til å anta at slike bestemmelser er lite aktuelle som hinder mot å utlevere personopplysninger til vedkommende person.

Retten til informasjon gjelder heller ikke for opplysninger som utelukkende finnes i tekst som er utarbeidet for den interne saksforberedelse og som heller ikke er utlevert til andre, se § 23 bokstav e. Dette unntaket kan også gjelde materiale som kan være bevis. En viktig forutsetning er imidlertid at opplysningene ikke er utlevert til andre, for eksempel til politiet.

Et siste alternativ for unntak som skal nevnes her er § 23 bokstav f og det tilfellet at utlevering ”*vil være i strid med åpenbare og grunnleggende private eller offentlige interesser…*”. Kravene her er meget strenge, og det skal meget til for at dette alternativet kan begrunne nekting av innsyn.

Lovens § 23 tredje ledd etablerer plikt til på eget initiativ å gi en begrunnelse for avslag på begjæringer om innsyn. Avslaget skal være skriftlig og inneholde en presis henvisning til det unntaksalternativet som begrunner avslaget.

4.9 Særlig om utlevering av opplysninger til politiet

Dersom politiet ønsker opplysninger som private sitter med utlevert til seg, vil en slik utlevering i seg selv være en behandling av opplysninger på den private behandlingsansvarliges hånd som må ha hjemmel i lov, jf personopplysningsloven § 8 og eventuelt § 9. Som et utgangspunkt må utleveringen ha et tilstrekkelig rettslig grunnlag i samsvar med personopplysningsloven § 8 eller § 9. Det mest aktuelle grunnlaget er også her at det foreligger lovhjemmel som pålegger eller tillater fremleggelse av bevis.

Det følger av personopplysningsloven § 39 at personopplysninger som er innsamlet ved billedopptak gjort ved fjernsynsovervåking bare kan 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. Bestemmelsen er utformet slik at både den behandlingsansvarlige og politiet kan initiere slik utlevering. Paragraf 39 er med andre ord en lovhjemmel for utlevering til politiet av opptak fra fjernsynsovervåkning, og det er i slike tilfelle ikke nødvendig å lete etter andre hjemler.

Straffeprosesslovens regler om beslag og utleveringspålegg vil generelt kunne være en hjemmel for utlevering av innsamlede digitale bevis til politiet, jf personopplysningsloven § 8 og straffeprosessloven kapittel 16. Det følger av straffeprosessloven § 203 at ”*ting som antas å ha betydning som bevis, kan beslaglegges inntil rettskraftig dom foreligger i saken. Det samme gjelder ting som antas å kunne inndras eller å kunne kreves utlevert av fornærmede*”. Både dokumenter og opplysninger som er lagret elektronisk vil være omfattet av uttrykket ”ting”.[30] Det er påtalemyndigheten og i noen tilfelle forhørsretten som tar stilling til spørsmålet om det kan tas beslag.

---

[29] Se Ot. prp. nr. 92 s 121.

[30] Se Rt 92/904 og Rt 92/928.

4.10 Rettsavgjørelser vedrørende bevis som er innsamlet i strid med personopplysningslovgivningen

Det er i norsk rett ingen alminnelig regel mot å føre ulovlig eller utilbørlig ervervet bevis. Retten kan altså tillate fremleggelse av bevis selv om de er fremskaffet i strid med for eksempel personopplysningsloven. I siste omgang vil avgjørelsen avhenge av den interesseavveiningen retten må gjøre. Domstolene har i slike saker basert avgjørelsen på at hensynet til sakens opplysning og fri bevisbedømmelse må veie tyngre enn personvernet.[31]

Retten har i noen viktige og prinsipielle avgjørelser etter en konkret vurdering nektet fremleggelse av bevis, med henvisning til at slik fremleggelse vil krenke ulovfestet eller lovfestet personvern for den registrerte. Retten har da funnet at krenkelsen i forhold til den registrerte har vært såpass inngripende at personvernhensynene må veie tyngre.[32] Domstolene har imidlertid i en rekke nyere avgjørelser etter en tilsvarende vurdering kommet til at en overvekt av hensyn taler for fremleggelse. Høyesteretten har i en kjennelse fra 2002[33] lagt til grunn at den ulovfestede bevisavskjæringsregel må forstås slik at domstolene kan tillate bevis fremlagt selv om de er fremskaffet på en i utgangspunktet uakseptabel måte, til og med om det har vært handlet i strid med formelle regler.

4.11 Oppsummering av personopplysningslovens betydning for privates adgang til å behandle digitale bevis

I det følgende skal vi kort oppsummere de viktigste punktene i forhold til behandling av personopplysninger som kan være digitale bevis. Forutsetningen for gjennomgangen er at det skjer *behandling av personopplysninger* i regi av en *behandlingsansvarlig* som er *etablert i Norge*. Vi anbefaler at vurderingene skjer i samme rekkefølge som punktene nedenfor.

1 Etabler et system for internkontroll. Internkontroll skal særlig omfatte alle de følgende punktene, og skal dessuten omfatte andre deler av personopplysningsloven som ikke inngår i denne utredningen, men som kommer til anvendelse på behandlingen. Dette gjelder særlig spørsmål vedrørende allmennhetens og registrertes rettigheter mv, se avsnitt 4.8 og lovens kapittel III.

- Internkontroll må ta utgangspunkt i alle relevante lover, forskrifter, enkeltvedtak (herunder konsesjoner) og rettsavgjørelser.
- Internkontroll skal skje systematisk og være planlagt. Kravet til planlegging innebærer blant annet at selve internkontrollsystemet skal være etablert og at internkontroll er gjennomført, før behandlingen igangsettes. Deretter skal internkontroll skje fortløpende.
- Loven krever bare at eventuelle tiltak skal dokumenteres. Siden det er tale om behandling av opplysninger som skal benyttes som bevis, er det imidlertid grunn til å dokumentere også andre deler av internkontrollen, særlig bakenforliggende risikovurderinger.

---

[31] Se blant annet Borgarting lagmannsretts kjennelse 12. desember 2003.

[32] Se blant annet Rt 91/616. I de fleste av sakene hvor retten har nektet fremleggelse av bevis, har det vært snakk om skjult videoovervåkning av de ansatte, hvor retten har nektet fremleggelse av videoen.

[33] Se Rt 02/1500.

2 Klarlegg hvem som har behandlingsansvaret for de digitale bevisene. Den behandlingsansvarlige har de fleste pliktene etter loven.

- I den grad politiet er behandlingsansvarlig og opplysningene kommer inn under straffeprosessloven eller andre rettspleielover, gjelder ikke personopplysningslovens bestemmelser.

3 Klarlegg og beskriv formålet/formålene med behandlingen av personopplysningene, og beskriv herunder alle deler av formålet som gjelder behandling av bevis, spesielt hvorledes slike bevis kan tenkes anvendt av den behandlingsansvarlige, politimyndigheter, private etterforskere eller andre.

- Opplysninger kan ikke utleveres til politiet som bevis dersom utleveringen ikke dekkes av formålet, med mindre slik utlevering har lovhjemmel. For eksempel kan utlevering til politiet skje selv om denne utleveringen ikke er beskrevet som et formål med å behandle personopplysningene, forutsatt at kravene i personopplysningsloven § 39 er oppfylt. Dersom det rettslige grunnlaget kun er samtykke eller "nødvendighet", må formålet alltid beskrive utlevering til politiet.

4 Klarlegg hva som er det rettslige grunnlaget for behandlingen av personopplysninger, herunder behandling av digitale bevis (jf lovhjemmel, samtykke og "nødvendighet"). Grunnlaget må omfatte innsamling, utlevering og alle andre typer operasjoner som kan utføres på personopplysninger. For eksempel må det rettslige grunnlaget dekke utlevering til politiet.

- Lovhjemmel er en type rettslig grunnlag. Straffeprosessloven § 203 og personopplysningsloven § 39 er sentrale eksempler på lovhjemler for slik utlevering av digitale bevis til politiet.

- Samtykke fra den registrerte kan også være aktuelt som rettslig grunnlag selv om det formålet med behandlingen er innsamling av bevis. I slike tilfelle kan det imidlertid være et problem å tilfredsstille kravene til *frivillig* samtykke. Dersom det er knyttet sanksjoner til nektelse av samtykke, vil det ikke foreligge et gyldig samtykke.

- I mangel av annet rettslig grunnlag er det mulig å ha tilstrekkelig grunnlag for behandling av digitale bevis hos private dersom dette er nødvendig for å ivareta en berettiget interesse som overstiger interessen i personvern. Det er neppe anledning til å anvende "nødvendig grunn" som rettslig grunnlag uten å ha saklige grunner for ikke å innhente samtykke. Slikt rettslig grunnlag vil i tillegg ofte være usikkert og fundert på vide og vage vurderinger.

5 Klargjør eventuelle usikkerheter knyttet til identifiseringen av personer som opplysningene kan gjelde. Begrunn at identifiseringen er tilstrekkelig sikker, og treff eventuelle tiltak for å sikre et tilstrekkelig nivå. Kravene til identifisering må antas å stige dersom det er sannsynlig at opplysningene vil bli brukt på en måte som alvorlig kan krenke personvernet eller på annen måte ha inngripende virkninger for de aktuelle personene. Bruk av opplysninger som bevis vil normalt innebære høye krav.

6 Klargjør hvilken opplysningskvalitet som forventes. Analyser risiko for utilstrekkelig kvalitet, og fastsett eventuelt proaktive tiltak for å sikre kvaliteten.

- Kvalitetskravene må vurderes i relasjon til formålet med behandlingen av personopplysninger. Dette innebærer generelt strenge kvalitetskrav når formålet med behandlingen er innsamling av bevis.

- Tiltakene for å sikre tilstrekkelig kvalitet må særlig omfatte lovens krav til retting og sletting av opplysninger mv, se § 27.

7 Gjennomfør nødvendig sikring av opplysningenes konfidensialitet, tilgjengelighet og integritet. Anvend de samme kravene til arbeidsmåte som skissert for internkontrollarbeidet, jf punkt 1. Legg også merke til detaljerte krav til sikkerhetsarbeidet i personopplysningsforskriftens kapittel 2.

8 Påse at det eksisterer rutiner for ivaretagelse av rett til innsyn og plikt til å gi informasjon ved innsamling av personopplysninger, jf avsnitt 5.8 og lovens kapittel III.

9 Vurder om det foreligger konsesjonsplikt, eventuelt meldeplikt, og gjennomfør tilhørende rutiner, jf avsnitt 5.7 (ovenfor) og lovens kapittel VI.

10 Når konsesjon er gitt (eventuelt melding er sendt) og eventuelle vilkår i konsesjonsvedtaket er implementert, kan behandlingen av personopplysninger igangsettes.

5. BEHANDLING AV PERSONOPPLYSNINGER ETTER STRAFFEPROSESSLOVEN

5.1 Innledning

For å sikre ivaretakelse av rettigheter som frihet, sikkerhet og rettferd er det nødvendig å etterforske og forfølge kriminelle handlinger på en adekvat og hensiktsmessig måte. Det er viktig å sikre at politi og myndigheter har mulighet til å etterforske kriminalitet som involverer bruk av elektroniske kommunikasjonssystemer, samtidig som man i tilstrekkelig grad ivaretar hensynet til personvernet.

Elektronisk kommunikasjon medfører økte muligheter for kommunikasjon og informasjonsflyt som benyttes av alle – både vanlige lovlydige borgere og av kriminelle. Kriminelles bruk av elektronisk kommunikasjon kan sammenfattes i begrepet IKT-kriminalitet. Med IKT-kriminalitet menes kriminalitetsformer der bruk av eller skade på IKT er et fremtredende element. Begrepet dekker typiske kriminalitetsformer som datainnbrudd og skadeverk via telekommunikasjonsnettet.[34] Data knyttet til slik elektronisk kommunikasjon er særlig viktig og verdifullt som verktøy for å hindre, etterforske, oppdage og forfølge kriminelle handlinger.

Straffeprosesslovens saksbehandlingsregler omfatter blant annet regler for innsamling av opplysninger for å gjennomføre etterforskning, jf straffeprosessloven § 224, § 225 og § 226. Det gis også hjemmel for opprettelse av enkelte registre for politi- og påtalemyndigheten, som STRASAK og PÅSAK.[35] Loven gir altså hjemmel for integritetskrenkende handlinger som i utgangspunktet er forbudt, som for eksempel ransakelse, beslag og kommunikasjonskontroll.

5.2 Forholdet til personopplysningsloven

Personopplysningsloven gjelder ikke for saker som behandles eller avgjøres i medhold av rettspleielovene (domstolloven, straffeprosessloven, tvistemålsloven og tvangsfullbyrdelsesloven mv), se personopplysningsforskriften § 1-3. Behandling av personopplysninger som gjøres i medhold av disse lovene, reguleres direkte i den enkelte lov, som går foran personopplysningsloven.

Dette unntaket gjelder imidlertid bare behandling av opplysninger som skjer *i medhold av* rettspleielovene. Dersom opplysningene er samlet inn på annet grunnlag, for eksempel av en privat arbeidsgiver i medhold av personopplysningsloven, og opplysningene senere skal benyttes i en rettsprosess (arbeidsrettssak eller lignende), vil selve innsamlingen falle inn under personopplysningsloven. Fremleggelsen av bevisene som sådan for retten reguleres av den lovfestede og ulovfestede prosessretten.

---

[34] Førsteadvokat Inger Marie Sunde, ØKOKRIM, IKT-kriminalitet: Etterforskningsmetoder og personvern.

[35] Straffeprosessloven § 62 og påtaleinstruksen § 2-1.

5.3 Krav til rettslig grunnlag

5.3.1 Når kan personopplysninger behandles?

Straffeprosessloven § 224 gir det rettslige grunnlaget for når etterforskning kan iverksettes. Et sentralt element i så å si all etterforskning vil være innsamling og sikring av opplysninger, herunder personopplysninger, som kan tjene som bevis. Digitale bevis er et viktig element i all etterforskning.

Straffeprosessloven § 224 lyder som følger:

> *"Etterforsking foretas når det som følge av anmeldelse eller andre omstendigheter er rimelig grunn til å undersøke om det foreligger straffbart forhold som forfølges av det offentlige.*
>
> *Etterforskningsplikten etter første ledd gjelder også der en mulig lovbryter ikke kan straffes fordi vedkommende var mellom 12 og 15 år på handlingstidspunktet. Riksadvokaten kan gi retningslinjer om den nærmere gjennomføringen og om begrensninger i plikten.*
>
> *Har et barn som ikke er fylt 12 år, forøvet en ellers straffbar handling, kan det foretas så vel rettslig som utenrettslig etterforskning.*
>
> *Ved brann og andre ulykker kan det foretas etterforsking om årsaken selv om det ikke er grunn til mistanke om straffbart forhold."*

Etterforskning er et rettslig begrep som må avgrenses mot annen virksomhet som blir utført av politiet. Politiet vil for eksempel også arbeide for å forebygge straffbare handlinger, ordenstjeneste og forvaltningsgjøremål, for eksempel utstedelse av pass.

Avgrensningen av etterforskningsbegrepet har særlig betydning for hvem som har ansvaret for behandlingene som foretas. Det kan her trekkes en parallell til det personvernrettslige behandlingsansvaret. Det vil være riksadvokaten,[36] som har det overordnede ansvaret for påtalemyndigheten, som er ansvarlig for etterforskningshandlinger, mens Justisdepartementet vil være ansvarlig for blant annet forvaltningsgjøremål utført av politiet. Riksadvokaten gir direktiver (i form av rundskriv) om hvordan etterforskningen skal gjennomføres. Riksadvokaten vil gjennom disse rundskrivene blant annet legge føringer på hvilke hjelpemidler som skal benyttes i etterforskningen, jf personopplysningsloven § 2, nr 4. Det personvernrettslige behandlingsansvaret for behandling av personopplysninger som skjer i etterforskningsøyemed vil dermed i utgangspunktet påligge riksadvokaten. Avhengig av hvem som har påtalemyndighet for forholdet som etterforskes, det vil si hvor alvorlig forholdet som etterforskes er, vil man imidlertid kunne ha et delt behandlingsansvar mellom riksadvokaten og statsadvokaten.

Avgrensningen av etterforskningsbegrepet vil også ha betydning for hvilke regler som kommer til anvendelse på virksomheten som utføres. Straffeprosessloven og påtaleinstruksen

---

[36] I norsk rett er Kongen i statsråd øverste påtalemyndighet, og avgjør om tiltale skal reises for straffbare handlinger av embetsmenn i tjenesten og andre tjenestemenn tilsatt av Kongen. Under ham sorterer riksadvokaten, som har den overordnede ledelsen av påtalemyndigheten. Riksadvokaten avgjør om tiltale skal reises i visse grove forbrytelser. Under riksadvokaten kommer den assisterende riksadvokaten. Deretter kommer statsadvokatene, som avgjør tiltalespørsmålet i saker om forbrytelser hvor ikke Kongen i statsråd eller riksadvokaten har påtalerett.

regulerer innsamling av opplysninger i etterforskningsskritt, mens blant annet forvaltningsloven og politiloven vil gjelde for annen virksomhet politiet utfører. I praksis er det vanligvis ikke vanskelig å foreta denne avgrensningen. Det avgjørende er hva formålet med virksomheten som utføres er. Formålet med etterforskning vil være å avklare om det har funnet sted et straffbart forhold og å innhente de opplysninger som er nødvendig for sakens påtalemessige avgjørelse og eventuelle behandling i rettsapparatet. Kravet til formålsangivelse vil bli nærmere behandlet nedenfor i punkt 4.

Etter straffeprosessloven § 224 kan etterforskning foretas enten som følge av en anmeldelse eller dersom det foreligger andre omstendigheter som gjør at det er rimelig grunn til å foreta nærmere undersøkelser. Det er ikke noe vilkår for å sette i gang etterforskning at det er noen bestemt mistenkt eller siktet i saken. Opplysninger som samles inn og behandles av politiet vil imidlertid som regel enten direkte eller indirekte relatere seg til en eller flere enkeltpersoner, uten at disse har strafferettslig status som mistenkt eller siktet i etterforskningen. Slike opplysninger vil være personopplysninger i personopplysningslovens forstand, og enkeltindividene som opplysningene kan knyttes til vil være å betrakte som den eller de "registrerte". Utover hjemmel til å samle inn opplysningene, gir loven imidlertid få regler for hvordan disse innsamlede opplysningene skal behandles videre av politiet, for eksempel tilsvarende kravene om internkontroll og informasjonssikkerhet, jf personopplysningsloven § 13 og § 14. Påtaleinstruksen § 2-2 gir regler om oppbevaring av dokumenter i straffesaker, men gir i hovedsak kun anvisning på hos hvilken instans dokumentene skal oppbevares, og ikke hvordan opplysningene skal behandles. Reglene om taushetsplikt vil også oppstille et vern av slike opplysninger, men det hadde etter vår mening vært en fordel om også straffeprosessloven og påtaleinstruksen inneholdt mer eksplisitte regler om behandlingen av personopplysninger samlet inn av politiet i forbindelse med etterforskning. Dette vil særlig gjelde den såkalte overskuddsinformasjonen.

I praksis vil etterforskning ofte bli iverksatt på grunnlag av en anmeldelse. Der det ikke foreligger noen anmeldelse, vil det ofte være tvil om det foreligger slike andre omstendigheter som gjør at det foreligger rimelig grunn til å iverksette etterforskning. Som nevnt kreves det ikke at mistanken er rettet mot en bestemt person. Om en etterforskning bør iverksettes eller fortsettes vil likevel bl.a. kunne avhenge av om undersøkelsene retter seg mot en eller flere konkrete personer eller ikke. Avgjørelsen vil bero på et konkret skjønn, hvor viktige momenter vil være sannsynligheten for at det foreligger et straffbart forhold, sakens alvor og hvilken etterforskningsinnsats som vil være aktuelle.[37]

Straffeprosessloven § 224 er en regel som verner om enkeltpersoners integritet. Etterforskning skal ikke foretas med mindre det foreligger en anmeldelse eller rimelig grunn til mistanke. Dette er minimumskrav som må være oppfylt før etterforskning skal iverksettes, noe som også innebærer et krav om at personopplysninger ikke kan behandles før vilkårene i bestemmelsen er oppfylt. Når bevis som er innhentet av private overleveres av politiet, må de derfor alene eller sammen med andre bevis være tilstrekkelig klart knyttet til en eller flere personer, ha et slikt innhold og være av en slik kvalitet at disse minimumskravene er oppfylt. Selv om kravene er oppfylt, kan imidlertid kapasitetshensyn og politiets prioriteringer innebære at forholdet likevel ikke blir etterforsket.

[37] Bjerke/Keiserud, Straffeprosessloven Kommentarutgave, Bind II, 3. utg. 2001, s 808 flg.

5.3.2 Hvem bestemmer når personopplysninger kan behandles?

Straffeprosessloven § 225 gir regler om iverksetting og utførelse av etterforskningsarbeidet, nærmere bestemt hvem som iverksetter og utfører etterforskningen.

Straffeprosessloven § 225 lyder som følger:

> *"Etterforsking iverksettes og utføres av politiet. Uten beslutning av overordnet kan enhver politimann foreta skritt som ikke uten skade kan utsettes.*
>
> *Riksadvokaten og vedkommende statsadvokat kan gi pålegg om å iverksette etterforsking og om hvordan den skal gjennomføres, samt om stansing, jf § 75.*
>
> *Etterforsking av straffbare handlinger forøvd om bord i norsk skip, kan også foretas av norske utenrikstjenestemenn etter nærmere regler som Kongen gir."*

Det følger av 1. ledd at politiet foretar etterforskningen av straffbare handlinger. Med "politiet" menes i denne sammenheng påtalemyndighetens[38] tjenestemenn i politiet, i motsetning til enhver politimann. Ansvarlig for behandlingen vil altså være påtalemyndigheten, jf gjennomgangen av ledelsen av påtalemyndigheten ovenfor.

Det følger imidlertid av 1. ledd, annet punkt at enhver politimann har adgang til å foreta skritt som ikke uten skade kan utsettes. Slike etterforskningsskritt kan foretas uten at det foreligger beslutning fra overordnet.

Etterforskning blir normalt gjennomført av polititjenestemenn (etterforskere) som ikke hører til påtalemyndigheten. Men det er altså påtalemyndighetens tjenestemenn i politiet som har ansvaret for at etterforskningen, herunder behandling av personopplysninger, skjer innenfor de rammer som er trukket opp i lov eller instrukser. De er også ansvarlige for at formålet med etterforskningen, jf lovens § 226, blir oppfylt.

I forhold til kravene til selve lovhjemmelen for integritetskrenkende handlinger som i utgangspunktet er forbudt, som har blitt konkretisert gjennom rettspraksis fra både EMD og norske domstoler, er det relevant å reise spørsmålet om behandlingsansvaret for etterforskning burde gått klarere frem av loven.

5.4 Krav til lovgrunnlaget – formålsangivelse

Straffeprosessloven § 226 fastslår hva som er formålet med etterforskningen. Det overordnede formålet er å skaffe til veie de nødvendige opplysninger for avgjørelsen av påtalespørsmålet og å tjene som forberedelse til sakens behandling i retten.

Straffeprosessloven § 226 lyder som følger:

> *"Formålet med etterforskningen er å skaffe til veie de nødvendige opplysninger for*
>
> *a) å avgjøre spørsmålet om tiltale,*
>
> *b) å tjene som forberedelse for rettens behandling av spørsmålet om straffeskyld og eventuelt spørsmålet om fastsettelse av reaksjon,*

[38] Den offentlige myndighet som har kompetanse til å etterforske og påtale straffbare handlinger, utføre offentlige straffesaker ved domstolene og å anvende rettsmidler mot disse avgjørelser. For ledelse av påtalemyndigheten, se fotnote 32.

c) å fullbyrde straff og andre reaksjoner og

d) å tjene som forberedelse for barneverntjenestens behandling av spørsmålet om det skal sette i verk tiltak etter lov 17. juli 1992 nr. 100 om barneverntjenester.

Om personundersøkelse og mentalobservasjon gjelder reglene i kap 13.

Er en bestemt person mistenkt, skal etterforskingen søke å klarlegge både det som taler mot ham og det som taler til fordel for ham.

Etterforskingen skal gjennomføres så raskt som mulig og slik at ingen unødig utsettes for mistanke eller ulempe."

På samme måte som formålsangivelsen fastsatt av private og offentlige aktører som behandler personopplysninger, vil også formålsangivelsen i straffeprosessloven § 226 sette de rettslige skrankene for hvilke etterforskningsskritt, herunder behandling av personopplysninger, som kan foretas. Parallellen til kravet om formålsangivelse som følger av personopplysningsloven § 11 er klar.

Etter straffeprosessloven § 226 er det flere formål med etterforskningen. For det første skal man gjennom etterforskningen skaffe til veie opplysninger og bevis til avgjørelsen av påtalespørsmålet. For det andre skal etterforskningen gi grunnlag for sakens eventuelle behandling ved retten, og for det tredje å fremskaffe opplysninger av betydning for spørsmålet om reaksjon. Formålet vil også være fullbyrding av straff og andre reaksjoner.

Som ledd i etterforskning vil det måtte innhentes opplysninger om en eventuelt mistenkts personlige forhold. Ved avhør skal det settes opp en såkalt personaliarapport, jf påtaleinstruksen § 8-12. Innhenting av mer omfattende opplysninger skal skje i form av en personundersøkelse. Det oppstilles imidlertid få bestemmelser som regulerer behandlingen og oppbevaringen av opplysninger knyttet til andre enn den som har fått status som mistenkte i saken. Under etterforskning er det så å si alltid nødvendig å innhente opplysninger om en eller flere andre personer som har direkte eller indirekte tilknytning til forholdet. Politiet må for eksempel avhøre vitner, sjekke alibi og så videre. Påtaleinstruksen § 2-2 regulerer oppbevaring av dokumenter i straffesaker. Slike "dokumenter i straffesaker" vil kunne inneholde opplysninger om andre enn den som eventuelt har fått status som mistenkt i saken. Bestemmelsen oppstiller imidlertid ikke særlig detaljerte krav til selve behandlingen av opplysningene, tilsvarende personopplysningsloven § 13 og § 14 og særlig bestemmelsene i forskriften knyttet til disse, noe som svekker bestemmelsen i påtaleinstruksen fra et personvernmessig ståsted. For opplysninger som er undergitt taushetsplikt, oppstiller påtaleinstruksen § 3-4 i første ledd en varslingsplikt. Vedkommende myndighet skal sørge for at taushetsplikten blir kjent for dem det gjelder, og kan kreve skriftlig erklæring om at de kjenner og vil respektere reglene. I annet ledd gis det anvisning på hvordan opplysningene skal behandles. Dokumenter og annet materiale som inneholder opplysninger undergitt taushetsplikt, skal oppbevares på betryggende måte. Også dette er svakt sammenlignet med personopplysningsloven § 13 og § 14 med tilhørende forskrifter.

Et viktig rettssikkerhetsprinsipp, og også på mange måter et personvernrettslig prinsipp, er prinsippet om at påtalemyndigheten skal innta en objektiv og upartisk stilling under etterforskningen, jf § 226, 3. ledd. Det er viktig at dette prinsippet etterleves i praksis, og at for eksempel mistenktes anmodninger om konkrete etterforskningsskritt blir undergitt en

seriøs vurdering. Dette prinsippet underbygges av lovens § 241 som gir mistenkte adgang til å begjære rettergangsskritt til avkreftelse av mistanken.[39]

5.5 Politiets innsamling og bruk av digitale bevis ved særskilte etterforskningsmetoder

5.5.1 Innledning

Nedenfor vil vi redegjøre for politiets hjemler til å anvende enkelte særskilte etterforskningsmetoder som innebærer behandling av personopplysninger.

5.5.2 Fjernsynsovervåkning

Forbud mot hemmelig fjernsynsovervåkning og billedopptak på offentlig sted fantes tidligere i straffeloven § 390b, men ved vedtakelsen av personopplysningsloven ble denne bestemmelsen opphevet og erstattet av personopplysningsloven § 40. Etter denne bestemmelsen skal det *"ved fjernsynsovervåkning på offentlig sted eller sted hvor en begrenset krets av personer ferdes jevnlig, skiltes eller på annen måte gjøres tydelig oppmerksom på at stedet blir overvåket og hvem som er behandlingsansvarlig*".

Det følger av personopplysningsloven § 39 at *"personopplysninger som er innsamlet ved billedopptak gjort ved fjernsynsovervåkning, bare kan 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. Selv kan politiet i utgangspunktet benytte hemmelig fjernsynsovervåkning i etterforskning. Årsaken er at behandling av personopplysninger som skjer i medhold av rettspleielovene (herunder straffeprosessloven) er unntatt fra personopplysningsloven, se personopplysningsforskriften § 1-3.

Etter straffeprosessloven § 202a, kan politiet foreta skjult fjernsynsovervåkning på offentlig sted når det foreligger skjellig grunn til mistanke om en eller flere handlinger som etter loven kan medføre høyere straff enn fengsel i 6 måneder, forutsatt at det er av vesentlig betydning for etterforskningen. Beslutning om fjernsynsovervåkning må tas av retten. Bestemmelsen gir ikke hjemmel for slik overvåkning av private rom.

5.5.3 Telefonavlytting

Det er en grunnleggende holdning i norsk rett at det knytter seg alvorlige prinsipielle betenkeligheter mot at myndighetene skal kunne foreta telefonavlytting. Skrekkvisjonen er utviklingen mot et totalitært overvåkningssamfunn, der myndighetene har full oversikt og kontroll over individene.

---

[39] Johs. Andenæs, Norsk Straffeprosess, Bind II, 3. utg. 2000, side 817 flg. Et nærliggende spørsmål i relasjon til § 226 er om formålsangivelsen er så presis at den gir en tilfredsstillende skranke for politiets behandling av personopplysninger i etterforskningsøyemed, og om den foreliggende formålsangivelsen sikrer tilfredsstillende forutberegnelighet for allmennheten, jf EMDs avgjørelser i tilknytning til EMK art 8, 2. ledd. Spørsmålet har så vidt vi vet ikke vært oppe for norske domstoler eller EMD.

Dette har blant annet kommet til uttrykk i straffeloven § 145a, som i utgangspunktet forbyr telefonavlytting. Straffeloven § 145a setter straff for den som foretar hemmelig avlytting eller opptak av samtale som han ikke selv deltar i.[40] Dersom et slikt opptak av samtale mellom to eller flere identifiserbare personer skjer ved hjelp av elektroniske hjelpemidler, vil det være behandling av personopplysninger i personopplysningslovens forstand. Private som gjør opptak for å samle inn bevis, vil komme inn under personopplysningslovens alminnelige bestemmelser. Forbudet i § 145a innebærer at ingen av nødvendighetsgrunnene i personopplysningsloven § 8 kan komme til anvendelse og det må derfor foreligge et eksplisitt samtykke fra den registrerte eller lovhjemmel for at opptaket skal være lovlig.

Straffeprosessloven gjør det lovlig for politiet å foreta visse typer avlytting som ledd i etterforskning. Politiet er gitt slik hjemmel i straffeprosessloven kapittel 16, 16a og 16b, men det er på alle punkter knyttet klare vilkår for at slik avlytting kan skje. Telefon- og kommunikasjonsavlytting er sterkt integritetskrenkende etterforskningsmetoder, og lovgiver har understreket at *"den enkeltes rett til privatliv og til å kunne meddele seg til andre uten innsyn fra utenforstående er en fundamental menneskerettighet."*[41] I visse tilfeller har lovgiver imidlertid funnet at hensynet til den personlige integritet (personvernet) må vike av hensyn til mer tungtveiende interesser og åpnet for muligheten for avlytting.[42]

Straffeprosessloven sondrer mellom kommunikasjonsavlytting og annen kommunikasjonskontroll. Lovens § 216a regulerer kommunikasjonsavlytting, og lyder som følger:

> *"Retten kan ved kjennelse gi politiet tillatelse til å foreta kommunikasjonsavlytting når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling*
>
> *a) som etter loven kan medføre straff av fengsel i 10 år eller mer, eller*
>
> *b) som rammes av straffeloven kapittel 8 eller 9, av § 162 eller § 317, jf § 162 eller av lov om kontroll med eksport av strategiske varer, tjenester og teknologi m v § 5.*
>
> *[…]*
>
> *Kommunikasjonsavlytting kan bestå i å avlytte samtaler eller annen kommunikasjon til og fra bestemte telefoner, datamaskiner eller andre anlegg for elektronisk kommunikasjon som den mistenkte besitter eller kan antas å ville bruke.*
>
> *Tillatelsen kan gis uten hensyn til hvem som eier eller tilbyr det nett eller den tjeneste som brukes ved samtalen eller kommunikasjonen. Politiet kan pålegge eier eller tilbyder av nett eller tjeneste å yte den bistand som er nødvendig ved gjennomføringen av avlyttingen."*

---

[40] Hemmelig opptak av samtale som man selv deltar i er ikke straffbart. Det følger av straffeprosessloven § 216l at politiet kan føre som bevis opptak av en telefonsamtale som politiet hadde hatt med en mistenkt. Dette gjelder imidlertid ikke dersom den mistenkte (den registrerte) i samtale med politiet blir forledet til å snakke om eventuelle straffbare forhold. Hvis vedkommende blir forledet av politiet, vil dette stride mot vedkommendes rett til å forholde seg taus, og beviset må avvises. Bestemmelsen gjelder imidlertid bare avlytting eller opptak som skjer med politiets medvirkning. Opptak som er gjort uten politiets mellomkomst reguleres ikke, og det forutsettes i forarbeidene til loven at slike opptak uten særlig lovhjemmel kan brukes som bevis i straffesak.

[41] Ot.prp. nr 64 for 1998-99 side 46.

[42] Johs. Andenæs, Norsk Straffeprosess, Bind II, 3. utg. 2000, side 200.

Kommunikasjonsavlytting kan etter straffeprosessloven § 216a, 1. ledd altså finne sted når noen med skjellig grunn mistenkes for handling eller forsøk på handling som kan medføre straff av fengsel i 10 år eller mer. Videre kan avlytting finne sted, uavhengig av strafferammen, ved mistanke om spionasje eller ved narkotikaforbrytelser. Mistanken må gjelde fullbyrdet eller forsøkt overtredelse. Så lenge det bare er tale om straffrie forberedelseshandlinger kan avlytting ikke besluttes.[43] Det som kan avlyttes er telefoner, datamaskiner, anlegg for telekommunikasjon eller datakommunikasjon som den mistenkte besitter eller kan antas å ville benytte, se straffeprosessloven § 216a, 3. ledd. Avlytting må være av vesentlig betydning for å oppklare saken.

Annen kommunikasjonskontroll reguleres av § 216b. Bestemmelsen lyder som følger:

> *"Retten kan ved kjennelse gi politiet tillatelse til å foreta annen kontroll av kommunikasjonsanlegg når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling*
>
> *a) som etter loven kan medføre straff av fengsel i 5 år eller mer, eller*
>
> *b) som rammes av straffeloven kapittel 8 eller 9, eller av §§ 145 annet ledd, 162, 162 c, 204 første ledd bokstav d, 317, jf. §§ 162 eller 390 a.*
>
> *Reglene i § 216 a første ledd annet punktum og annet ledd gjelder tilsvarende.*
>
> *Kontrollen kan gå ut på*
>
> *a) å innstille eller avbryte overføring av samtaler eller annen kommunikasjon til eller fra bestemte telefoner, datamaskiner eller andre kommunikasjonsanlegg som den mistenkte besitter eller kan antas å ville bruke,*
>
> *b) å stenge anlegg som nevnt i bokstav a, for kommunikasjon, eller*
>
> *c) at eier eller tilbyder av nett eller tjeneste som benyttes ved kommunikasjonen, skal gi politiet opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom skal settes eller har vært satt i forbindelse med anlegg som nevnt i bokstav a, og andre data knyttet til kommunikasjon.[…]"*

Her kreves det ikke mistanke om så grove forbrytelser som ved kommunikasjonsavlytting. Kommunikasjonskontroll kan for eksempel innebære stenging av et anlegg for kommunikasjon, eller pålegge eieren av et kommunikasjonsnett å gi politiet opplysninger om bruken av telefoner i et bestemt tidsrom og lignende.

Avgjørelse om kommunikasjonsavlytting og -kontroll skal som utgangspunkt treffes av tingretten ved kjennelse. Tillatelsen gis for bestemt tid, ikke for mer enn 4 uker av gangen. I særskilte tilfeller, hvor det er fare ved opphold, kan beslutning om kommunikasjonsavlytting og -kontroll tas ved ordre fra påtalemyndigheten. Avlytting og kontroll kan da ikke foretas for lenger enn 24 timer, og beslutningen må snarest mulig forelegges for retten for godkjenning.

Avgjørelsen treffes uten at den mistenkte gis anledning til å uttale seg, se § 216e, 2. ledd. Uten denne bestemmelsen ville formålet med kontrollen og avlyttingen forspilles. Det følger imidlertid av § 100a at når retten behandler sak om telefonavlytting eller annen kommunikasjonskontroll, skal det straks oppnevnes en offentlig forsvarer for den mistenkte (den registrerte).

---

[43] Johs. Andenæs, Norsk Straffeprosess, Bind II, 3. utg. 2000, side 202.

I to avgjørelser fra 1991 la Høyesterett til grunn at både påtalemyndigheten og tiltalte hadde adgang til å legge frem lydopptak og utskrifter fra avlytting.[44] En slik bevisføring medførte imidlertid også innsynsrett for tiltalte med krav om å få opplyst om avlytting var foretatt, og eventuelt få fremlagt lydbånd og utskrifter av samtalene. Påtalemyndigheten hevdet at dette kunne blottstille politiets kilder og arbeidsmetoder, og være uheldig under etterforskningen. Dette førte til at det ble tatt inn en regel i loven om at opptak eller notater gjort i forbindelse med telefonkontroll ikke kunne brukes som bevis under hovedforhandlingen, og at den tiltalte ikke hadde rett til dokumentinnsyn i dokumenter eller opplysninger fra slik kontroll.[45] Ved lovrevisjonen i 1999 kom man imidlertid til en annen konklusjon på dette spørsmålet, og man fant at det ikke var tilstrekkelig grunn til å gjøre unntak fra de generelle regler om bevisføring og innsynsrett. En viss begrensning i innsynsretten fremgår imidlertid av § 242, 1. ledd, hvoretter innsyn kan nektes hvis det kan skade etterforskningen av andre saker.

5.6 Overskuddsinformasjon

Bruken av såkalt overskuddsinformasjon har også vært oppe til drøfting. Med overskuddsinformasjon tenker man på opplysninger om andre typer lovbrudd som kommer frem ved telefonavlytting. Politiets bruk av overskuddsinformasjon reguleres i lovens § 216i 1, ledd, 3. punktum, punkt b, hvor det heter at taushetsplikten ikke er til hinder for at opplysningene brukes som bevis for et straffbart forhold som kan begrunne den form for kommunikasjonskontroll som opplysningene stammer fra. Overskuddsinformasjonen kan ikke benyttes som bevis for andre lovbrudd. Informasjonen kan imidlertid brukes i etterforskningen av alle slags straffbare forhold, jf punkt a i samme bestemmelse. Fra denne regelen kan man trekke klare paralleller til det personvernrettslige kravet til formålsangivelse og begrensninger på annen og senere bruk av personopplysninger, jf personopplysningsloven § 11, hvor det er lovfestet at innsamlede personopplysninger ikke senere kan benyttes til andre formål som ikke er forenlige med det opprinnelige behandlingsformålet. Hvis det opprinnelige formålet med kommunikasjonskontrollen var å etterforske og bevise for en domstol at en person har spionert, kan ikke overskuddsinformasjon fra denne kommunikasjonskontrollen senere benyttes som bevis for et forhold som ikke omfattes av § 216a. Opplysningene kan imidlertid benyttes i etterforskning av andre straffbare forhold.

5.7 Utlevering av personopplysninger fra teletilbydere

Saker om Internett-kriminalitet åpnes normalt på bakgrunn av en anmeldelse, for eksempel etter tips fra en interesseorganisasjon vedrørende spredning av barneporno. Utgangspunktet er da at det foreligger mistanke om en straffbar handling. Teletilbydere vil i slike tilfeller ofte sitte på avgjørende informasjon for politiets etterforskningsarbeid.

Utlevering av personopplysninger til politiet fra tilbydere av teletjenester, reguleres av ekomloven[46]. Hensynet til å oppklare forbrytelser tilsier at politiet bør få slike opplysninger raskt og uten å måtte innhente rettslig utleveringspålegg. Utgangspunktet er imidlertid at opplysningene teletilbyderen sitter på er underlagt taushetsplikt, jf ekomloven § 2-9. Lovens § 2-9 pålegger tilbyder av teletjenester taushet om innholdet av telekommunikasjon og andres

[44] Rt 91/1018 og Rt 91/1142.

[45] Johs. Andenæs, Norsk Straffeprosess, Bind II, 3. utg. 2000, side 205.

[46] Lov om elektronisk kommunikasjon av 4. juli 2003 nr 83.

bruk av telekommunikasjon. Denne taushetsplikten er imidlertid ikke til hinder for at opplysninger gis til politiet eller påtalemyndigheten, jf 3. ledd. Politiet får opplysningene direkte fra tilbyderen, og anmodningen skal etterkommes med mindre særlige forhold gjør det utilrådelig, jf 4. ledd.[47]

5.8 Krav til lovhjemmelen ved politiets bruk av overskuddsinformasjon

Det er bred enighet om at politiets bruk av overskuddsinformasjon og bruk av kommunikasjonskontroll er et inngrep i borgernes sfære, og derfor ikke kan skje uten lovhjemmel. Som det fremgår av gjennomgangen ovenfor, er slik lovhjemmel gitt i straffeprosessloven kapittel 16. Det må imidlertid i tillegg stilles krav til selve lovhjemmelen, den må være klar og sikre forutberegnelighet for allmennheten. Dette følger av en rekke avgjørelser fra EMD, se blant annet Doerga v the Netherlands[48], Khan v the United Kingdom[49] og Kruslin-saken[50]. I Doerga-saken uttalte domstolen følgende: *"The expression "in accordance with the law" requires, firstly, that the impugned measure should have some basis in domestic law; secondly, it refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and that it is compatible with the rule of law […]*." Min understrekning.

Det vil bero på en konkret vurdering av den enkelte sak om bestemmelsene i straffeprosessloven kapittel 16 sikrer slik tilstrekkelig tilgjengelighet og forutberegnelighet for borgerne.

* * *

[47] Bestemmelsen erstatter den gamle teleloven, § 9-3. (Lov om telekommunikasjon 23. juni 1995 nr 39.)

[48] Saksnummer 50210/99.

[49] Saksnummer 35394/97.

[50] Saksnummer 4/1989/164/220.