PERSONOPPLYSNINGSVERN I SIVILE SAKER

- konsekvenser av unntaket i personopplysningsforskriften § 1-3

Universitetet i Oslo
Det juridiske fakultet

Kandidatnummer: 543

Leveringsfrist: 25.november 2011

Til sammen 17 881 ord

24.11.2011

Innholdsfortegnelse

1 INNLEDNING

1.1 Tema og problemstilling

Tema for denne oppgaven er spenningsforholdet mellom to ulike rettsområder, henholdsvis personvernlovgivning og sivilprosesslovgivning, nærmere bestemt forholdet mellom personopplysningsloven og tvisteloven. Disse to regelsettene har ulike formål. Formålet med personopplysningsloven er "å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger […] og bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn", jf. personopplysningsloven § 1. Denne oppgaven løser personopplysningsloven hovedsaklig ved å tildele rettigheter til den det er registrert opplysninger om og plikter til den som behandler personopplysninger. Eksempelvis må enhver behandling av personopplysninger være knyttet til ett eller flere bestemte formål som er kjent for, og samtykket til av den det gjelder. Loven legger grensen for hvor mye informasjon som kan samles inn til det som er nødvendig for å oppnå formålet, og stiller krav til varsling, opplysningskvalitet og informasjonssikkerhet. Rettighetene for registrerte personer omfatter blant annet rett til innsyn i lagret informasjon om seg selv, og i utstrakt grad retten til å kreve retting og sletting av slike opplysninger.

Tvistelovens overordnede formål er å legge til rette for en "rettferdig, forsvarlig, rask, effektiv og tillitskapende" behandling av sivile saker, og "ivareta den enkeltes behov for å få håndhevet sine rettigheter og løst sine tvister og samfunnets behov for å få respektert og avklart rettsreglene", jf. tvisteloven § 1-1. I dette ligger et overordnet mål om at domstolene skal treffe materielt riktig avgjørelse. Under behandlingen av en sivil tvist, vil det naturligvis forekomme behandling av personopplysninger, men i prosessen med å finne frem til en materielt riktig avgjørelse, vil hensynet til sakens opplysning kunne komme i konflikt med hensynet til personvern. Denne interesseavveiningen vil være en tilbakevendende problemstilling som domstolen må ta stilling til, og hensynet til personvern vil av og til måtte vike. Likevel har målsetningen om at sivil tvisteløsning skal være forsvarlig og tillitskapende også en side til personvernet. Det bør kunne

forventes at behandling av personopplysninger i domstolsapparatet også utføres i samsvar med grunnleggende personvernprinsipper. Under dagens rettstilstand gjelder imidlertid ikke personopplysningsloven for "saker som behandles eller avgjøres i medhold av" tvisteloven, jf. personopplysningsloven § 3 tredje ledd, jf. personopplysningsforskriften § 1-3. Konsekvensen av dette er at personopplysningsloven ikke kan bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn på sivilprosessens område. Omfanget av virkeområde for unntaksbestemmelsens drøftes i kapittel 2.4, og konklusjonen vil vise at utgangspunktet for de videre drøftelsene er at personopplysningsloven ikke gjelder for domstolenes virksomhet.

Problemstillingen etter dette, er i hvilken grad tvisteloven ivaretar hensynene som personopplysningsloven bygger på ved behandling av personopplysninger i sivile saker. Tvisteloven er ikke skrevet spesielt med tanke på å regulere personopplysninger, og oppgaven blir derfor å identifisere bestemmelser som likevel har betydning for slik behandling. Det er mulig å tenke seg flere situasjoner hvor det forekommer behandling av personopplysninger i personopplysningsloven forstand før, under og etter en sivil domstolsbehandling. For å skape en god parallell til personopplysningsloven, vil jeg konsentrere meg om en type behandling som faller inn under personopplysningsloven virkeområde, nemlig elektronisk behandling av personopplysninger. Fokuset rettes mot tvistelovens regler om bevis, nærmere bestemt undersøkes det hvilket vern personopplysninger har når de befinner seg i elektronisk lagret materiale som brukes som bevis.

1.2 Problemstillingens aktualitet

I samfunnet vi lever foregår det en konstant teknologisk utvikling. Innen IKT og relaterte områder som e-handel og digitalisering av offentlig sektor har denne utviklingen vært enorm. I de seneste års personverndebatt har *elektroniske spor* vært et mye debattert tema. Særlig i forbindelse med kriminalitetsbekjempelse har slike spor vist seg nyttige, og den mye omdiskuterte innføringen av EUs datalagringsdirektiv har

fostret nye argumenter til fordel for personvernet.[1] Slike spor etterlates ofte uten at vi er klar over det, og de kan lagres og bearbeides på en annen måte enn tidligere. Eksempelvis kan sporene, som legges igjen når man besøker en internettside, brukes av nettbaserte tjenesteleverandører til å lage en brukerprofil. Formålet er som regel å utnytte informasjonen kommersielt for en mer effektiv markedsføring. Et annet eksempel er arbeidsgivers bruk av teknologi på arbeidsplassen. Formålet kan være effektivisering av kommunikasjonsmetoder og kompetansedeling, for eksempel ved tildeling av egen e-post til bruk på arbeidsplass og opprettelse av interne elektroniske kunnskapsbaser. Et annet formål kan være å bekjempe kriminalitet ved kontroll av ansatte etc. Dersom arbeidsgiver ønsker å videoovervåke sine lokaler, oppstiller personopplysningsloven krav til hvordan dette skal gjøres, herunder meldeplikt til Datatilsynet, og varsel av de ansatte. Problemet oppstår når disse innsamlede opplysningene blir brukt til andre formål enn de opprinnelig ble registrert for, eller utlevert til andre for slik bruk. Dersom det nye formålet er å anvende opplysningene som bevis i en sivil rettssak, er spørsmålet hvilke regler som gjelder for slik innhenting.

Innen sivilprosessen medfører utvidelsen av samfunnets informasjonsgrunnlag at elektronisk lagret materiale ofte er gjenstand for bevis. Dette er en naturlig konsekvens av at stadig mer informasjon lagres elektronisk. Problemet med elektroniske bevis, er at de lett kan manipuleres eller slettes. Dette gjør bevisene spesielt utsatte, og skaper et behov for å sikre dem til bruk i en aktuell rettssak, noen ganger allerede før det er tatt ut stevning. Det er særlig ved bevissikring uten varsel til motparten, at situasjonen kan oppleves som inngripende og som en belastning for motparten. I noen tilfeller vil det sikrede materiale kunne inneholde svært sensitive personopplysninger. Det er grunn til å tro at samfunnet vil skape større mengder elektronisk lagret materiale i fremtiden, og at behovet for sikring av slikt materiale vil øke. Dette kan medføre at reglene om bevissikring i tvisteloven kapittel 28 kommer til å bli mer anvendt.

[1] EP/Rdir 2006/24/EF

1.3 Avgrensning av oppgaven

Temaet som skal behandles er forholdet mellom personvernlovgivning og sivilprosesslovgivning. Ved behandling av "personvernlovgivning", begrenses oppgaven i all hovedsak til å behandle de reglene som er gitt i personopplysningsloven, med tilhørende forskrifter og bakenforliggende internasjonale regler. Forutsetningen for drøftelsene er unntaket fra personopplysningsloven i personopplysningsforskriften § 1-3. Det er kun personopplysningsloven som unntas ved denne bestemmelsen. Andre personvernregler som er å finne i lovverket, herunder materielle og prosessuelle, har egne bestemmelser om virkeområdet. Eksempler på slike regler gir åndsverkloven § 45 c (retten til eget bilde), eller forvaltningsloven § 13 (regler om taushetsplikt). Det ligger utenfor denne oppgavens problemstilling å undersøke når andre personvernregler gjelder, eventuelt ikke gjelder, ved saker som behandles under tvisteloven. Disse reglene vil kun bli nevnt der det er hensiktsmessig.

Tvistelovens regler om bevissikring uten varsel i § 28-3 fjerde ledd antas å være i samsvar med EMK Artikkel 6.[2] Avhandlingen avgrenses mot spørsmålet om hvilken virkning EMK, og andre internasjonale menneskerettighetsregler får ved anvendelse av personopplysningsloven og tvisteloven.

1.4 Metode og rettskildebilde

Bevissikring vil bli brukt som et av eksemplene på når personopplysninger behandles under tvisteloven. Det foreligger svært lite tilgjengelig rettspraksis som tar stilling til spørsmålet om bevissikring. En av hovedårsakene er trolig at en sak om bevissikring sjelden kommer lenger enn tingretten. Når tingretten tillater bevissikring, unntar tvisteloven kjennelsen fra offentlighet frem til bevissikring er gjennomført, eller til minst 6 måneder etter at begjæring eventuelt ble avslått jf. § 28-3 fjerde ledd annet punktum. Min erfaring med å søke etter slike kjennelser er at det er meget tilfeldig hvilke saker som rutinemessig blir offentliggjort, hvilke som forblir i domstolenes arkiv, og hvilke som unntas fra innsynsrett. Selv om underrettspraksis normalt har begrenset rettskildemessig verdi, kan det tillegges vekt der det ikke finnes annen

[2] Ot.prp. nr. 33 (2003-2004) side 5, og Reusch note 1350

praksis. I det følgende vil upubliserte kjennelser fra tingretten brukes hyppig som eksempel under drøftelsene av bevissikring.

Høyesterett har behandlet to saker om bevissikring som vil bli brukt som eksempler gjennom hele oppgaven. Derfor finner jeg grunn til å innledningsvis gi en kort presentasjon av sakskompleksene. Rt-2006-626, også kalt "Normarc-saken", gjaldt en sak hvor noen tidligere ansatte i selskapet Normarc, hadde startet konkurrerende virksomhet med innflygningsinstrumenter til flyplasser. Normarc mistenkte at de tidligere ansatte hadde "gjennomført et storstilt datatyveri" ved å kopiere elektronisk lagret materiale som tilhørte Normarc, og anvende dette i sin egen virksomhet Norwegian SM. Etter å ha analysert sitt eget datasystem, fremsto mistanken som sannsynlig, og Normarc fremsatte begjæring om bevissikring etter tvistemålsloven § 271a. Retten tok begjæringen til følge, og bevissikring ble gjennomført ved at namsmannen tok speilkopi av alt datamateriale hos fire navngitte personer. Til sammen er dette antatt å tilsvare ca. 285 millioner A4- sider.[3] Partenes ulike syn på prosessuelle spørsmål og bruk av rettsmidler sammenholdt med sakens kompleksitet har ført til at saken trolig er den eldste som fremdeles går i norsk rettsapparat. Saken er fra 2004 og har fremdeles ikke kommet til hovedforhandling i tingretten. Per dags dato omfatter den hele 9 avgjørelser i lovdata: Rt-2006-626, Rt-2006-146, LB-2009-14942, LB-2010-110691, LB-2007-37182, LB-2005-59502, TOSLO-2005-4190-2, TOSLO-2005-4190-1 og TOSLO-2004-42431. Ved henvisning til "Normarc-saken" i teksten, vil det samtidig henvises til den aktuelle avgjørelsen i fotnoten.

Rt-2010-774, heretter kalt "Altibox-saken", gjaldt en sak der rettighetshavere til spillefilmer på egen hånd hadde drevet privat overvåkning av ulovlige fildelere på internett. Privatetterforskningen resulterte i en avsløring av enkelte IP-adresser som kunne knyttes til den ulovlige virksomheten. Spørsmålet for Høyesterett var om rettighetshaverne til to spillefilmer, "Max Manus" og "Kautokeinooppgjøret", kunne kreve at internettleverandøren utleverte identiteten til abonnenten bak IP-adressen som de mente hadde brutt åndverksloven. Denne informasjonen var i utgangspunktet

[3] LB-2005-59502

taushetsbelagt, jf. ekomloven § 2-9. Bevissikring ble begjært etter reglene i tvisteloven kapittel 28, jf. tvisteloven § 22-3 andre og tredje ledd. Retten tok begjæringen til følge, og tillot bevissikring uten varsel til abonnenten.

1.5 Den videre fremstillingen

Oppgavens hoveddel består av kapittel 2 og 3, hvor kapittel 2 drøfter hvordan § 1-3 skal tolkes, mens kapittel 3 belyser konsekvensene denne tolkningen får for behandling av personopplysninger i sivile saker. Som et naturlig utgangspunkt innleder kapittel 2.1 og 2.2 med en kort innføring i selve begrepet personopplysningsvern og de moderne utfordringene knyttet til IKT-samfunnet. I punkt 2.3 følger en oversikt over bruken av interesseavveininger som et sentralt virkemiddel i personopplysningsloven, herunder de grunnleggende interesser og prinsipper for behandling av personopplysninger. I punkt 2.4 drøftes virkeområdet for unntaket i personopplysningsforskriften § 1-3, mens punkt 2.5 belyser bakgrunnsrettens betydning for tolkningen av § 1-3.

Kapittel 3 inneledes med en oversikt over kapittelet og elektroniske bevis i punkt 3.1-3.2. I punkt 3.3 drøftes det hvordan personopplysninger blir ivaretatt gjennom tvistelovens regler om tilgang til realbevis, deretter presenteres utfordringer knyttet til reglene om bevissikring i punkt 3.4. I punkt 3.6 drøftes spørsmålet om hvilken praksis domstolene følger for avskjæring etter tvisteloven § 22-7 av bevis som er fremskaffet i strid med personopplysningsloven. Et avsluttende kapittel 4 inneholder en kort rettspolitisk vurdering av personopplysningsforskriften § 1-3 basert på drøftelsene i kapittel 2 og 3.

2 SENTRAL LOVGIVNING PÅ SIVILPROSESSENS OG PERSONVERNETS OMRÅDE

2.1 Hva er personopplysningsvern?

Det finnes ingen "personvernlov" i Norge, derimot har vi lov om behandling av personopplysninger (personopplysningsloven) med tilhørende forskrifter.[4] Personopplysningsloven § 1 forklarer begrepet "personvern" ved å vise til "grunnleggende personvernhensyn", eksemplifisert ved hensynet til "personlig integritet", "privatlivets fred" og "tilstrekkelig kvalitet på personopplysninger". Formålsparagrafens henvisning til grunnleggende personvernhensyn kan leses som en henvisning til innarbeidede oppfatninger av personvern, slik dette blir nedfelt i rettspraksis, forvaltningspraksis og i etablert personvernteori.[5]

Det finnes en rekke enkeltbestemmelser om personvern spredt rundt i lovverket, herunder både materielle og prosessuelle bestemmelser. Eksempler fra formell lov bl.a. helseregisterlovens krav til hvordan personopplysninger skal behandles, eller forvaltningslovens regler om taushetsplikt.[6] I tillegg til slike bestemmelser har vi inkorporasjonslover som innebærer at internasjonale reguleringer av personvern gis virkning i norsk rett. Menneskerettsloven er et eksempel på en inkorporasjonslov, og den fører til at privatlivsbestemmelsen i EMK artikkel 8 og SP artikkel 17 ikke bare får virkning i norsk rett, men også forrang dersom bestemmelsene skulle kollidere med annen norsk lov, jf. menneskerettsloven § 3.

[4] Bl.a. personopplysningsforskriften, kommunikasjonskontrollforskriften, Forskrift om kredittavtaler mv.

[5] Schartum (2000) side 546

[6] for en mer utførelig redegjørelse se Høgberg (2010)

I forbindelse med forberedelsen av personopplysningsloven ble begrepet utredet av Skauge-utvalget i 1997.[7] Den forståelsen av personvernets innhold og begrunnelse som ble lagt til grunn i lovutvalget, er langt på vei også lagt til grunn av lovgiver.[8] Fokuset i det følgende vil først og fremst rettes mot begrepet i betydning ”personopplysningsvern”. Dette er et begrep som er tatt i bruk i Norge i nyere tid, og omhandler ”normer for behandling av personopplysninger med sikte på å verne om personlig integritet, herunder autonomi og privatlivets fred”.[9] Personvernkommisjonen beskrev det slik i sin delrapport fra 2008:

> ”**Personvern** dreier seg om ivaretakelse av personlig integritet, mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse. **Personopplysningsvern** dreier seg om regler, retningslinjer og standarder for behandling av personopplysninger, og som har ivaretakelse av personvern som hovedformål. En personopplysning i denne sammenhengen er en opplysning som direkte eller indirekte kan knyttes til en fysisk person”(mine uthevelser).[10]

Som det fremgår, er ”personopplysningsvern” et underbegrep av ”personvern”. Verneobjektet går fra å være *personen selv* til de *opplysninger* som beskriver personen. I det følgende vil fokus rettes mot ”personopplysningsvernet” fordi det er personopplysningene i det elektronisk lagret materiale som er sårbare når slikt materiale blir brukt som bevis. Spørsmålet er i hvor stor grad hensynet til personopplysningsvern er ivaretatt i lovgivningen som regulerer sivile saker.

2.2 IKT – utfordringer i en ny dimensjon

”Integritetskrenkelser påvirkes av den teknologi som til enhver tid er tilgjengelig”.[11] Informasjons- og kommunikasjonsteknologi (IKT), omfatter ”teknologi for innhenting,

---

[7] Utvalg ledet av Arne Skauge som avga innstillingen NOU 1997:19 ”Et bedre personvern”, se overskriften til kapittel 3

[8] Schartum (2011) side 22-23

[9] Schartum (2011) side 18 med henvisning til Berg 1999 og NOU 2009:1 punkt 4.1.5

[10] Personvernkommisjonens delrapport (2008) side 4

[11] Schartum (2011) side 32

overføring, bearbeiding, lagring og presentasjon av informasjon".[12] En kan tenke seg at mennesket omgir seg med ulike sfærer, og at hver og en selv skal bestemme hvem som skal komme innenfor hver sfære. Selv om disse grensene alltid har vært vanskelig å plassere nøyaktig og generelt, har IKT bidratt med å viske ut overgangene. Med facebook, twitter, blogging, dokumentutveksling og bildedeling er overgangen mellom privatliv og verden utenfor i stor grad blitt flytende. Den økende bruken av IKT har på sett og vis tilført det tradisjonelle personvernet en ny dimensjon.

De teknologiske løsningene gjør det mulig å samle inn og bearbeide en enorm mengde personopplysninger. Hver eneste dag omgir vi oss med teknologiske hjelpemidler. Dette resulterer i at vi legger igjen elektroniske spor. Hver og en av disse sporene representerer en opplysning som gir en bit av informasjon om den det gjelder. Informasjonen kan sammenlignes med en del av et puslespill. Jo flere biter man har tilgang til, jo tydeligere kan man se hele bildet. Man trenger ikke alle bitene for å danne seg et detaljert bilde av personen. Isolert utgjør en bit med informasjon sjelden en trussel for den de kan knyttes til, med mulig unntak for sensitive personopplysninger.[13] Det er først når de ulike bitene med informasjon kobles sammen at det oppstår situasjoner som kan true personverninteresser. En slik kobling av informasjon vil nesten alltid innebære behandling av personopplysninger, og dermed reguleres av personopplysningsloven. Personopplysningsloven stiller krav til formålsangivelse ved innsamling av informasjon, og setter grenser for bruk av denne informasjonen til nye formål – som kobling med annen informasjon som oftest vil innebære.

2.3 Interesseavveining

2.3.1 Interesseavveininger

Både tvisteloven og personopplysningsloven bygger på interesseavveininger ved anvendelse av bestemmelsene. I personvernteorien skilles det mellom individuelle interesseavveininger og generelle interesseavveininger. En *individuell avveining* av personverninteresser betegner "de situasjoner der den enkelte person selv tar stilling til

[12] Definisjon i *Store Norske Leksikon* (sitert 2001-11-08)

[13] Personopplysningsloven har strengere regler for behandling av sensitive personopplysninger

hvor stor vekt han eller hun vil tillegge personvernhensyn i forhold til andre private hensyn". *Generelle avveininger* betegner "de allmenne vurderinger som politiske myndigheter, tilsynsmyndigheter, behandlingsansvarlige og andre må gjennomføre av hensyn til personvernmessige, økonomiske og andre konsekvenser av et generelt opplegg for behandling av personopplysninger".[14] Ved nærmere analyse av personopplysningslovens bestemmelser fremgår det at lovgiver har lagt stor vekt på individuelle avveininger ved å la den enkelte få ivareta sitt personvern gjennom egne interesseavveininger og avgivelse av samtykke.

2.3.2 Grunnleggende personvernprinsipper og interesseteori – lovanvenderens verktøykasse

De grunnleggende personvernprinsippene oppsummerer kjernen i europeiske personvernregler, som stammer fra de samme EU-direktiv som den norske personopplysningsloven bygger på. I tillegg fungerer de som retningslinjer for Datatilsynet (og klageorganer) når disse foretar skjønnsmessige avveininger.[15] Stikkordsmessig er de mest sentrale prinsippene omtalt ved rettferdig og rettmessighet, minimalitet/nødvendighet, formålsbestemthet, opplysningskvalitet, proporsjonalitet og medbestemmelse.[16] Prinsippene reflekterer i stor grad gjeldende rett, og kan lett gjenfinnes i personverndirektivet og de ulike nasjonale lovene som gjennomfører direktivet. [17]

I norsk personvernteori er det utarbeidet en "katalog" over ulike interesser som formulerer og spesifiserer hensynet til personvern i bestemte situasjoner. I rettspolitiske diskusjoner er det bedre å ta utgangspunkt i enkelte personverninteresser enn i de grunnleggende personvernprinsippene.[18] Denne "interesseteorien" ble utviklet tidlig på

---

[14] Schartum (2007) side 43

[15] Schartum (2011) side 100 flg. og NOU 2009:1 punkt 4.4.2

[16] Schartum (2011) side 99-105. Prinsippene er utarbeidet av internasjonale arbeidsgrupper og komiteer som for eksempel Europakommisjonen, Artikkelgruppe 29, og OECD.

[17] Schartum (2011) side 100

[18] Schartum (2011) side 101

70-tallet og har siden blitt omformulert, justert og supplert flere ganger.[19] Dette skyldes i stor grad den stadige utviklingen på dette området i samfunnet. Da Skauge-utvalget avga sin innstilling i 1997, sammenfattet de interesseteorien til syv sentrale interesser, herunder fire individuelle og tre kollektive. De individuelle interessene ble beskrevet som ”interessen i diskresjon, innsyn, fullstendighet og privatlivets fred”, mens de kollektive ”angis ved stikkordene en borgervennlig forvaltning, et robust samfunn og et begrenset overvåkningsnivå”.[20] Dersom alle personverninteressene ble innfridd, ville man oppnådd et fullstendig vern av personopplysninger, men man ville samtidig sette andre viktige interesser til side. Enhver personvernmessig vurdering forutsetter derfor at det foretas en interesseavveining der personverninteressene avveies mot andre samfunnsinteresser.[21] Det er viktig å understreke at interesseteorien ikke sier noe om hvilken vekt de ulike interessene skal tillegges i interesseavveiningen, men kun noe om *eksistensen* av og *forholdet mellom* de ulike interessene.[22] Det ville være umulig å gi klare regler om hvordan personverninteresser skal vektes i forhold til hensynet til kommersielle interesser, kriminalitetsbekjempelse, samfunnskontroll, eller effektivitet. I forarbeidene understreker likevel Justisdepartementet at personverninteresser bør ”tillegges betydelig vekt i avveiningen mot kommersielle interesser”.[23]

2.3.3 Personopplysningslovens interesseavveininger

For at behandling av personopplysninger skal være lovlig krever personopplysningsloven at ett av tre alternative grunnlag foreligger: samtykke, lovhjemmel, eller nødvendighet jf. personopplysningsloven § 11, jf. §§ 8 og 9. Nærmere analyse viser at alle de tre grunnlagene inneholder en form for interesseavveining. Hovedforskjellen ligger i *hvem* som skal foreta avveiningen. Samtykke, som lovens hovedregel, baserer seg på en individuell interesseavveining. Lovhjemmel, forutsetter at Stortinget har foretatt en generell interesseavveining.[24]

---

[19] Schartum (2011) side 41-80

[20] NOU 1997:19 punkt 3.4.2

[21] Schartum (2007) punkt 4

[22] Schartum (2011) side 43

[23] Ot.prp.nr.92(1998-1999) merknader til § 8

[24] Johansen (2001) side 99

Nødvendighetskriteriet baserer seg på generelle interesseavveininger, hvorav noen er lagt til den behandlingsansvarlige, mens andre er lagt til Datatilsynet. Eksempelvis må den som ønsker å behandle personopplysninger selv veie hensynet til den registrertes personvern mot hensyn som taler for behandling. Ved usikkerhet om hvordan interesseavveiningen bør slå ut, kan man rådføre seg med Datatilsynet som i slike tilfeller har et særlig veiledningsansvar, jf § 42 tredje ledd nr 6. Avveininger foretatt av den behandlingsansvarlige, kan i ettertid uansett bli overprøvd av Datatilsynet, Personvernnemnda eller domstolen. Dersom behandlingen krever konsesjon er interesseavveiningen lagt direkte til tilsynsmyndigheten, se personopplysningsloven § 33. I alle tilfeller er det innholdet i praksis fra disse institusjonene som er avgjørende for hvilke momenter man kan legge vekt på ved anvendelse av de ulike bestemmelsene.[25]

Et eksempel på en interesseavveining som ikke er tillagt Datatilsynet direkte, er å finne i personopplysningsloven § 8. Bestemmelsen regulerer selve grunnvilkåret for å behandle personopplysninger etter personopplysningsloven. Dersom det verken foreligger samtykke eller lovhjemmel, må det foretas en vurdering av hvorvidt behandling er "nødvendig" for å oppfylle et av de alternative formål opplistet i § 8 første ledd a – f. Når en advokat inngår en oppdragsavtale vil for eksempel advokatens behandling av klientens personopplysninger, i forbindelse med det konkrete oppdraget, kunne hjemles i § 8a.[26] Derimot vil behandling av opplysninger om *motparten og vitner* i forbindelse med det samme oppdraget kunne hjemles i 8f. Ved "nødvendighetsvurderingen" etter bokstav f, skal ulempene behandling medfører for den registrertes personvern veies mot den berettigede interessen den behandlingsansvarlige eller tredjeperson skal ivareta ved å få utlevert opplysningene. Dersom "nødvendighets"-interessen skal få gjennomslagskraft, må det foreligge interesseovervekt i dens favør. I advokateksempelet, vil advokatens taushetsplikt i de fleste tilfeller avgrense de ulemper det medfører for motparten at advokaten behandler personopplysninger, slik at hensynet til å kunne gjennomføre behandlingen blir avgjørende.

[25] Johansen (2001) side 104

[26] Haram (2008)

Advokaters behandling av sensitive personopplysninger ble vurdert av Personvernnemnda i et vedtak av 5. november 2010 (”Antipirat-saken”). Rettskildemessig må vedtaket tillegges begrenset vekt, særlig med tanke på dissensen. De to fraksjonenes ulike vektlegging av interesser er likevel godt egnet til å illustrere vurderingens kompleksitet, og hvordan en interesseavveining kan slå ut i ulike retninger.

Advokatfirmaet Simonsen klaget inn Datatilsynets avslag på forlengelse av firmaets konsesjon til å behandle personopplysninger.[27] Formålet med behandlingen var ”å bistå rettighetshavere til musikk og filmverk i deres arbeid med å stanse ulovlig” fildeling.[28] I sitt arbeid, registrerte Simonsen IP-adressene til de som delte ulovelige filer. Her sto bransjens legitime interesse i å beskytte seg mot krenkelse av immaterielle rettigheter mot fildelernes personvern. Etter personopplysningsloven § 34 må Datatilsynet foreta en vurdering i tre trinn: først må det vurderes om behandling ”kan volde ulemper for den enkelte”, deretter om disse kan avhjelpes gjennom lovens personvernbestemmelser eller ved å sette vilkår til konsesjon etter § 35, og til sist om ulempene etter en samlet vurdering oppveies av de hensyn som taler for behandlingen.

Personvernnemnda delte seg i et flertall og et mindretall (4-3). Flertallet kom frem til at personverninteressen måtte vike fordi personvernulempene ikke var store nok til å begrunne avslag på forlengelse. Det ble ikke bestridt at behandlingen medførte ulemper for de som ble registrert, men påpekt at disse kunne dempes og nøytraliseres ved hjelp av vilkår som stilles til konsesjonen. Det ble vist til at Datatilsynet hadde foretatt en interesseavveining ved første konsesjonsinnvilgelse, og at det ikke forelå forhold som kunne endre utfallet av den tidligere interesseavveiningen med det resultat at forlengelse ble nektet. I forbindelse med spørsmålet om utelevering av identiteten bak en registrert IP-adresse, viste flertallet i nemnda til ”Altibox-saken” hvor Høyesterett bygde sin konklusjon på at en abonnent ikke kan ”ha en berettiget forventning om

[27] PVN-2009-18

[28] PVN-2009-18

beskyttelse av rettstridig bruk".[29] Rettsikkerheten måtte anses tilbørlig ivaretatt ved at et spørsmål om tillatelse til å få utlevert identiteten bak en IP-adresse alltid vil måtte vurderes av enten påtalemyndighet, domstol eller departement.

Mindretallet var av en helt annen oppfatning og mente at en konsesjon ville utfordre grunnleggende personvernprinsipper. Det ble uttalt:

> "Mindretallet kan ikke slutte seg til den perspektivering av saken som til dels er gjort; at det her er tale om alene en konflikt mellom nødvendige tiltak for ivaretakelse av lovbeskyttede økonomiske rettigheter, mot på den annen side kriminelles vern mot legitim rettslig forfølgning. Et slikt fokus er for snevert. En konsesjon vil utfordre grunnleggende personvernprinsipper som til dels har ligget motiverende bak utviklingen av vår lovgivning på dette område i mer enn tretti år. Personvern relaterer seg til mer enn den konkret krenkedes interesse. Det gjelder til sist spørsmålet om hvilket samfunn vi vil ha."[30](mine understrekninger)

Her viser mindretallet til prinsippet om *opplysningskvalitet*, jf. personopplysningsloven § 1 "tilstrekkelig kvalitet på opplysningene", og peker på at muligheten for at *feil* personer blir registrert som ulovlige fildelere er relativt høy. I prinsippet kan en feilregistrering føre til "tvangsmessig bevissikring uten varsel, altså en fysisk intervenering i den registrertes tilværelse, uten forvarsel".[31] En registrering ville også føre til "en systematisk helomvending av innarbeidede bevisprinsipper", idet abonnenten ville måtte sannsynliggjøre at det ikke var vedkommende som sto bak den ulovlige fildelingen. I den avsluttende avveiningen etter personopplysningsloven § 34 annet ledd la mindretallet vekt på at formålet med registreringen ikke ble oppnådd ved den aktuelle behandling. Det ble uttalt at dette var en objektiv vurdering der "konstaterbare eller klart påregnelige fordeler en konsesjon vil gi konsesjonæren (eller som her, hans oppdragsgiver), må vektlegges." Slutningen ble basert på de manglende resultater fra den allerede fireårige konsesjonen. Behandlingen kunne dermed ikke

[29] PVN-2009-18 med henvisning til Rt-2010-774 premiss 52

[30] PVN-2009-18

[31] PVN-2009-18 sml. Rt-2010-744

anses som å gi fordeler som kunne veie opp for de personvernmessige betenkelighetene en forlengelse av konsesjon ville medføre.

2.4 Forholdet mellom personopplysningsloven og tvisteloven

2.4.1 Lovens utgangspunkt og formålet med unntaksbestemmelsen

Personopplysningsloven § 5 regulerer forholdet til andre lover og lyder:

> ”Bestemmelsene i loven gjelder for behandling av personopplysninger om ikke annet følger av en særskilt lov som regulerer behandlingsmåten.”

Regelen er et utslag av at personopplysningsloven er en generell lov som får virkning både i privat og offentlig sektor.[32] Bestemmelsen lovfester en regel som ellers ville følge av lex specialis-prinsippet; ved motstrid mellom regler av samme rang, går spesielle regler foran mer generelle regler. I tillegg åpner loven for å gi forskrifter om unntaksregler for bestemte institusjoner og saksområder jf. § 3 tredje ledd. Slike forskrifter er gitt, og forholdet til tvisteloven er utfyllende regulert i personopplysningsforskriften § 1-3:

> ”Personopplysningsloven gjelder ikke for saker som behandles eller avgjøres i medhold av rettspleielovene (domstolloven, straffeprosessloven, tvisteloven og tvangsfullbyrdelsesloven mv.)”

Personopplysningsforskriften § 1-3 unntar personopplysningsloven fra å gjelde ved behandling av personopplysninger i henhold til rettspleielovene. Rettspleielover er de lovene som regulerer domstolenes, politiets og påtalemyndighetens virksomhet. På sivilprosessens område, nevner forskriften eksempelvis domstolloven og tvisteloven. Forarbeidene til § 1-3 er beskjedne, og inneholder en sparsom begrunnelse for å unnta personopplysningsloven:

---

[32] NOU 1997:19 kommentar til § 44 (§ 44 i forslaget tilsvarer § 5 i loven)

> ”Når det gjelder politiets behandling av personopplysninger, er unntak fra innsyns- og varslingsregler nødvendig for ikke å umuliggjøre politiets etterretnings- og etterforskningsarbeid. Som en naturlig konsekvens av dette gjøres det unntak fra den registrertes rett til å kreve opplysninger rettet og slettet.”(mine understrekninger).[33]

Om forholdet til den sivile rettspleie, sier forarbeidene ingenting. En mulig begrunnelse for å unnta personopplysningsloven fra rettspleien generelt, er hensynet til *domstolenes uavhengighet*. Dette hensynet kommer ikke direkte til uttrykk i forarbeidene, men kan forankres i maktfordelingsprinsippet.[34] Datatilsynet har som oppgave å påse at personvernlovgivningen blir overholdt, jf. personopplysningsloven § 42. Ved å unnta domstolene fra personopplysningslovens virkeområde, unntas de også fra forvaltningens tilsynsordninger. Slik sikres domstolenes uavhengighet fra forvaltningen.[35] Mot dette kan det innvendes at man kunne opprettholdt maktprinsippet ubeskåret ved å kun unnta Datatilsynets tilsynskompetanse. En lignende løsning er foreslått i forbindelse med prøveprosjekt for innføring av elektronisk kommunikasjon i domstolene.[36] Forslaget innebærer å gjøre personopplysningsforskriften kapittel 2 gjeldende for portalløsningen i domstolene, men slik at Datatilsynets påleggskompetanse etter § 2-2 unntas. På samme måte kunne man tenke seg at personopplysningsloven gjaldt i rettspleien som ellers, men at Datatilsynet ikke hadde tilsynskompetanse.

Ved at personopplysningsloven er unntatrt i sin helhet, fremstår tvisteloven som et komplett regelsett for behandling av tvister. Domstolene er en unik institusjon i samfunnet, noe som kan føre til at en generell og altomfattende lov som personopplysningsloven, ikke nødvendigvis passer til å ivareta de hensyn som bør ivaretas for å sikre en forsvarlig rettergang. Ved gjennomføring av en rettslig prosess, vil det alltid være kryssende hensyn som gjør seg gjeldende. Selv om noen hensyn kan

---

[33] Se kongelig resolusjon av 15. desember 2000 nr. 1265, kommentarer til § 1-3

[34] Maktfordelingsprinsippet skal sikre at makten i samfunnet er fordelt mellom en utøvende, en lovgivende og en dømmende makt. Domstolenes uavhengighet er grunnlovsfestet i Grunnloven § 88

[35] Datatilsynet har selv vist til dette hensynet i en høringsuttalelse fra Datatilsynet av 14. september 2011

[36] Høringsbrev fra Justis – og politidepartementet av 30. juni 2011

synes viktigere enn andre, har ingen hensyn krav på fullstendig gjennomslag på bekostning av alle andres interesser.[37] Det overordnede mål i sivilprosessen, er at dommeren skal komme frem til et riktig resultat. [38] Dette omtales som det *materielle sannhetsprinsipp* og innebærer at *hensynet til sakens opplysning* settes høyt. I noen tilfelle kan hensynet til sakens opplysning lede til at hensynet til personopplysningsvern kommer i bakgrunn. Dette i seg selv kan tale for at en lov som hovedsaklig er gitt for å verne én kategori hensyn, ikke bør gis anvendelse på de interesseavveininger som krever en bredere vurdering.

Ved å unnta personopplysningsloven var trolig forutsetningen at sivilprosesslovgivningen selv har mekanismer for å ivareta hensynet til personopplysningsvern. Når man studerer forarbeidene til tvisteloven og personopplysningsloven, inneholder disse ingenting som tyder på at det er gjennomført en grundig vurdering av om dette faktisk er tilfelle etter gjeldende rett. Det er verdt å merke seg at de formålene som løftes frem ved innføringen av personopplysningsforskriften § 1-3, ene og alene er begrunnet i hensyn som gjør seg gjeldende på straffeprosessens område. Det kan stilles spørsmål til hvorvidt hensyn som gjør seg gjeldende for politi- og påtalemyndighet, også kan begrunne unntak fra loven på domstolenes område. Problemstillingen er ikke reist i personopplysningsforskriftens forarbeider, og er heller ikke nevnt i personopplysningslovens forarbeider. Som det vil fremgå av den videre drøftelse, gjør unntaket et kraftig innhugg i lovens anvendelsesområde. Det kunne derfor være naturlig å forvente at omfanget ble klargjort og begrunnet i forarbeidene, uten at dette er gjort.

2.4.2 Saklig virkeområde for personopplysningsforskriften § 1-3

Etter ordlyden er det kun *saker der rettpleielovene får anvendelse* som er unntatt. Det første spørsmålet er hvordan "saker" skal forstås. Det er i hovedsak tre kategorier av saker som behandles av domstolene: *rettssaker, forvaltningssaker* og *administrative*

[37] Torgersen (2006) side 536

[38] Robberstad (2009) side 11, og for eksempel NOU 2001:32A side 131 og 454

saker.[39] Ordlyden nevner de saker som "behandles eller avgjøres i *medhold av rettspleielovene".* En naturlig forståelse av språkbruken tilsier at dette kun er rettssaker. Denne løsningen støttes av uttalelser i forarbeidene til § 1-3, hvor det presiseres at rettspleiens behandling av personopplysninger på *andre områder enn nevnt* i forskriften, ikke er omfattet av unntaket. Som eksempel på slike områder nevnes "blant annet rent forvaltningsmessige saker".[40] Henvisningen viser tydelig at unntaket ikke var ment å omfatte alle saker. Dette innebærer at behandling av personopplysninger i forvaltningssaker, for eksempel tinglysning, skifte- eller konkursbehandling, reguleres av personopplysningsloven. Administrative saker, det vil si interne saker i domstolsapparatet uten direkte betydning for parter eller utenforstående, har det til felles med forvaltningssaker at de hovedsakelig heller ikke behandles etter reglene i rettspleielovene, jf. forvaltningslovens § 4 første ledd bokstav a.[41] Det er vanskelig å se at hensyn skal tale for at administrative saker bør behandles annerledes enn forvaltningssaker. I personopplysningsforskriften § 7-18 er det gjort unntak fra konsesjons- og meldeplikt for den behandlingen av personopplysninger som domstolene utfører i forbindelse med slik virksomhet. Dette unntaket hadde vært meningsløst, dersom personopplysningsloven allerede var unntatt etter § 1-3. Dette innebærer at det er *rettssaker* som omfattes av unntaket i § 1-3.

2.4.3 Begrensninger i det saklig virkeområde innenfor rettspleien

Av juridisk teori fremgår det at unntaket har blitt tolket slik at det kun gjelder for behandling av *den enkelte sak*, og ikke slik at det unntar det generelle opplegget (systemet) for behandling av personopplysninger.[42] Det generelle opplegget eksemplifiseres ved personopplysningslovens krav til rettslig grunnlag i §§ 8 og 9, informasjonssikkerhet i § 13 og internkontroll i § 14.[43] Ut fra ordlyden i § 1-3 kan bruken av ordet "saker*"* leses som en innskrenkning av unntakets virkeområde, og støtte en slik tolkning. Hvis en ville gjøre et generelt unntak fra

[39] Ot.prp.nr.8 (2002-2003) pkt.3.1.1

[40] Se kongelig resolusjon av 15. desember 2000 nr. 1265, merknader til § 1-3

[41] Bernt, note 56

[42] Schartum (2011) side 142

[43] Schartum (2010) punkt 3.2.5

personopplysningsloven, kunne en skrevet at behandling av personopplysninger som skjer i medhold av rettspleielovene unntas. I teorien vises det til at en slik tolkning følger av direkte uttalelser i forarbeidene, men det presiseres ikke hva i forarbeidene som peker i den retning. I en fotnote henvises det til forarbeidene til forskriften, men så langt jeg kan se, tar disse kun utgangpunkt i politiets behandling, og ikke rettspleiens behandling generelt. Det samme må sies å gjelde for forarbeidene til forskrifthjemmelen. Her heter det blant annet.:

> "I påvente av en generell revisjon av strafferegistreringsloven vil det være hensiktsmessig å la den nye personopplysningsloven gjelde for politiregistrene i utgangspunktet, og samtidig åpne for unntak ved forskrift fra deler av loven […] Unntak vil særlig være påkrevet i forhold til reglene om den registrertes rett til innsyn og den behandlingsansvarliges varslingsplikt, men kan også være nødvendig i forhold til regler om konsesjons – eller meldeplikt, regelen om Datatilsynets tilgang til opplysninger osv. På den annen side er det grunn til å anta at f eks lovens generelle krav til saklig og korrekt behandling i § 11 samt kravene til informasjonssikring i § 13 og internkontroll i § 14 bør kunne gjelde også for denne type registre."[44]

Uttalelsen bærer preg av en meningsytring fra Justis – og politidepartementets side, idet de bruker ord som "grunn til å anta" og "bør". Den kan riktignok tolkes dit hen at hensikten *ikke* har vært å unnta loven generelt, men begrunnelsen begrenser seg også her til straffeprosessens område (politiregisteret). Et nytt forskriftsforslag fra samme departement om elektronisk kommunikasjon i domstolene, bidrar til ytterligere forvirring med hensyn til hvorvidt personopplysningsloven er generelt unntatt, som følge av unntaket i personopplysningsforskriften § 1-3. I forslaget foreslår Justis – og politidepartementet at personopplysningsforskriftens regler om informasjonssikring gjøres gjeldende for domstolenes portalløsning.[45] Som eksempel på virksomhet som trenger særlig regulering vises det blant annet til innsending av prosesskriv og elektronisk samhandling mellom de ulike aktørene i en rettssak. Personopplysningsforskriftens kapittel 2 har hjemmel i personopplysningsloven § 13

[44] Ot.prp.nr.92 (1998-1999) punkt 4.6.4

[45] Høringsbrev fra justis- og politidepartementet av 30. juni 2011

fjerde ledd, og er et av eksemplene fra juridisk teori på regler som ikke omfattes av unntaket i § 1-3. Når departementet foreslår å gi disse reglene anvendelse ovenfor domstolenes portalløsning, viser de at de forutsetter at disse reglene ikke kommer til anvendelse etter dagens rettstilstand. Det samme departementet som ved utarbeidelsen av personopplysningsforskriften uttalte at kravene til informasjonssikring i § 13 "bør kunne gjelde for" politiregisteret, gir i dag uttrykk for at slike regler faktisk ikke gjelder for domstolenes portalløsning, som på sett og vis deler flere funksjoner med et register. Sett i sammenheng taler dette for at domstolenes behandling av saker er unntatt i sin helhet.

I sin høringsuttalelse benyttet Datatilsynet muligheten til å kommentere departementets tolkning av § 1-3.[46] Det rettes ikke kritikk mot selve innføringen av forskriftsreglene, men det argumenteres for at disse gjelder fra før fordi § 1-3 ikke unntar dem. Datatilsynet viser for det første til at elektronisk forsendelse av dokumenter ikke naturlig faller inn under ordlyden i § 1-3. Etter min mening er dette en svakt fundert påstand. Som nevnt, omfatter forskriften blant annet elektronisk samhandling mellom de ulike aktørene i en rettssak. Slik samhandling må være en del av *behandlingen* av en sak under rettspleielovene. Videre viser Datatilsynet til at unntaket i § 1-3 er begrunnet i ønsket om en "uavhengig rettspleie", og uttaler at oppstilling av "overordnede systematiske krav om informasjonssikkerhet og internkontroll ved domstolenes *kommunikasjonsvirksomhet*" etter deres vurdering ikke svekker denne uavhengigheten. Til dette må det presiseres at selv om overordnede systematiske krav ikke vil svekke domstolenes uavhengighet, innebærer ikke det at slike krav gjelder. I sin konklusjon avslutter Datatilsynet med en anmodning til departementet om å foreta en ny vurdering av om domstolenes kommunikasjon faller utenfor personopplysningslovens virkeområde på grunn av betydningen en tolkning av personopplysningsforskriften § 1-3 vil få også utenfor rammen av den gjeldende sak. Slik vurdering forelå ikke da denne oppgaven gikk i trykken.

Hvis § 1-3 skal forstås som et generelt unntak, er enkelte av den oppfatning at personopplysningsvernet innen de områder som reguleres av rettspleielovene blir

[46] Høringsuttalelse fra Datatilsynet av 14. september 2011

redusert til en mer begrenset og tilfeldig regulering av personopplysningsvern i disse lovene.[47] Personopplysningsvernet vil avhenge av hver enkelt rettspleielovs egen regulering. Hvis unntaket derimot innskrenkes til den enkelte sak, innebærer det at alle bestemmelser i personopplysningsloven som fastsetter rettigheter for registrerte personer eller plikter for den behandlingsansvarlige overfor slike personer, ikke gjelder. Dette vil omfatte innsynsrettigheter, plikter til å informere, rette, og slette mv.[48] Derimot vil de systemmessige kravene fortsatt gjelde, i den grad ikke andre bestemmelser i rettspleielovene går foran som lex specialis jf. personopplysningsloven § 5. Dette samsvarer godt med ordlyden i § 1-3, og gir en dekkende personopplysningsregulering, samtidig som særlige behov innen rettspleien får gjennomslag.

Etter mitt skjønn fremstår det som tvilsomt hvorvidt det kan oppstilles et skille mellom systemregler og regler tilknyttet den enkelte sak. Departementets tolkning av § 1-3 kan tyde på at et slikt skille ikke praktiseres av domstolene i dag. Som en unik samfunnsinstitusjon krever domstolene regler som er tilpasset deres virksomhet. Eksempelvis er både offentlegloven og forvaltningsloven unntatt fra å gjelde for domstolene. Dersom formålet med § 1-3 kun var å unnta regler som gjelder for behandling av den enkelte sak, kunne dette enkelt vært presisert i forskriften. Selv om løsningen kan diskuteres, er min konklusjon at unntaket i § 1-3 må forstås å gjelde generelt.

2.4.4 Hvilke aktører omfattes av personopplysningsforskriften § 1-3?

Det første som må drøftes, er om unntaksbestemmelsen får ulik anvendelse på den behandling av personopplysninger som utføres av henholdsvis domstoler, advokater eller andre rettshjelpere. Dette vil bero på en tolkning av hvem som kan, og hva det vil si, å *behandle* eller *avgjøre* saker i medhold av rettspleielovene. For domstolene, taler ordlydens henvisning til "rettspleielovene" for at unntaket gjelder for all behandling som utføres i domstolene. Domstolens funksjon er regulert i rettspleielovene, og dens handlingsrom er begrenset til det som reguleres i disse. Det er utvilsomt domstolen som

[47] Schartum, e-post 26. oktober 2011

[48] Schartum (2011) side 142-143 og Schartum (2010) side 15-16

avgjør saker på grunnlag av rettspleielovene, og i stor utstrekning også den som foretar *behandlingen*. På denne bakgrunn bør det kunne konstateres at unntaket omfatter domstolenes saksvirksomhet fullt ut. Unntaket medfører at når elektroniske bevis behandles i domstolene, løftes personopplysningene ut av personopplysningslovens verneområde, og inn under sivilprosessens regler.[49]

Drøftelsene i kapittel 3.4 vil vise at når bevissikring utføres uten varsel til motparten, overlater tingretten ofte den praktiske gjennomføringen til namsfogden. Spørsmålet er derfor om unntaket i personopplysningsforskriften § 1-3 omfatter namsfogdens behandling av personopplysninger. Namsfogdens hovedoppgaver utføres i medhold av tvangsfullbyrdelsesloven, og den har plikt til å bistå tingretten i saker om tvangsfullbyrdelse jf. tvangsfullbyrdelsesloven § 2-2 tredje ledd. Tvangsfullbyrdelsesloven er ved siden av tvisteloven omfattet av de rettspleielover som unntas i henhold til personopplysningsforskriften § 1-3. Namsfogdens bistand i forbindelse med bevissikring er ikke direkte regulert av tvisteloven, men som følge av at loven ikke gir noen nærmere anvisning for gjennomføring, har domstolene i praksis overlatt oppgaven til namsfogden.[50] I likhet med domstolene, vil alt namsfogden foretar seg, skje i medhold av rettspleielovene. Selv om bevissikring ikke reguleres direkte, opptrer namsfogden på instruks fra tingretten, og det er antatt at den har anledning til å bruke tvangsmidler som er gitt i tvangsfullbyrdelsesloven.[51] Konklusjonen må derfor bli at personopplysningsforskriften § 1-3 medfører at namsfogdens behandling av personopplysninger ikke reguleres av personopplysningsloven.

Hva gjelder så for advokaters behandling av personopplysninger? I en beslutning fra Disiplinærutvalget av 15. september 2003 var spørsmålet om en advokats oversendelse av personopplysninger til namsmannen i forbindelse med en inkassosak, utgjorde et brudd på reglene om god advokatskikk.[52] Datatilsynet hadde på forhånd avgjort at handlingen utgjorde et brudd på personopplysningsforskriften, og uttalte at unntaket i

[49] Coll (2004) punkt 5.2

[50] Rt-2006-626, TAHER-2006-184362, og Schei side 1259

[51] Schei (2007) side 1259

[52] ADA-2003-37

personopplysningsforskriften § 1-3 kun gjaldt behandling av personopplysninger i *politiet og i domstolen.* Selv om tvangssalget skjedde i namsretten og med hjemmel i tvangsfullbyrdelsesloven, var altså ikke *advokatens behandling* av personopplysninger unntatt fra personopplysningsloven. Disiplinærutvalget fant ingen grunn til å bestride dette, men fant ikke at advokaten hadde brutt reglene om god advokatskikk. I begrunnelsen ble det lagt vekt på at Datatilsynets tolkning av personopplysningsforskriften § 1-3 fremsto som uklar og det faktum at verken namsmann eller oppdragsgiver syntes å ha innsett at innsendingen kunne komme i konflikt med personopplysningsloven. Beslutningen er vist til i en avgjørelse fra Personvernnemnda, som et eksempel på når unntaket i § 1-3 ikke kommer til anvendelse.[53] Det nevnes ingenting om at tolkningen ikke er riktig. Med andre ord tyder praksis fra Datatilsynet, Advokatforeningens Disiplinærutvalg og Personvernnemnda på at unntaket i § 1-3 ikke omfatter advokaters behandling av personopplysninger. En slik løsning er lovteknisk enkel å forholde seg til, idet den fører til at personopplysningsloven gjelder uten unntak. På en annen side er det vanskelig å basere en tolkning som innskrenker ordlyden, på en noe uklar uttalelse fra Datatilsynet som ikke er bestridt.

Advokaters rettshjelpvirksomhet skjer i henhold til rettspleielovene, herunder domstollovens kapittel 11 ”om rettshjelp og advokatvirksomhet”. Etter den vidt formulerte ordlyden i § 1-3 skulle advokaters virksomhet derfor være unntatt fra personopplysningslovens anvendelsesområde. Ordet ”behandles” er ikke definert, og vil derfor kunne unnta all behandling som reguleres av rettspleielovene, så langt ikke annet er bestemt. Ved tvil om innholdet i en bestemmelse kan overskriften være til hjelp. Overskriften i § 1-3 taler for at unntaket får betydning for andre enn bare domstolene, og lyder ” Behandling av personopplysninger i rettspleien”. Dette kan forstås til å omfatte behandling *i* domstolen, men ikke uten videre begrenses til behandling *av* domstolen. Forskriftshjemmelen gir adgang til å unnta loven helt eller delvis fra å gjelde for ”institusjoner og sakområder*”*, se personopplysningsloven § 3 tredje ledd. I personopplysningsforskriften er dette gjort for en *institusjon* i § 1-1, jf.

[53] PVN-2008-02 SSP

"Riksrevisjonens behandling" og et *saksområde* i § 1-2, jf. "behandling som er nødvendig for rikets sikkerhet". § 1-3 er ikke avgrenset til en institusjon, men kan leses som et unntak for saker som reguleres av prosessregler. Som nevnt unntar ikke § 1-3 domstolenes behandling av personopplysninger i forvaltningssaker. Dette viser at det ikke er gjort unntak for domstolene som institusjon. Dersom hensikten var å unnta domstolene som institusjon, kunne dette enkelt vært presisert. Når dette ikke er gjort, er det mer nærliggende å tolke unntaket til omfatte behandling som utføres av advokater, så lenge behandlingen reguleres av en rettspleielov.

Så vidt meg bekjent, er betydningen § 1-3 får for advokaters behandling av opplysninger ikke eksplisitt drøftet noe sted. Derimot er advokaters forhold til personopplysningsloven grundig behandlet av Haram i en oversikt laget på oppdrag fra Advokatforeningen i 2008.[54] Her er det klare utgangspunkt at advokatvirksomhet er underlagt personopplysningsloven. Fordi betydningen av personopplysningsforskriften § 1-3 ikke er vurdert, fremstår oversikten som mangelfull. Etter en personlig henvendelse der spørsmålet tas opp, svarte Haram at § 1-3 *får* betydning for advokater i forbindelse med en verserende sak for domstolene. Hun understreket likevel at det ikke betyr at advokaten er fritatt fra å følge personopplysningsloven i sitt arbeide med innhenting av opplysninger i forbindelse med arbeid med saker for klienter. Advokater er pålagt å følge personopplysningsloven på lik linje med andre som innhenter opplysninger om andre personer.[55] Det er ikke gitt hvordan dette skal forstås, men det støtter oppfatningen om at § 1-3 leder til at advokater ikke alltid vil være underlagt personopplysningslovens regler. Så langt kan det konkluderes med at § 1-3 får anvendelse på advokaters behandling av personopplysninger.

2.4.5 Når kommer unntaket til anvendelse?

Utfordringen etter dette blir å trekke skjæringspunktet for når personopplysningsloven gjelder for advokater, og når den unntas. At det må oppstilles en grense, er en naturlig

[54] Haram (2008)

[55] Haram, e-post av 25. oktober 2011

konsekvens av at personopplysningsloven gjelder for advokater der personopplysningsforskriften § 1-3 ikke unntar den. Ordlyden i § 1-3 dekker behandling som utføres når saken er kommet inn i domstolsapparatet, men med tanke på at tvisteloven også omfatter saksbehandling i forkant av rettsmøtet, til og med før sak reises, vil også slik behandling kunne omfattes. Grensen bør derfor trekkes på et tidligere stadium i prosessen, slik at eksempelvis utveksling av personopplysninger gjennom prosesskriv, og sikring av bevis før rettssak gjennom reglene i tvisteloven kapittel 28, også unntas fra personopplysningslovens regler. En enkel løsning er å trekke grensen ved tidspunktet for det første *rettslige skritt*. Dette vil normalt markeres ved innsending av stevning, men også utløses av en begjæring om bevissikring før sak er reist. Løsningen medfører at behandling av personopplysninger som skjer før det tas rettslige skritt, *er underlagt personopplysningsloven*. For eksempel vil behandling i forbindelse med en prosessrisikovurdering, ikke unntas fra personopplysningslovens regler. Grensetilfeller oppstår i forbindelse med utførelse av arbeid og plikter *før sak reises*. Noen av disse er fastsatt i tvisteloven kapittel 5. Disse pliktene er regulert i tvisteloven, men de involverer ikke domstolene. Andre følger av forpliktelser ovenfor klienten som regelmessig vil bestå i undersøkelser og innhenting av materiale for å underbygge krav som skal fremmes i stevningen.

Denne forberedende virksomheten må sies å ligge i gråsonen av § 1-3 sitt nedslagsfelt. Det er ikke gitt at behandling av personopplysninger i forbindelse med forberedelse til å ta ut stevning unntas fra personopplysningsloven, men dersom grensen trekkes ved rettslige skritt, vil loven gjelde så lenge stevning eller begjæring ikke er innsendt domstolen. Dette kan bidra til et veldig tilfeldig personopplysningsvern, og gjøre loven vanskelig å etterlever for en stor andel advokater. Størst forvirring utløses i tilknytning til de pliktene personopplysningsloven pålegger den behandlingsansvarlige i tilknytning til den registrerte, herunder plikten til å varsle osv. De *systemmessige krav* som loven stiller til advokatvirksomheten vil, dersom de i utgangspunktet gjelder, tas i bruk selv når loven ikke gjelder. Har man først etablert informasjonssikkerhetsrutiner osv, er det ingen grunn til ikke å ta dem i bruk, selv om man er i en rettssak. Tvert i mot vil en saks sensitive karakter gi større grunn til å opprettholde høy informasjonssikkerhet og internkontroll.

Rettstekniske hensyn, som behovet for en klar og praktisk anvendelig regel, tilsier at grensen bør trekkes på en klar måte, til tross for at løsningen kan medføre en viss inkonsistens. Det er rom for uenighet, men etter mitt skjønn taler de beste hensyn for at *rettslige skritt* markerer grensen for når personopplysningsloven slutter å gjelde. For oppgavens undersøkende formål tjener en slik grense til å belyse problemstillingene på en ryddig måte ved å skape en oversiktlig fremstilling av når personopplysningsloven kommer til anvendelse.

2.5 Gir personopplysningsloven hjemmel for å unnta rettpleien generelt?

Det kan reises grunnleggende spørsmål til om utformingen unntaket i § 1-3 er gitt samsvarer med bakgrunnsretten, herunder internrettslige spørsmål om forvaltningskompetanse, og EØS-rettslig spørsmål om de norske reglene samsvarer med personverndirektivet. Dette vil utgjøre en del av bakgrunnsstoffet i vurderingen av § 1-3, jeg har derfor valgt å skissere hovedspørsmålene som oppstår i dette avsnittet. Formålet er å danne et bilde av usikkerheten rundt nedslagsfeltet til § 1-3 og den utformingen den er gitt.

Som vist gjør § 1-3 et markant unntak fra personopplysningslovens saklige virkeområde. Det kan stilles spørsmål ved om ordlyden i forskriftehjemmelen dekker et så generelt unntak fra loven, se personopplysningsloven § 3 tredje ledd. Personopplysningsforskriften § 1-3 unntar all behandling av personopplysninger i ”saker som behandles eller avgjøres i medhold av rettspleielovene” med blant annet tvisteloven og domstolloven som eksempler. Bruken av ”mv.” viser at eksemplifiseringen ikke er uttømmende, og understreker at unntaket omfatter en *generell og vid kategori* lover. Meg bekjent har rekkevidden aldri vært utfordret, men om unntaket ikke går utover ordlyden, må det sies å ligge i ytterkant av hva som er hjemlet i § 3 tredje ledd som tillater unntak for *bestemte* institusjoner og saksområder.

En annen problemstilling er unntakets forhold til personverndirektivet.

Personopplysningsloven gjennomfører EU's personverndirektiv i norsk rett.[56] I kommentaren til personopplysningsloven presiseres det at der personopplysningsloven tillater lovregulerte unntak fra egne bestemmelser, må slik behandling likevel tilfredsstille personverndirektivets krav til behandling av personopplysninger, idet direktivet gjelder for alle behandlinger av personopplysninger som foregår i de landene som er EU- eller EØS-medlemmer.[57] Det er ingen grunn til at unntak i medhold av personopplysningsforskriften § 1-3 skal behandles annerledes enn unntak i henhold til eksplisitt lovhjemmel. Hvis de behandles likt innebærer det at behandling av personopplysninger i rettspleien må tilfredsstille personverndirektivets krav til behandling av personopplysninger. Dette reiser for det første et spørsmål om i hvilken grad personverndirektivet gir medlemsstatene anledning til å gjøre unntak, og for det andre et spørsmål om Norge har holdt seg innenfor denne grensen, eller om det har oppstått en motstrid som ikke kan la seg bortfortolke. Dersom man kommer til at unntaket i § 1-3 ligger utenfor det som personverndirektivet gir adgang til i lys av EØS-rettens krav til gjennomføring, vil unntaket likevel gjelde som norsk lov. En opprettholdelse av unntaket kan i så fall risikere å bli angrepet av ESA.

Det første spørsmålet beror på en tolkning av personverndirektivet. Direktivets virkeområde er fastsatt i artikkel 3. I artikkel 3 nr. 2 gjøres det unntak fra virksomhet som ikke omfattes av *fellesskapsrettens virkeområde* og bestemmelsene på statens virksomhet på det *strafferettslige område*: "Dette direktiv får ikke anvendelse […] og ikke under noen omstendighet på behandling som gjelder offentlig sikkerhet […] og statens virksomhet på det strafferettslige område", jf. artikkel 3 nr.2 første strekpunkt. Direktivteksten nevner ingenting om unntak fra statenes virksomhet på det *sivilrettslige område*. Det er så vidt meg bekjent bare Norge som har gitt et så generelt unntak som § 1-3 fastsetter. De ulike medlemslandene har utarbeidet forskjellige personopplysningslover ved gjennomføringen av personverndirektivet. Fordi direktivet består av minimumsstandarder, kan medlemslandene fritt fastsette et bedre, men ikke et dårligere vern enn det som er bestemt der.[58] Til sammenligning har Sverige ikke gjort

[56] EP/Rdir 95/46/EF

[57] Johansen (2001) side 99

[58] Schartum (2011) side 114

lignende unntak fra personuppgiftslagen. Danmarks har ved å unnta deler av loven på straffeprosessens område, valgt en løsning som langt på vei tilsvarer direktivets. Persondatalov § 2 stk. 4 lyder som følger:

> "Bestemmelserne i lovens kapitel 8 og 9 og §§ 35-37 og § 39 finder ikke anvendelse på behandlinger, der foretages for *domstolene* inden for det *strafferetlige område* [...] finder heller ikke anvendelse på behandlinger, der foretages for *politi og anklagemyndighed* inden for det *strafferetlige område*."[min kursivering].

Kapittel 8 og 9 gjelder informasjonsplikt ovenfor og innsynsrett for den registrerte, mens de øvrig nevnte paragrafer gjelder den registrerte innsigelsesrett mot behandling. Videre er *hele loven* unntatt for "behandlinger, der udføres for politiets og forsvarets efterretningstjenester", jf. § 2 stk.11. Det gis ingen tilsvarende unntaksbestemmelser for domstolenes eller andres behandling på det sivilrettslige område. Dette gir grunn til å spørre om direktivet gir adgang til å gjøre unntak fra rettspleien generelt. En mulig forklaring på at Norge har valgt en annen løsning enn sine naboland, kan være forskjellen på EU- og EØS-landenes nasjonale prosessautonomi. Sivilprosessen er ikke omfattet av EØS-avtalen, og er dermed ikke EØS-relevant. Derimot inneholder EU-avtalen regler om samarbeid om sivilrettslige spørsmål i tredje del kapittel 3. Dette innebærer at Sverige og Danmark som EU-medlem, ikke står like fritt til å bestemme hvordan sivilprosessen skal utformes. [59] Det burde uansett kunne forventes at lovgiver klargjorde formålet for unntaket da det ble vedtatt, men den spinkle begrunnelsen som er gitt i forarbeidene til § 1-3 omhandler som nevnt kun strafferettslige hensyn, det vises til det som ble sagt under punkt 2.4.1. Av plasshensyn, kan spørsmålet om saksbehandling etter tvisteloven er i samsvar med personverndirektivet ikke drøftes i sin fulle bredde.

[59] se Fredriksen (2008) for en grundig fremstilling av forholdet mellom tvisteloven og EØS-avtalen

3 KONSEKVENSER AV UNNTAKET I § 1-3 I SIVILE SAKER

3.1 Innledning

I dette kapittelet forutsettes det at personopplysningsloven ikke kommer til anvendelse når det er tatt rettslige skritt for en domstol i en sivil sak. Det vises til det som ble sagt i kapittel 2.4. Tema i det følgende er hvilke *konsekvense*r unntaket fra personopplysningsloven får for personopplysninger som behandles i sivile saker. På bakgrunn av at personopplysninger *inngår i bevismaterialet* i en sivil sak, tas det utgangpunkt i tvistelovens regler om bevis. Først presenteres elektroniske bevis i punkt 3.2. Deretter drøftes tre ulike eksempler på regler som medfører behandling av personopplysninger grundig, herunder de alminnelige reglene om plikten til å stille bevis til rådighet i punkt 3.3 og de spesielle reglene om bevissikring i punkt 3.4. Til slutt behandles det særlige bevisforbudet som følger av § 22-7 på bevis som er innhentet i strid med personopplysningsloven i 3.5.

3.2 Elektroniske bevis

Bevis er det som legges frem av partene i en rettssak for å underbygge de fakta som hver part bygger sin sak på. Siden personopplysningsloven gjelder for ”behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler”, rettes fokus mot *elektroniske bevis*. ”Elektroniske bevis” brukes i det følgende som betegnelse på elektronisk lagret materiale som tas i bruk som bevis. Tvisteloven kategoriserer elektronisk lagret materiale som *realbevis* jf. tvisteloven § 26-1:

> ”Realbevis er personer og gjenstander (fast eiendom, løsøre, dokumenter, elektronisk lagret materiale mv.) hvor personen eller gjenstanden, eller dens egenskaper tilstand eller innhold, inneholder informasjon som kan ha betydning for det faktiske avgjørelsesgrunnlaget i saken”.

I juridisk litteratur har elektroniske bevis blitt definert som ”et hvert digitalt materiale

som er samlet for å underbygge en håndgripelig omstendighet som antas å være rettslig relevant".[60] Det er umulig å gi en uttømmende liste over hva som regnes som elektroniske bevis, men typiske eksempler som ofte brukes er elektronisk lagrede dokumenter, e-poster eller lyd- og bildeopptak.

Det oppstår noen særlige problemstillinger i tilknytning til bruk av elektronisk lagret materiale som bevis. En av hovedutfordringene er at slikt materiale er svært enkelt å manipulere, fabrikkere eller slette. Fra et beslutningsperspektiv skal personvernregler sørge for at opplysninger som danner grunnlag for beslutninger behandles forsvarlig og ikke misbrukes.[61] Hvis informasjonssikkerheten er dårlig, øker faren for ukorrekte opplysninger. Manipulasjon trenger ikke å være et resultat av onde hensikter. Ofte redigerer og endrer man på dokumenter og e-poster uten å tenke over det. En e-post som er en del av en lengre tråd, kan tas ut av sin kontekst og gis et nytt meningsinnhold dersom den sendes uten den forutgående korrespondansen. Dersom tidligere e-postkorrespondanse slettes, er beviset borte. System som er sårbare for manipulering øker faren for ukorrekte opplysninger og representerer en trussel for personvernet. Denne svakheten får også betydning for den faktiske muligheten til å gjøre bruk av materialet, og for bevisverdien. Elektronisk lagret materiale bør derfor søkes sikret på et tidlig stadium, slik at man unngår faren for ødeleggelse.

En annen type utfordring oppstår der materialet er så omfattende at det nærmest fremstår som en umulig oppgave å finne frem til det som er relevant. Til illustrasjon er det antatt at det sikrede materialet i "Normarc-saken" tilsvarer ca. 285 millioner A4-sider.[62] Dette materialet omfatter dokumentdata der bevisverdien ikke kun ligger i innholdet, men også i tilknyttede metadata, som kan betegnes som "data over dataene". *Metadata* er data tilknyttet en datafil som kan gi opplysninger om hvem som har opprettet et dokument, når det ble lagret, endret, skrevet ut osv. I tillegg finnes *systemdata*, som er de data som inneholder informasjon om rutinefunksjoner på selve systemet, herunder når en data ble slått av og på, etablering og sletting av programfiler,

[60] Se bl.a. Coll (2004) punkt 1

[61] NOU 1997:19 punkt 3.2.4

[62] LB-2005-59502

tilkobling til andre datamaskiner, skrivere og internett osv.[63] Felles for denne typen data er at den kan gi verdifull informasjon ved validering av om et dokument er ekte. For worddokumentet kan for eksempel metadataene vise at noen andre enn den som opprettet dokumentet, har vært inne og endret det i ettertid.

Litt på siden av problemstillingen ligger utfordringen ved at det ofte trengs teknisk kompetanse og utstyr for å bedømme om beviset er ekte eller manipulert. I en artikkel trykt i "Revisjon og Regnskap" om "bevisverdien av elektronisk informasjon" påpekes det at Advokatforeningen har gitt utrykk for at "begrenset teknisk kompetanse gjør at så vel påtalemyndighet som advokater og dommere forholder seg tilfeldig til elektroniske bevis som legges frem".[64] Selv utrykker forfatterne bekymring for konsekvensene det kan ha for rettssikkerheten at teknologiske utfordringene knyttet til elektroniske bevis, ikke tas på alvor av partene i rettsystemet. Det vises blant annet til at prinsippet om fri bevisføring også medfører "fri misbruk av teknologi", og slikt kan føre til at viktige avgjørelser treffes på feil grunnlag. Etter hvert som elektroniske bevis blir stadig mer aktuelle, vil det også oppstå et behov for å sikre teknisk kompetanse i rettsvesenet.

3.3 Plikten til å stille elektroniske bevis til rådighet

3.3.1 Problemstillingen

Tvisteloven § 21-3 første ledd første punktum knesetter det grunnleggende *prinsippet om fri bevisføring*. Effektiv bevisføring forutsetter regler som sikrer tilgang til bevis som parten ikke har. Partene vil ofte være uenige om plikten til å legge frem bevis, og man har derfor egne regler i kapittel 26 om tilgang til realbevis. Etter tvisteloven § 26-5 første ledd foreligger det en allmenn plikt "til, etter begjæring, å stille til rådighet som bevis dokumenter og andre gjenstander som inneholder informasjon som kan ha betydning for det faktiske avgjørelsesgrunnlaget i saken". Definisjonen gjør det klart at det bare er gjenstander mv. som inneholder informasjon *som har betydning for* saken som utgjør bevis i saken. Det betyr videre at man ikke har plikt til å fremlegge

[63] Monsen (2007) side 199-200

[64] Thorvaldsen (2007)

gjenstander som ikke er relevante for saken. Hvis saksøkte nekter å stille beviset til rådighet frivillig, kan retten pålegge saksøkte å gi saksøker tilgang jf. tvisteloven § 26-7.

Sett i lys av oppgavens tema aktualiserer reglene om bevistilgang spørsmål om hvilke regler som ivaretar partenes og tredjepersons personopplysningsvern. Forutsatt at den informasjonen som "stilles til rådighet" jf. tvisteloven § 26-5 inneholder *personopplysninger*, vil "sammenstilling, lagring og utlevering [av slike] eller en kombinasjon av slike bruksmåter" representere "behandling av personopplysninger" jf. personopplysningsloven § 2 første ledd nr. 2. Når slik behandling skjer elektronisk kommer – isolert sett – personopplysningsloven til anvendelse, jf. ordlyden i personopplysningsloven § 3 første ledd bokstav a, og oppstiller plikter for den behandlingsansvarlige og rettigheter til den registrerte. Fordi bestemmelsen i personopplysningsforskriften § 1-3 unntar personopplysningsloven fra å gjelde, oppstår det spørsmål om hvilke regler tvisteloven har for å sikre en forsvarlig behandling av personopplysninger som finnes i bevismateriale. Jeg finner det hensiktsmessig å behandle rådighetsstillelse av bevis som inneholder personopplysninger som kan knyttes til *egen person* og *tredjeperson* hver for seg.

3.3.2 Personopplysninger om egen person

I tilknytning til spørsmålet om hvordan man kan kontrollere andres bruk av *egne personopplysninger* kan det skilles mellom de tilfeller der tilgang gis frivillig, og de tilfeller der retten pålegger å stille beviset til rådighet. Der tilgang gis frivillig må dette sees som et samtykke til videre behandling av personopplysningene. I slike tilfeller holdes domstolen utenfor, hvilket innebærer at den som sitter med rådighet over bevisene i større grad vil ha mulighet til selv å luke ut/holde tilbake sensitiv informasjon og personopplysninger. På grunn av partenes opplysnings- og sannhetsplikten, jf. § 21-4 jf. § 21-5, begrenses denne muligheten for selektivitet seg til irrelevant informasjon. Dersom materialet kan stilles til rådighet i papirutgave begrenses likevel muligheten for spredning, muligheten for å søke i materialet, og muligheten for å sammenstille det på andre måter.

Dersom den som blir bedt om å stille bevis til rådighet nekter, kan retten avgjøre spørsmålet ved kjennelse, jf. § 26-7 jf. § 19-1 annet ledd bokstav d. I den grad informasjon man ønsker å holde privat ikke kan "skilles" fra resten av materialet, gir tvisteloven anledning til å imøtegå begjæringen med henvisning til reglene om bevisfritak og bevisforbud jf. § 26-7 annet ledd. Dersom materialet har bevisverdi, og ingen av unntakene er påberopt, skal materialet fremlegges, jf. Rt-2011-757. Kjennelsen gjaldt en sak mellom Åsne Seierstad/Cappellen Damm og bokhandleren i Kabul, og spørsmålet for Høyesterett var om Seierstad pliktet å legge frem sine private notater. Retten mente notatene utgjorde bevis i saken, og uttalte at "det følger av tvisteloven § 21-5 siste punktum at plikten til å gi tilgang til bevis bare begrenses av reglene om bevisforbud og bevisfritak. Slike grunner er ikke påberopt."[65] Det er retten som skal avgjøre hvorvidt det omtvistede materialet utgjør bevis i saken. Dersom den påberopte unntaksregel ikke er absolutt, beror utfallet på rettens vektlegging av hensyn. I Rt-2010-1409 opphevet Høyesterett lagmannsrettens kjennelse fordi lagmannsretten ikke hadde foretatt denne vurderingen selv, men pålagt parten å stille det omtvistede elektronisk lagret materiale til rådighet for motpartens egen vurdering av bevisverdien.[66]

I de tilfellene retten pålegger plikt til å stille sensitivt materiale til rådighet, vil dette kunne oppleves som krenkende for den som omfattes. Krenkelsen forsterkes ved allmennhetens innsynsrett i bevismateriale, jf. § 14-2 første ledd bokstav c. Belastningen ved at opplysningene blir kjent kan fjernes ved at retten gjør unntak fra innsynsretten etter reglene i § 14-4 annet eller tredje ledd dersom vilkårene er til stede. Slik vil opplysningene kun brukes til å belyse den aktuelle saken. Dette vil samsvare med *prinsippet om minimalitet* ved behandling av personopplysninger, og medfører at krenkelsen ved å tillate bevisene reduseres til tidsrommet for gjennomføring av den aktuelle tvist. For å sikre en slik begrensning av bruken har retten anledning til å bestemme at beviset skal føres for lukkede dører under pålegg om taushetsplikt for de som er til stede, jf. § 22-12.[67] Denne taushetsplikten gjelder også under

[65] Rt-2011-757 premiss 16

[66] Rt-2010-1409 premiss 16 og 17

[67] Schei (2007) side 1069 og 1132 flg.

saksforberedelsen.[68] Når kjennelsen gjøres offentlig, kan personopplysninger vernes ved å anonymisere avgjørelsen. Hvis ikke en anonymisering er tilstrekkelig til å ivareta hensynet til de involverte kan avgjørelsen i sjeldne tilfeller unntas offentlighet, jf. domstolloven § 130.[69]

3.3.3 Tredjepersons personopplysninger

Et annet spørsmål er hvilken beskyttelse *tredjeperson* har mot at opplysninger om han selv, som en annen sitter på, ikke utleveres til andre. Elektronisk lagret materiale som utleveres til bruk for en rettssak kan inneholde informasjon som kan knyttes til flere personer enn den som besitter beviset. I en erstatningssak mellom den norske stat og et rederi, påla lagmannsretten staten å utlevere en pdf-fil med 800 e-brev mellom statens tjenestemenn og andre som til dels inneholdt sensitiv og irrelevant informasjon.[70] I en trygderettssak for Høyesterett ble fremleggelse av legejournalnotater pålagt på den betingelse at taushetsbelagte opplysninger om tredjeperson, ikke fremgikk.[71] I disse sakene var det parten som fremla beviset som tok tredjepersons personopplysninger i forsvar. Det kan ikke forventes at alle vil forsvare tredjepersons interesse i å kontrollere andres bruk av hans personopplysninger. Enhver som frivillig gir fra seg bevis, eller pålegges å stille bevis til rådighet, kan komme i skade for enten bevisst, eller ubevisst, overlevere informasjon som inneholder personlige opplysninger om andre. Denne informasjonen kan være knyttet til saken og slik tjene sakens opplysning, eller den kan være såkalt "overskuddsinformasjon" som ikke er luket ut. [72]

---

[68] Schei (2007) side 1133 og Rt-2009-125 premiss 25

[69] Kjennelsen fra Oslo tingrett av 8.januar 2007 er unntatt i medhold av domstolloven § 130, se punkt 4.2

[70] Borgarting lagmannsrett kjennelse av 19. august 2010. Høyesterett opphevet kjennelsen i Rt-2010-1409. Se omtale av dommen ovenfor i punkt 3.4.2 andre avsnitt.

[71] Rt-2009-1209 Merk at fremleggelse av pasientjournaler er underlagt egne regler i særlovgivningen, se for eksempel helseregisterloven kapittel 4. Her gjaldt helsepersonelloven § 21

[72] Utrykket overskuddsinformasjon brukes som regel i forbindelse med bruk av materiale som stammer fra kommunikasjonskontroll og romavlytting i tilknytning til kriminaletterforskning, jf. NOU 2009:15 punkt 2.5.2. I denne sammenheng siktes det til informasjon som ikke er relevant for det formål det er samlet inn for. Når overskuddsinformasjon følger med på lasset kan det skyldes en ren forglemmelse, eller at det ville være svært arbeidskrevende eller umulig å skille den informasjonen fra det vesentlige.

Problemstillingen kan illustreres med et eksempel:

Part (A) begjærer tilgang til et bevis (X) som befinner seg i institusjon (B) sin besittelse. X inneholder personopplysninger om en uvitende tredjeperson (Y). Hvis A får tilgang til bevis X vil han kunne føre beviset for domstolen, noe som medfører at opplysningene spres fra B til A, motparten, domstolen og allmennheten så langt innsynsretten etter tvisteloven kapittel 14 rekker. Det forutsettes at den opprinnelige innsamlingen og lagringen av personopplysninger som B har foretatt er gjort i samsvar med personopplysningsloven, hvilket innebærer at "den registrerte" Y er varslet, og har hatt mulighet til å rette og slette opplysninger etter reglene i personopplysningsloven. En utlevering til A er derimot ikke forenelig med innsamlingsformålet, og omfattes ikke av samtykket. Desto mer sensitiv personopplysningene er, desto større grunn er det til å tro at Y ikke ønsker at opplysningene skal spres til uvedkommende.

Dersom B hadde vært underlagt personopplysningsloven, ville utlevering av opplysningen til et nytt formål krevet innhenting av samtykke jf. personopplysningsloven § 11første ledd bokstav c, med unntak for lovregulert plikt til å utgi opplysninger.[73] Det nærmeste tvisteloven kommer til krav om samtykke fra tredjeperson, er kravet om samtykke fra den det gjelder dersom informasjon som er omfattet av forbudsreglene ønskes ført. Dette vil gjelde for en del taushetsbelagte opplysninger jf. tvisteloven §§ 22-3 annet ledd, 22-4 første ledd annet punktum og 22-5 tredje ledd. I de tilfellene samtykke fra tredjeperson gir en mulighet for å oppnå tilgang til beviset, gir det partene insentiv til å innhente slikt samtykke. Men siden det kun gjelder for en begrenset type informasjon, kan ikke samtykke sies å være vektlagt stor betydning.

Videre kan det spørres om part A eller institusjon B har noen plikt til å informere tredjeperson Y. A ville normalt hatt en informasjonsplikt etter personopplysningsloven § 20 for innsamling av opplysninger hos andre enn den registrerte. Tvisteloven pålegger

[73] for eksempel til Skattemyndigheter etter ligningsloven, eller konkurransetilsynet etter konkurranseloven.

verken A eller B noen lignende form for informasjonsplikt. Dersom det er av "betydning for en part å varsle tredjeperson om saken, *kan* parten varsle tredjeperson ved prosesskriv, som forkynnes", jf. tvisteloven § 15-9 første ledd, (min kursivering). Regelen passer etter sin ordlyd, men er ment å brukes i situasjoner der det kan være aktuelt for en tredjeperson å tre inn som part eller partshjelper.[74] Selv ved anvendelse oppstiller bestemmelsen kun en mulighet til å varsle tredjeperson, ikke en plikt.

Dersom retten pålegger bevistilgang, oppstår spørsmålet om *retten* har en plikt til å informere Y om avgjørelsen. Rettens avgjørelse om bevistilgang treffes ved kjennelse jf. § 19-2 annet ledd bokstav d, og skaper en plikt for retten til å forkynne avgjørelsen for *parter og partshjelpere* jf. § 19-5 første ledd. Forutsatt at Y ikke er i en posisjon der han kan bli partshjelper, innebærer dette at ikke retten heller har noen plikt til å underrette tredjeperson.[75] Konsekvensen av dette er at Y risikerer å forbli uvitende.

For å sikres kontroll over sine egne personopplysninger, er det en forutsetning at man informeres dersom opplysningene blir brukt til noe man ikke har samtykket til. I personvernretten følger dette av *prinsippet om medbestemmelsesrett*.[76] Til sammenligning vil et pålegg om å stille bevis til rådighet gi tredjeperson B en prosessuell plikt. B gis derfor ankerett over avgjørelse om bevistilgang jf. tvisteloven § 29-8 annet ledd. Tredjeperson Y har derimot verken prosessuelle plikter eller rettigheter. I kommentaren til tvisteloven § 22-5 gis det et eksempel på at en tredjeperson, som Y, har prosessuelle rettigheter. I tilknytning til *overprøving* av departementets samtykke til føring av bevis som er underlagt taushetsplikt jf. tvisteloven § 22-5 annet ledd, antas det at en tredjeperson som har krav på hemmelighold etter den aktuelle bestemmelse om taushetsplikt, også kan kreve rettslig overprøving.[77] På samme måte kunne en tenkelig løsning være å gi tredjepersoner som med interesse i å hindre at bevismateriale stilles til rådighet, adgang til å anke et pålegg

[74] Ot.prp.nr.51 (2004-2005) merknad til § 15-9

[75] Se også Schei (2007) side 1070

[76] Schartum (2011) side 103

[77] Schei (2007) side 1070 uttalelse i tilknytning til rettens overprøving av departementets samtykke til å tillate bevis uten hinder av lovbestemt taushetsplikt etter tvisteloven § 22-5(2).

om å stille slike bevis til rådighet. For at en slik mulighet skal bli reell, er det en forutsetning at Y varsles.

Dersom tilgang gis, kan det oppstå spørsmål om anonymisering av opplysninger. Et grunnleggende prinsipp for behandling av personopplysninger er prinsippet om *minimalitet*[78]. Konkret innebærer prinsippet et krav om at det ikke må samles inn større mengder informasjon enn det som er nødvendig for å realisere formålet. Dette kan også begrunne tiltak for anonymisering av opplysninger.[79] I eksempelet er spørsmålet om B har en rett eller plikt til å *anonymisere* informasjon som ikke er nødvendig for sakens opplysning, før materialet stilles til As rådighet. I en kjennelse fra Oslo tingrett av 3. september 2009 behandlet retten et krav om erstatning etter uaktsom eller grov uaktsom forsømmelse av Avinors ansatte ("Avinor-saken").[80] Retten påla blant annet Avinor å fremlegge en telefonlogg fra flygelederen. Denne telefonloggen inneholdt også opplysninger om en utenforstående tredjeperson. Retten kan med hjemmel i tvisteloven § 26-7 tredje ledd i nødvendig utstrekning gi "nærmere bestemmelser om måten beviset skal gjøres tilgjengelig på". Av hensyn til tredjeperson påpekte retten at Avinor kunne anonymiseres opplysningene før de ble overgitt:

> Denne personens navn kan sladdes, og hvis det ikke er tilstrekkelig til å sikre vedkommendes anonymitet, kan setningen/avsnittet etter rettens vurdering sladdes i den utstrekning det er nødvendig for å sikre slik anonymitet." [81]

Her tar retten på eget initiativ ansvar for å beskytte personopplysninger om tredjeperson. Det må antas at en part som oppfordres om å anonymiseres vil gjøre det, men bruken av ordet "kan" gir utrykk for at anonymiseringen av hensyn til tredjeperson snarere er et valgfritt alternativ enn en plikt.

---

[78] jf. personverndirektivet artikkel 6 nr.1c, og artikkel 7-8

[79] Schartum (2011) side 102

[80] TOSLO-2009-22961-1

[81] TOSLO-2009-22961-1

I rettpraksis er spørsmålsstillingen som regel om de bevis man har fått tilgang på i anonymisert form, kan kreves fremlagt i originalversjon. Rt-2010-1404 gjaldt krav om fremleggelse av forvaltningsdokumenter, og behandler spørsmålet om sladdede verifikasjonsrapporter fra forvaltningen skulle legges frem i original versjon. Høyesterett opphevet lagmannsrettens avgjørelse om å gi innsyn i dokumentene. Disse var i utgangspunktet sladdet av hensyn til faren for at forvaltningens kilder skulle utsettes for represalier.[82] Hjemmelen for å nekte innsyn var forbudet mot å føre taushetsbelagt informasjon i tvisteloven § 22-3 første ledd. I vurderingen viste Høyesterett til at fare for at forvaltningens kilder ble utsatt for represalier utvilsomt var dekket av tvisteloven § 22-9 tredje ledd, og uttalte: "I den foreliggende saken har behovet for bevisforbud materialisert seg på en annen måte enn de situasjonene § 22-9 tredje ledd umiddelbart dekker. Men bestemmelsen viser at hensyn av samme karakter som gjør seg gjeldende i vår sak, er relevante hensyn etter tvisteloven."[83] Kjennelsen gir et eksempel på at tredjepersons personopplysninger vernes, men oppstiller ingen plikt for B (her representert ved forvaltningen) til å anonymisere. Anonymiseringen fulgte som resultat av regler om taushetsplikt i forvaltningsloven. Personopplysninger som ikke er taushetsbelagt, ville ikke vernes på tilsvarende måte.

3.3.4 Oppsummering

Gjennomgangen viser at tredjepersons personopplysninger er de som er minst ivaretatt av tvisteloven regler. Med tanke på at tvisteloven skal sikre rettigheter for parter og partshjelpere, er det naturlig at tredjepersoner ikke har fått førsteprioritet. Selv om tredjeperson ikke alltid vil være klar over at personopplysninger om han behandles i forbindelse med en sivil sak, betyr ikke det at disse opplysningene ikke bør vernes. Det enkleste er antageligvis å gi tredjeperson mulighet til å ivareta egne interesser selv, ved å gjøre han oppmerksom på at opplysningene er utlevert.

Tvisteloven oppstiller ingen varslingsplikt. Etter personopplysningslovens system har den behandlingsansvarlige plikt til å varsle den registrerte dersom opplysningene brukes

[82] Rt-2010-1404 og LB-2010-64856

[83] Rt-2010-1404 premiss 29

til noe annet enn de ble innsamlet for. Når en tredjeperson med behandlingsansvar leverer ut informasjon til en annen behandlingsansvarlig/databehandler(domstolen/part), er det den som samler inn, som har plikt til å varsle, jf. personopplysningsloven § 20. Unntaket i personopplysningsforskriften § 1-3 fører til at tredjeperson mister denne retten til informasjon. Betydningen av å slippe å varsle har åpenbare fordeler for den advokat eller part som innsamler opplysninger i forbindelse med en rettssak. Avhengig av sakens størrelse og omfang, kan en varslingsplikt gi enorme arbeidsmengder som ikke står i forhold til ulempen det innebærer for tredjeperson å ikke bli varslet. For eksempel ville en bedrift som ble gjenstand for et gruppesøksmål få en formidabel jobbe med å varsle alle tredjepersoner som kunne være omfattet av bevismateriale som knyttet seg til gruppen.

Dersom noen bør pålegges en varslingsplikt, er det den som utleverer informasjon som er nærmest til å ta dette ansvaret. En parallell – uten sammenlignbarhet for øvrig – kan trekkes til det varselet banken er pålagt å sende sine kunder dersom den har utlevert kredittopplysninger. Etter personopplysningsforskriften § 4-4 skal "gjenpart, kopi eller annen melding" sendes den opplysningene gjelder, slik at denne får anledning til å rette opp i eventuelle feil. Like enkelt kunne det være for enhver som sitter med et behandlingsansvar å sende ut et varsel til tredjeperson ved utlevering av personopplysninger om denne. På den måten ville tredjeperson fått anledning til å ivareta sine egne interesser.

3.4 Bevissikring etter tvisteloven kapittel 28

3.4.1 Bevissikring uten å varsle - formål og hensyn

Som vist i punkt 3.3 oppstår plikten til å stille bevis til rådighet som hovedregel *under saksforberedelsen*. Tvisteloven kapittel 28 inneholder likevel regler om bevissikring utenfor rettssak, *før sak er reist*. I forarbeidene presiseres det at regelen er ment som et ekstraordinært virkemiddel med et snevert anvendelsesområde.[84] Behovet for å sikre bevis oppstår særlig for den typen bevismateriale som lett kan gå tapt. At dette gjelder

[84] NOU 2001:32 side 988

elektronisk lagret materiale illustreres ved at de fleste rettsavgjørelser om bevissikring gjelder nettopp elektroniske bevis.[85]

Spørsmålet er hvordan bevissikring kan føre til spredning av personopplysninger som er irrelevante for sakens opplysning, og om tvisteloven i slike situasjoner har regler som ivaretar partenes og tredjepersons personopplysningsvern. Tvisteloven § 28-3 fjerde ledd, gir adgang til å gjennomføre bevissikring *uten forhåndsvarsel* til motparten dersom det er grunn til å frykte for at varsel vil kunne hindre formålet med bevissikring.[86] Av forarbeidene fremgår det at formålet er å forhindre bevisforspillelse og derigjennom sikre materielt riktige avgjørelser.[87] Typisk situasjon vil være der det er grunn til å mistenke motparten for å ville *ødelegge* de aktuelle bevisene før bevissikring iverksettes, dersom vedkommende er varslet på forhånd. Eksempelvis ble sikring i "Normarc-saken" begrunnet i faren for at motparten, med sin datakyndighet, skulle manipulere materialet slik at bevis ble slettet og gikk tapt.[88]

Når det gis tillatelse til bevissikring uten å gi varsel, avsier retten kjennelse uten at den annen part har fått mulighet til å uttale seg. Denne fremgangsmåten representerer en mulighet til å "gå bak ryggen" til motparten. På denne bakgrunn er det viktig at reglene om bevissikring også ivaretar hensynet til den det søkes sikret hos, slik at bevissikringsinstituttet ikke blir et verktøy for å "fiske" etter private opplysninger om motparten. Muligheten for kontradiksjon kommer dersom motparten begjærer etterfølgende muntlige forhandlinger, hvilket først er aktuelt *etter* at sikring er gjennomført. Dette medfører at den som sitter på materialet fratas muligheten til å forhindre at sensitiv og/eller privat informasjon "følger med på lasset". Lovgiver har vurdert det slik at kontradiksjon på et tidlig stadium kan føre til at saken ikke blir tilstrekkelig opplyst, og slik hindre at man kommer frem til et materielt riktig resultat.[89]

---

[85] Robberstad (2010) side 160

[86] Bestemmelsen viderefører tvistemålsloven § 271a, som ble innført for å oppfylle Norges forpliktelser i henhold til TRIPS-avtalen artikkel 50 (Trade-Related Aspects of Intellectual Property Rights)

[87] Ot.prp.nr.33 (2003-2004) side 5 og Innst.O.nr.66 (2003-2004)

[88] TOSLO-2004-42431

[89] Ot.prp.nr.33 (2003-2004) punkt 3

Begrunnelsen er at retten til etterfølgende muntlig forhandling, muligheten til å holde tilbake beviset fra motparten, samt hensynet til å få saken opplyst veier opp for at kontradiksjon og offentlighet utsettes til senere. Dette endrer ikke det faktum at sikring kan oppleves som krenkende, særlig når sikring tillates i private hjem.

Det finnes flere eksempler på at tingretten har tillatt sikring i hjemme hos enkeltpersoner. Dette var tilfellet i en kjennelse avsagt i Oslo tingrett 8.januar 2009, heretter "Testament-saken". Saken var foranlediget av at (A) nylig hadde mistet sin bror (C), og i den anledning krevde bevissikring i C's datamaskiner og annet datamateriale hos sin svigerinne (B), og på C's arbeidsplass på bakgrunn av en mistanke om eksistensen av et senere testament enn oppgitt. På forespørsel hadde B nektet å oppgi navnene på forloverne, som var antatt å ha kunnskap om et testament, med den begrunnelse at de ønsket å være anonyme. Retten anså årsaken til kravet som konkret og ikke oppkonstruert, og uttalte at "A har objektive grunner til å føle en viss uro", at "konsekvensene av en eventuell uriktig avgjørelse uansett vil være beskjedne sammenlignet med en uriktig avgjørelse i motsatt retning" og tillot sikring.[90] Et annet eksempel er en kjennelse fra Asker og Bærum tingrett av 30.juni 2008, "Vema-saken". Saken gjaldt en tidligere arbeidsgiver (A)s ønske om å sikre bevis hos tidligere arbeidstager (B) etter mistanke om brudd på en konkurranseklausul i arbeidskontrakten. Retten ga den begjærende part tillatelse til å sikre e-post både fra arbeidsplass og hans privat hjem.[91] Retten viste til at det var "en nærliggende risiko for at X og Y ville forsøke å slette e-poster og gjøre e-poster utilgjengelig for motparten dersom de ble varslet.

I hjemmet oppbevarer man gjerne private informasjon om seg selv som er ikke taushetsbelagt, men vernet av husets "fire vegger" og regler om beskyttelse av privatlivets fred. I punkt 2.1 ble det presisert at regler om personopplysningsvern har som formål å verne om "personlig integritet, herunder autonomi og privatlivets fred".[92]

---

[90] Kjennelsen er unntatt fra offentlighet av hensyn til partene og sakens svært sensitive karakter, jf. domstolloven § 130 første ledd bokstavva. Utdrag gjengitt i TOSLO-2008-191303

[91] Asker og Bærum tingretts kjennelse av 30. juni 2008

[92] Schartum (2011) side 18

I tilknytning til bevissikringsreglene vil fokus i større grad rettes mot ivaretakelsen av hensynet til personlig integritet og privatlivets fred.

3.4.2 Den praktiske gjennomføringen

3.4.2.1 Hvem utfører selve sikringsakten?

Tvisteloven kapittel 28 inneholder ingen særskilte saksbehandlingsregler for gjennomføringen av bevissikring. I stedet gis reglene om tilgang til realbevis og bevisopptak i rettssak "anvendelse så langt de passer" jf. § 28-4. Uten bestemmelser som regulerer gjennomføringen, har domstolen gjennom rettspraksis antatt at bevissikring kan utføres med hjelp av *namsmannen*. I "Normarc-saken" knyttet verken lagmannsretten eller Høyesterett bemerkninger til tingrettens bruk av namsmannen. Fremgangsmåten ble fulgt opp av Asker og Bærum tingrett i "Tom&Jerry-saken" som uttalte at det ikke var noen reelle hensyn som tilsa en annen løsning.[93] I senere praksis er namsmannen ofte blitt gitt jobben med å gjennomføre bevissikringen. Det må kunne legges til grunn at dette er den gjeldende hovedregel.

Selv om namsmannen oppfyller kravet til uavhengighet fra partene, har de ikke større teknisk kompetanse enn domstolene. Tvisteloven § 27-2 fjerde ledd, som gjelder tilsvarende så langt det passer, jf. § 28-4, hjemler overlatelse av bevisundersøkelser til sakkyndige der "sakkyndighet er nødvendig". I "Normarc-saken" uttalte Høyesterett at det etter omstendighetene ville "kunne være nødvendig å få oppnevnt en sakkyndig for å få skilt ut det materialet som det kan være grunnlag for å sikre og gi tilgang til."[94] Både "Normarc-saken", "Vema-saken" og "Testament-saken", gir eksempler på at namsmannen får bistand fra sakkyndige. Flere eksempler fra tingretten viser at bruk av sakkyndige er vanlig ved bevissikring i elektronisk lagret materiale.[95]

For motpartens personvern har bruken av namsmann og teknisk sakkyndige både positive og negative konsekvenser. På en side innebærer løsningen en mer forsvarlig

[93] RG-2007-736

[94] Rt-2006-626

[95] for eksempel kjennelser fra Vesterålen tingrett 14. juli 2005 og Sandefjord tingrett 21. februar 2007

behandling av den sensitive informasjonen sammenlignet med at den begjærende part selv, med eller uten teknisk kompetanse, får tilgang til opplysningene. På en annen side innebærer det at enda flere får innsyn i informasjon som er privat. Til tross for regler om konfidensialitet og taushetsplikt, kan dette oppleves som inngripende.

3.4.2.2 Kan det brukes tvang?

Reglene om personopplysninger har blant annet som formål å sikre den personlige integritet.[96] Hvis bevissikring gjennomføres ved bruk av tvang, vil dette raskt kunne oppleves som en integritetskrenkelse. I "Tom&Jerry-saken" sammenlignes bevissikring med *ransaking* i straffeprosessen:

> "Dessverre innebærer lovgivningsteknikken med å nøye seg med å henvise til de regler som gjelder bevisopptak i rettssak, at man unnlater å ta stilling til de særegne praktiske og prinsipielle problemer som oppstår når retten uten kontradiksjon og varsel til motparten, på basis av en privatpersons, organisasjons eller bedrifts begjæring, skal beslutte noe som ligge svært nær det som kalles ransaking i straffeprosessen. "[97]

Dersom tvang skal tillates må det foreligge utrykkelig hjemmel i lov, jf. legalitetsprinsippet. Retten understreket at den ikke har kompetanse til å gi namsmannen rett til å bryte seg inn, men at den derimot kan pålegge den det skal sikres hos å gi tilgang til de(t) aktuelle lokale(r). Sikring gjennomføres da ved at man dukker opp uanmeldt og "banker på døren". Spørsmålet er hva som skjer hvis namsmannen blir nektet adgang.

Tvisteloven § 26-8 første ledd hjemler adgang til tvangsfullbyrdelse dersom *tredjeperson* nekter å oppfylle sin plikt til å stille bevis til rådighet under saksforberedelsen, men dette forutsetter at det foreligger rettskraftig kjennelse om slik fremleggelsesplikt.[98] Denne regelen passer ikke på bevissikring der motpart eller

---

[96] Schartum (2011) side 18

[97] RG-2007-736

[98] Schei (2007) side 1226

tredjeperson ikke på forhånd er varslet om at bevissikring skal gjennomføres. At tvisteloven ikke gir mulighet for å tvinge en part til å stille bevis til rådighet under saksforberedelsen, taler for at dette heller ikke kan skje på et tidligere stadium. Tolkningen støttes av den elektroniske lovkommentaren til tvisteloven hvor det uttales at det *ikke foreligger* hjemmel for tvang.[99] Asker og Bærum tingrett tolket åpenbart regelen på den måten da den i "Tom&Jerry-saken" understreket at den ikke kunne gi hjemmel til å bryte seg inn.[100]

I en annen retning går Scheis kommentar til tvisteloven hvor det antas at namsmannen *kan bruke de tvangsmidler som er gitt etter tvangsfullbyrdelsesloven*.[101] Tvangsfullbyrdelsesloven § 5-10 gir namsmannen hjemmel til å bruke nødvendig makt, og til å kreve bistand fra politiet, dersom det skulle bli nødvendig. Hvis man ikke har adgang til å bruke tvang, kan den som pålegges å gi tilgang enkelt nekte å gi adgang, og slik få mulighet til å varsle motparten og slette eller manipulere bevis før en eventuell rettssak. Dette vil medføre at reglene om bevissikring uten varsel uthules. På den annen side er det prinsipielt betenkelig å bruke namsmannen som fotsoldat for å skaffe parter bevis til en *sivil sak* hvor det ikke er tatt ut søksmål. Dette vil uten tvil oppleves som svært inngripende ovenfor den som må gi tilgang. Selv om rettens bruk av namsmann har karakter av fast praksis, finnes det ingen klar hjemmel som sier at tvangsfullbyrdelseslovens § 5-10 skal komme til anvendelse. Etter dette fremstår det som tvilsomt hvorvidt det er adgang til å bruke tvang ved bevissikring. Det man kan si er at dersom tvang er tillatt, burde det gis en klar lovhjemmel for dette.

3.4.2.3 Speilkopiering

"Tom&Jerry"- kjennelsen er interessant fordi retten knytter en del bemerkninger til den praktiske gjennomføringen av bevissikring. Retten uttalte:

> "Kanskje mer problematisk i praksis er hvorledes gjennomføringen skal skje i et samfunn hvor svært mye av det som i sivile saker vil være relevante bevismidler, befinner seg lagret i

[99] Reusch note 1365

[100] RG-2007-736

[101] Schei (2007) side 1259

elektronisk form, og gjerne på en server som kan befinne seg hvor som helst i verden. I så fall er det ikke noe fysisk å ta med seg før man ved hjelp av programvare, nødvendig systemkunnskap og passord kan få skrevet ut den informasjon som er relevant bevismiddel. Om dataene antas lagret på en i lokalet tilgjengelig PC, kan man tenke seg å ta med seg datamaskinen for nærmere undersøkelser. Da vil man imidlertid ta med seg masse overskuddsinformasjon som er irrelevant i forholdet mellom partene, og ikke skal være tilgjengelig for andre enn myndigheter med særlig hjemmel for tilgang til slik informasjon". [102]

Krav til *spesifisering* av hvilket materiale som ønskes sikret skal bidra til å forhindre at irrelevant materiale og overskuddsinformasjon følger med, men kravet er ikke tolket like strengt når det dreier seg om elektronisk lagret materiale.[103] I "Normarc-saken" uttalte Høyesterett at *praktiske forhold* gjør det vanskelig å spesifisere ved sikring av elektroniske data: *"*I tilfeller der det bevismessig er på det rene at det er foretatt ulovlig kopiering, bør da ikke kravet til spesifisering stilles så strengt at man blir avskåret fra å få vite hva som er ulovlig kopiert*"* [104].

Hvis man ikke vet nøyaktig hva man leter etter, kan det fort bli nødvendig å sikre alt innholdet, eller store mengder informasjon, for å "være på den sikre siden". Ved *speilkopiering* brukes et spesielt dataprogram til å kopiere alt innhold på ett medium over på et annet medium. En av fordelene er at dette sikrer at de tilhørende metadata og systemdata forblir intakte slik at speilkopien i større grad kan avsløre slettet og endret informasjon ved analyse. I tillegg er den korte tiden det tar å utføre prosedyren, kombinert med at motparten får beholde originalen, ansett å utgjøre en mindre ulempe for den det sikres hos. I en kjennelse fra Tinn og Heddal tingrett av 13. juni 2007, ble det anført at motparten ikke ville bli skadelidende av at det ble tatt en speilkopi, så lenge saksøker ikke kom i besittelse av kopiene, og disse ble beholdt i tingrettens eller nøytral tredjepersons besittelse. Gjennomgang av flere tingrettsavgjørelser viser at retten ofte påpeker at bevissikringen bør gjennomføres så skånsomt som mulig slik at

[102] RG-2007-736

[103] Rt-2006-626

[104] Rt-2006-626

den det sikres hos i minst mulig grad berøres av namsmannens intervensjon.[105]

I et sivilprosessperspektiv er utfordringen å gjennomføre sikringsakten på en måte som fører til at relevant materiale blir sikret, uten at man påfører den det sikres hos uforholdsmessig skade eller ulempe. I henhold til tvisteloven § 21-8 skal det "være et rimelig forhold mellom den betydningen tvisten har og omfanget av bevisføringen", og etter § 26-5 tredje ledd kan det nektes bevistilgang hvis det vil "medføre kostnader som ikke står i rimelig forhold til tvisten og den mulige verdien av beviset". Proporsjonalitetsprinsippet står så sterkt at det er lovfestet i tvisteloven formålsbestemmelse: "saksbehandlingen og kostnadene stå i et rimelig forhold til sakens betydning", jf. § 1-1 andre ledd fjerde strekpunkt. "Vema-saken" illustrerer hvordan proporsjonalitetsbetraktninger er avgjørende for utfallet av den interesseavveiningen retten må foreta etter tvisteloven § 28-3 fjerde ledd. Retten viste til hvordan departementet har veid disse hensynene, og uttalte at betenkeligheter med å tillate bevissikring uten å gi varsel ikke "knytter seg til at manglende kontradiksjon kan føre til uriktige avgjørelser, men til at ordningen kan påføre motparten uforholdsmessige tap eller bryderi sammenlignet med motpartens interesser. Retten mener at dette aspektet er viktig å ha for seg i interesseavveiningen, og at bevissikringen begrenses slik at den blir minst mulig inngripende for motparten." [106] (mine understrekninger).

Fra et *personvernperspektiv* kan det stilles spørsmål ved om speilkopiering er en skånsom måte å utføre bevissikring på ovenfor motparten? "Tap" og "bryderi" er ikke ulemper som naturlig kan knyttes til uønsket behandling av personopplysninger. Derimot er målsettingen om at sikring bør være "minst mulig inngripende" en referanse til personverninteresser. Hensynet til personopplysningsvern taler for at det ikke bør lagres mer informasjon enn det som er *nødvendig* for å oppnå formålet, som er å sikre bevis som kan belyse sakens faktum. At man kan gå inn sent en fredag og ta speilkopier utenom arbeidstiden, vil redusere en bedrifts risiko for økonomiske tap som følge av at maskiner må tas ut av drift, men faren for spredning av sensitiv informasjon i form av

[105] se for eksempel Sandefjord tingretts kjennelse av 21. februar 2007

[106] Ot.prp.nr.33 (2003-2004) side 5 og Asker og Bærum tingretts kjennelse av 30. juni 2008

så vel bedriftshemmeligheter som personopplysninger er større. For mange bedrifter, og særlig privatpersoner, vil det trolig være bedre om namsmannen brukte den tid som var nødvendig for å søke opp det materialet som var relevant for saken, selv om dette medførte økonomisk ulempe. Reglene for søk under sikringsakten må fastsettes av retten, og forutsetter at begjæringen gir retten grunnlag for å fastsette *søkeord* som er egnet til å sortere ut relevant informasjon. Dersom begjæringen ikke gir grunnlag for dette, kan det spørres om kravet til spesifikasjon er oppfylt. I "Vema-saken" fant retten at den mest skånsomme fremgangsmåten overfor X var å gi namsmannen 3 dager til å søke i PC'en etter relevant materiale.[107] Bevissikringen ble begrenset til de treff man fikk ved å søke etter filer som inneholdt navn på leverandører og konkurrenter. Dette må anses å være en betraktelig mer personvernvennlig metode, til tross for at PC'en ble beslaglagt i 3 dager.

3.4.3 Etterarbeidet

3.4.3.1 Søk i sikret bevismateriale og utlevering av treffene

Når materialet er sikret, registrert og deponert hos namsmannen, begynner den virkelige jobben med å finne frem til det som har bevisverdi. I den etterfølgende kontradiktoriske behandlingen kan partene forhandle om hvilken metode som skal brukes for å finne frem til relevante bevis, men selv med bruk av søkeord som partene er enige om, er det ingen garanti for at ikke svært sensitiv og personlig informasjon skal dukke opp. Bruk av søkeord vil både gi treff på relevant materiale og på filer som ikke skulle vært med, samtidig som relevant materiale faller utenfor treffene. Det er helt tilfeldig om treffene inneholder personopplysninger, og det finnes ingen regler eller retningslinjer for hvordan disse resultatene skal håndteres.

Når søket er fullført og de sakkyndige sitter med en samling informasjon basert på sine treff, er spørsmål hvor stor del av dette den begjærende part skal gis adgang til å se. På bakgrunn av at treffene fremdeles kan inneholde sensitiv informasjon, bør de ikke uten videre overlates til den begjærende part. Sakene fra underrettspraksis der begjæring er

[107] Asker og Bærum tingretts kjennelse av 30. juni 2008

tillatt, gir ingen informasjon om hvordan det sikrede materialet ble håndtert i ettertid, når det ikke foreligger etterfølgende muntlig forhandling eller andre etterfølgende avgjørelser. Vurderingsgrunnlaget er derfor spinkelt. Etter muntlige forhandlinger i saken fra Tinn og Heddal tingrett i 2007, bestemte retten at treffene fra de spesifiserte søkene kunne overleveres til den begjærende part etter at namsmannen hadde slettet overskuddmaterialet på en måte som "sikrer at de slettede filer ikke i ettertid kan rekonstrueres."[108] I "Testament-saken" hadde deler av materialet blitt sikret på C's arbeidsplass i domstol X. De sakkyndige hadde søkt etter alt som inneholdt ordet "testament", og organisert materialet etter treff på søkeordet. I en etterfølgende kjennelse bestemte retten at saksøkeren ikke fikk innsynsrett i dette treffmateriale, men at domstol X skulle få se treffene og vurdere om noe av materialet kunne være relevant for den gjeldende sak.[109] Dette ga den det ble sikret hos adgang til å sile ut relevant informasjon etter eget skjønn.

Hvis *den det sikres hos* skal være den som får lov til å sile ut relevant informasjon basert på treffene, oppstår spørsmål om i hvilken grad det er adgang til å "sensurere" søkeresultatet. En kan tenke seg sensur ved å ta ut informasjonen, eller å anonymisere den. En anonymisering vil være egnet til å fjerne belastningen av personopplysningene for den de gjelder.[110] I domstolloven er anonymisering et virkemiddel som blant annet brukes for å kunne offentliggjøre domstolens avgjørelser uten å krenke hensynet til personvern, se domstolloven § 130. Fullstendig unntak fra offentligheten tillates kun hvis anonymisering ikke er nok til å skjule den sensitive informasjonen. Dersom man overførte regelen på bevissikret materiale kan anonymisering i form av sladding være hovedregelen, og dersom dette ikke blir funnet tilstrekkelig, kan hele dokumentet unntas fra den begjærende parts innsyn. I en sak fra Høyesteretts som gjaldt krav om tilgang til bevis var spørsmålet om saksøker skulle få innsyn i originale forvaltningsdokumenter.[111] Retten kom frem til at saksøker kun fikk adgang til det sladdede materialet, men bestemte at originaldokumentene måtte legges frem for retten.

[108] Aust-Telemark tingretts kjennelse 2007

[109] TOSLO-2008-191303

[110] PVN-2003-02

[111] Rt-2011-837

En slik metode sikrer domstolen kontroll. Dersom motpart eller tredjeperson skal gis adgang til sensur, bør også denne kontrolleres av domstolen for å forhindre at ikke *relevant informasjon* lukes ut slik at formålet med bevissikring ikke oppnås.

3.4.3.2 Bruk av MD5-hash sjekknummer

Et av hovedproblemene med søk i speilkopier, er at det er vanskelig å finne en søkemetode som hindrer tilgang til irrelevant eller taushetsbelagt informasjon, og samtidig gir tilgang til relevante bevis. En løsning på problemet kan være å bruke såkalte ”sjekksummer”. I den nyeste kjennelsen i ”Normarc-saken” ga lagmannsretten Normarc/Aerodata tilgang til lister med såkalte ”MD5-hash sjekknummer”. MD5-hash er ”en ”sjekksum” i form av en entydig tallogaritme som er en unik identifisering av en/et konkret fil/dokument uavhengig av om filen er et worddokument, et bilde, et dataprogram eller noe annet.”[112] Sjekksummen kan betraktes som et ”fingeravtrykk” på den elektroniske filen. Hvis man får tilgang på sjekksummer fra det sikrede materiale, kan man sammenligne denne med sjekksummene på sin egen harddisk. Dersom man finner identiske sjekksummer, betyr dette at de samme filene foreligger på begge maskiner. Metoden innbærer ingen fare for avsløring av personlig informasjon, idet en sjekksum ikke gir noen mening i seg selv. Forutsetningen for et slikt søk er selvfølgelig at den begjærende part har et materiale å sammenligne sjekksummene med.

Et søk på lovdata viser at slik metode ikke er brukt i bevissikringssaker tidligere. Dersom sjekksummen gir en sikker identifisering, fremstår metoden som en personopplysningsvennlig måte å håndtere store mengder data på. Det er derfor merkelig at en slik metode ikke har blitt anvendt tidligere.

3.4.4 Tvistelovens sanksjon – erstatning

Etter tvisteloven § 28-3 femte ledd kan økonomisk tap en part er blitt påført som følge av bevissikringen utløse et erstatningskrav. Penger kan imidlertid ikke erstatte den skade som inngrep i ikke-økonomiske interesser medfører. Personverninteresser

[112] LB-2010-149042

kjennetegnes ved å være ideelle interesser. Det går ikke an å avveie økonomiske og kommersielle interesser mot ideelle interesser begrunnet i individets integritet og privatliv. Dette medfører at erstatningsreglene i § 28-3 ikke får noen særlig betydning for personopplysningsvernet.

3.4.5 Oppsummering

For elektronisk lagret materiale fremstår bevissikringsreglene som noe mer enn en snever unntaksregel. Dette tilsier at den praktiske gjennomføringen med fordel kunne vært lovregulert. Situasjonen i dag er svært skjønnspreget ved at det er opp til retten å avgjøre hvordan den praktiske gjennomføringen skal skje. Variasjon i kunnskap om gode metoder kan lede til forskjellsbehandling som får konsekvenser både for sakens opplysning og personopplysningsvernet. Veiledende retningslinjer kunne bidratt til en mer forutsigbar prosess, og sikret at de ulike hensyn ble ivaretatt på en forsvarlig måte. Bruken av MD5-sjekknummer i "Normarc-saken" viser at det kan foretas søk på en måte som gir nøyaktige treff i det relevante materialet, uten at hensynet til personvern må settes til side.

3.5 Føring av bevis som er innsamlet i strid med personopplysningsloven – spørsmålet om bevisavskjæring

3.5.1 Betydningen av regler om bevisforbud og -fritak og avskjæring av bevis

Et fellestrekk ved reglene om avskjæring i §§ 21-7 og 21-8 og reglene om bevisfritak og bevisforbud i kapittel 22, er at de i varierende grad bygger på interesseavveininger. Ved *absolutte bevisforbud* har lovgiver gjort en generell interesseavveining og kommet frem til at visse typer informasjon ikke kan føres, se for eksempel opplysninger om rettsforhandlinger og rettsavgjørelser i § 22-4 annet og tredje ledd. Det samme gjelder for *absolutte fritak,* for eksempel regler om nærstående opplysninger meddelt av parten i § 22-8 første ledd. Dersom den som beskyttes av bestemmelsen har mulighet til å *oppheve forbudet* er interesseavveiningen lagt til den enkelte, jf. § 22-3 annet ledd eller § 22-5 tredje ledd. I de tilfellene retten er gitt adgang til å *pålegge føring av beviset,* er avveiningen overlatt til domstolen.

Alle disse reglene er gitt av behovet for å ta hensyn til de interessene som kan tenkes krenket dersom en viss type informasjon brukes for å belyse saken. At lovgiver har laget ulike regler, til ulike typer informasjon, viser at behovet for vern er ansett som varierende. Betydningen av reglene ligger først og fremst i at adgangen til å bruke informasjon som inneholder personopplysninger *kontrolleres*. Denne lovgivningsteknikken sikrer adgangen til å tillate bevis som er nødvendige for å belyse saken, men påser samtidig at hensynet til øvrige interesser ikke settes til side dersom det ikke er nødvendig. På en måte kan man se på disse reglene som en del av tvistelovens system for å verne særlig sensitiv informasjon. Selv om hensynet til sakens opplysning i mange tilfeller vil skyve andre hensyn til side, vil kontrollen bidra til at den enkeltes rettssikkerhet ivaretas.

3.5.2 Bevisavskjæringsregelen i tvisteloven § 22-7

Et særlig bevisforbud følger av tvisteloven § 22-7 som bestemmer at retten "i særlige tilfeller kan nekte føring av bevis som er skaffet til veie på en utilbørlig måte". Som en tredje innfallsvinkel til hvordan personopplysningslovens regler får betydning i sivile saker, undersøkes det i det følgende hvordan domstolene anvender bevisavskjæringsregelen i tilfeller hvor bevis er innhentet i strid med personopplysningsloven. Domstolenes avvisningspraksis får i siste innstans betydning for hvilket vern personopplysninger har under personopplysningsloven når de inngår i bevismateriale for en sivil sak i domstolen.

Tvisteloven § 22-7 oppstiller vilkår om at beviset må være fremskaffet på en *utilbørlig måte,* og at føring av beviset vil kunne *krenke tungtveiende rettsikkerhets- og personvernhensyn*.[113] Begge vilkår må være oppfylt for at bevise skal avskjæres, jf. Rt-2003-1266, hvor Høyesterett opphevet lagmannsrettens kjennelse fordi de hadde hoppet rett inn i en interesseavveining uten å ta stilling til om "de aktuelle bevis krenket personopplysningsloven" eller "på annen måte kan anses for å være fremskaffet på

[113] NOU 2001:32 side 961

utilbørlig måte".[114] Ordet "utilbørlig" er valgt fremfor "ulovlig" for å markere at det ikke stilles krav om at fremskaffelsen har brutt positive lovbestemmelser.[115] Hvorvidt et brudd på formell lov alltid vil oppfylle kravet til utilbørlig, er grundig drøftet i Scheis kommentarutgave til tvisteloven.[116] Der konkluderes det med at brudd på en klar lovhjemmel alltid vil oppfylle grunnkravet, men at lovbruddets karakter og alvorlighetsgrad får betydning som moment i den interesseavveiningen som må foretas i trinn to. Denne fremgangsmåten har vært brukt av Høyesterett i en rekke saker, blant annet i Rt-1992-698, Rt-2004-858 og Rt-2006-582. Tolkningen støttes også av forarbeidenes forutsetning om å videreføre den ulovfestede bevisforbudsregelen om ulovlig fremskaffet bevis.[117] Etter dette må det kunne legges til grunn at *brudd på personopplysningsloven* vil oppfylle utilbørlighetskravet, men at bevisavskjæring beror på en vurdering av om føring av beviset medfører en krenkelse av tungtveiende rettssikkerhets- eller personvernhensyn. At personopplysningsloven er brutt, vil normalt innebære at personvernhensyn er krenket. Spørsmålet er derfor om føring av beviset vil representere en fortsatt og forsterket krenkelse. Dette vil ofte være tilfellet når utilbørlig innhentet bevis tillates ført. Dersom så er tilfellet, vil føring bero på en avveining mot hensynet til sakens opplysning og det materielle sannhetsprinsipp.[118]

I den ene enden av skalaen befinner lyd- og bildeopptak seg. Tendensen i rettspraksis er at ulovlige og utilbørlig ervervede bildeopptak som hovedregel ikke tillates benyttet som bevismiddel i sivile saker, jf. Rt-2001-668 ("Videoovervåking") og Rt-2004-878 ("Videoopptak"). Arbeidsgivers skjulte opptak av sine ansatte på arbeidsplassen har blitt ansett som et alvorlig inngrep som strider mot ulovfestede prinsipper om personvern. Opplysningsverdien i slike opptak må vike for hensynet til personvern. Personopplysningsloven har særlige regler om fjernsynsovervåking i kapittel VII, og i "Videoopptak-saken" ble utilbørligheten knyttet til brudd på personopplysningsloven

[114] Rt-2003-1266 avsnitt 20

[115] NOU 2001:32 side 961

[116] Schei (2007) side 1098-1099

[117] Schei (2007) side 1098-1099

[118] Ot.prp.nr.51 (2004-2005) side 459

§ 36. Ved brudd på slike regler har hensynet til personverninteresser blitt tillagt avgjørende vekt.

Brudd på personopplysningsloven kan likevel ikke alltid begrunne unntak i den frie bevisførsel. En årsak er personopplysningslovens høye abstraksjonsnivå som kan føre til at tolkning og anvendelse av loven i konkrete tilfeller kan volde tvil.[119] Brudd på personopplysningsloven kan dermed fremstå som mindre alvorlig, og føre til at interesseavveiningen går i favør av sakens opplysning. En advokat som brøt personopplysningsforskriftens regler ved oversendelse av sensitiv informasjon til namsretten, ble frikjent for anklagen om brudd på god advokatskikk.[120] I begrunnelsen la Disiplinærutvalget vekt på at Datatilsynets tolkning av personopplysningsforskriften § 1-3 fremsto som uklar, og det faktum at verken namsmann eller oppdragsgiver syntes å ha innsett at innsendingen kunne komme i konflikt med personopplysningsloven. En annen årsak er at brudd på personopplysningsloven ikke alltid oppleves like krenkende av dem det gjelder. Rettspraksis tyder på at krenkelsen ikke kan oppleves like alvorlig når arbeidsgiver skaffer seg innsyn i ansattes e-post og internettbruk. Ved mistanke om brudd på regler, kan arbeidsgiver se behov for å føre kontroll med de ansatte. Innsyn vil i mangel av samtykke fra den det gjelder, kreve at behandling har nødvendighetsgrunnlag i personopplysningsloven § 8 f. I interesseavveiningen må arbeidsgiverens behov for undersøkelser begrunnet i et legitimt behov for kontroll avveies mot den ansattes interesse i beskyttelse mot innhenting og bruk av opplysninger om personlige forhold. Samlet gir rettspraksis inntrykk av at arbeidsgiverens overvåkning av ansattes internettbruk representerer et mindre inngrep i personvernet enn ulovlig innhenting av lyd- og bildeopptak.[121]

Et eksempel på at bevis innhentet i strid med personopplysningsloven likevel ble tillatt ført er inntatt i RG-2004-347. I en arbeidsrettssak om oppsigelse fremla en arbeidsgiver filer som inneholdt pornografisk materiale hentet fra arbeidstagerens PC. Filene stammet fra arbeidstagerens *private område* på en PC som var satt til disposisjon av

[119] Schei (2007) side 1100

[120] ADA-2003-37

[121] Schei (2007) side 1103

arbeidsgiver. Innhentingen av filer uten varsel ble derfor ansett å være i strid med personopplysningsloven § 8. Beviset ble likevel tillatt ført. Lagmannsretten uttalte at "krenkelsen av personvernet gjennom brudd på bestemmelsene i personopplysningsloven er selvsagt alvorlig. Likevel må hensynet til sakens opplysning etter lagmannsrettens oppfatning tillegges utslagsgivende vekt."

En kjennelse fra Hålogaland lagmannsrett av 10. mars 2011 ("GPS-saken") gir et annet eksempel på at bevis tillates ført til tross for at innhentingen strider med personopplysningsloven. Lagmannsretten fastslo at utilbørlighetsvilkåret var oppfylt ved at arbeidsgiver hadde sammenstilt opplysninger fra en GPS med annen informasjon for å skaffe bevis for at en ansatt sjåfør ikke hadde gjort jobben sin. Retten kom likevel frem til at utskrifter av GPS-loggen kunne framlegges som bevis. Lagmannsretten uttalte:

> "Som et generelt utgangspunkt må overvåking ved bruk av GPS karakteriseres som mindre inngripende i sentrale rettsgoder enn overvåking ved bruk av lyd og bilde.[…] Føring av beviset kan vanskelig ses på som annet enn en fortsatt krenkelse av arbeidstakeren. Dette vil imidlertid ofte være situasjonen dersom bevis som er skaffet til veie på utilbørlig måte tillates ført. I tilknytning til dette hensynet legger lagmannsretten stor vekt på at graden av krenkelse er beskjeden. " [122]

I interesseavveiningen la lagmannsretten vekt på at beviset kunne bidra til sakens opplysning og være av vesentlig betydning for å oppnå en materielt riktig avgjørelse i saken. Sammenholdet med at utilbørligheten ikke ble ansett som særlig grov, og at krenkelsen var begrenset, ble resultatet at beviset ble tillat ført.

Avgjørelsene viser at brudd på personopplysningsloven ikke er tilstrekkelig til å begrunne unntak i den frie bevisføring. Unntak fra den frie bevisføring må forankres i interesseavveiningen domstolen må foreta. I både RG-2004-347 og "GPS-saken" ble arbeidsgivers bevis tillatt brukt til tross for at de var innhentet i strid med personopplysningslovens regler. Det er tankevekkende at brudd på

[122] RG-2011-321

personopplysningsloven ikke medfører konsekvenser for arbeidsgiver. Dersom brudd på personopplysningsloven kan gi de bevis en trenger for å få frem fakta i saken, uten at bruddet i seg selv medfører konsekvenser, er det grunn til å tro at loven vil bli brutt. Da Datatilsynet og Personvernnemnda ble forelagt spørsmålet om fortsatt behandling av GPS-opplysninger ville være lovlig etter personopplysningsloven, var svaret nei. Jeg må si meg enig med Datatilsynet når de uttaler:

> ”Datatilsynet er av den oppfatning at Hålogaland lagmannsretts kjennelse av 10.3.2011, hvor Avfallsservice tillates å legge frem GPS-data som bevis i sak om oppsigelse av arbeidsforholdet, sender et uheldig signal til arbeidsgivere i en tilsvarende situasjon […] Datatilsynet er bekymret for situasjoner hvor arbeidsgivere spekulerer i å samle og/eller sammenstille opplysninger for senere bruk i tvister i arbeidsforholdet til tross for at det fremstår som brudd på personopplysningsregelverket” (min understrekning)[123]

[123] PVN-2011-04 punkt 5

4 AVSLUTTENDE VURDERINGER

Problemstillingen ble innledningsvis i oppgaven formulert som et spørsmål om *i hvilken grad tvisteloven ivaretar hensynene som personopplysningsloven bygger på ved behandling av personopplysninger i sivile saker*. Oppgaven gir ingen uttømmende oversikt over alle regler i tvisteloven som kan få betydning for behandling av personopplysninger i den sivile rettspleie. Svaret på i hvilken grad tvisteloven ivaretar grunnleggende personvernhensyn må derfor avgrenses til de observasjoner som kan utledes av behandlingen av de utvalgte eksempler i kapittel 3.

Basert på de få kildene som finnes om personopplysningsforskriften § 1-3, kan det konstateres at det er uklart hvordan bestemmelsen skal og bør komme til anvendelse. Fordi personopplysningsloven regulerer omfattende plikter og rettigheter for ulike aktører, er det viktig å vite hvor grensen for når loven kommer til anvendelse skal trekkes. Hvis grensen blir for skjønnsmessig, blir reglene vanskelige å anvende.

Min vurdering av tvistelovens regler, er utført under forutseting om at personopplysningsloven ikke kommer til anvendelse på behandling av personopplysninger i en sak som kan eller skal føres for domstolen. Konsekvensen av en slik tolkning er at personopplysningsvernet i sivile saker begrenses der tvisteloven ikke oppstiller tilsvarende rettigheter. Gjennomgangen av plikten til å stille elektroniske bevis til rådighet, viser at dette særlig rammer tredjeperson som ikke er part eller partshjelper i saken. Tvisteloven oppstiller ingen plikt til å informere tredjeperson når det innhentes opplysninger som kan knyttes til han. Resultatet er at ivaretakelsen av tredjepersons personopplysningsvern får et tilfeldig preg.

Drøftelsen av bevissikring avdekker at det er reglene om bevissikring uten forhåndsvarsel som i minst grad tar hensyn til personopplysningsvernet. Det er likevel ikke åpenbart at bevissikring hadde blitt gjennomført annerledes hvis man ser bort i fra regelen i § 1-3. En utvidet rett til varsling og innsyn for den sikringen retter seg mot

ville umuliggjøre formålet med bevissikringen, og forhindre Norge i å oppfylle forpliktelsene etter TRIPS-avtalen. Ved slik motstrid bestemmer personopplysningsloven § 5 at de særlige reglene i tvisteloven går foran, jf. lex specailis-prinsippet. At tvisteloven ikke har særlige regler for den praktiske gjennomføringen av bevissikring, er en annen sak. Det kunne med fordel blitt utarbeidet retningslinjer for hvordan sikringsakten og gjennomgangen av det sikrede materialet bør foregå. Herunder regler om siling av resultatet, og mulighet for anonymisering av personopplysninger der dette ikke fjerner informasjon som er nødvendig for sakens opplysning. Slik kunne reglene ivaretatt hensynet til personvern, uten at det gikk utover formålet med reglene.

Det er vanskelig å felle en streng dom over tvisteloven. Som vist, bygger både tvisteloven og personopplysningsloven på en rekke interesseavveininger. Denne lovgivningsteknikken sikrer adgangen til å tillate bevis som er nødvendige for å belyse saken, men påser samtidig at hensynet til øvrige interesser ikke settes til side dersom det ikke er nødvendig. Domstolenes avveininger etter tvisteloven må sees i lys av det overordnede formål om å finne frem til et materielt riktig resultat. Formålet illustreres ved at domstolen viser tilbakeholdenhet med å avskjære bevis som kan opplyse saken, selv om lover og regler er brutt ved innhentingen. Konsekvensene av å avskjære sentrale bevis man vet eksisterer, er også egnet til å svekke borgernes tillitt til rettsvesenet. Å bruke avskjæring som sanksjon for brudd på personopplysningsloven, fremstår derfor som et lite adekvat virkemiddel for å hindre fremtidige brudd. Datatilsynets mulighet til å ilegge overtredelsesgebyr kan være en passende straff med tilsvarende preventiv effekt.

Det er overraskende at betydningen av § 1-3 ikke har blitt behandlet. Verken lovgiver eller juridiske forfattere behandler spørsmålet om unntakets betydning for den sivile rettspleie, og domstolene har i liten grad vært nødt til å behandle spørsmål om bestemmelsens rekkevidde. Etter min mening er det på tide at unntaket blir grundig analysert, både internrettslig, og i forhold til EØS-retten. En retningsgivende tolkning kunne forhåpentligvis bidra med å fjerne noe av den usikkerhet som knytter seg til anvendelsen av personopplysningsloven. Dersom en vurdering skulle konkludere med

at bestemmelsen unntar personopplysningsloven i like stor grad som denne oppgaven forutsetter, burde unntaket dessuten vurderes plassert i lovteksten som et eget unntak fra lovens saklige virkeområde.[124] En bestemmelse som gjør et så vesentlig unntak fra en lovs virkeområde, bør ikke stå i en forskrift.

[124] En slik teknisk endring ble foreslått i forslaget til revisjon av personopplysningsloven som ble utført i 2006. Se Bygrave (2006) side 183

5 KILDELISTE

5.1 Lover og forskrifter

1915 Domstolloven: *Lov om domstolene* av 13. august 1915 nr. 5.

1961 Åndsverkloven: Lov om opphavsrett til åndsverk m.v. av 12. mai 1961 nr. 2.

1967 Forvaltningsloven: *Lov om behandlingsmåten i forvaltningssaker* av 10. februar 1967 nr.98

2000 Personopplysningsloven: *Lov om behandling av personopplysninger* av 14. april 2000 nr. 31.

2000 Personopplysningsforskriften: *Forskrift om behandling av personopplysninger* av 15.desember 2000 nr. 1265

2005 Tvisteloven: Lov om mekling og rettergang i sivile tvister av 17. juni 2005 nr. 90.

2011 Gjennomføring av EUs datalagringsdirektiv i norsk rett: *Lov om endringer i ekomloven og straffeprosessloven mv.* av 15. april 2011 nr. 11

5.2 Forarbeider

NOU:1997:19	Et bedre personvern - forslag til lov om behandling av personopplysninger
NOU 2001:32	Rett på sak – Lov om tvisteløsning (tvisteloven)
NOU 2003:21	Kriminalitetsbekjempelse og personvern - politiets og påtalemyndighetens behandling av opplysninger
NOU 2009:1	Individ og integritet – Personvern i det digitale samfunnet
NOU 2009:15	Skjult informasjon – åpen kontroll Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker

Ot.prp.nr.92 (1998-1999)	Om lov om behandling av personopplysninger (personopplysningsloven)
Ot.prp. nr. 33 (2003-2004)	Om lov om endringer i tvistemålsloven (bevisopptak utenfor rettssak)
Ot.prp.nr.51 (2004-2005)	Om lov om mekling og rettergang i sivile tvister (tvisteloven)
Innst.O.nr.66 (2003-2004)	Innstilling fra justiskomiteen om lov om endringer i tvistemålsloven (bevisopptak utenfor rettssak)

Kongelig Resolusjon av 15. desember 2000 nr. 1265

5.3 Rettspraksis

Rt-2001-668	(Videoovervåkning)
Rt-2003-1266	
Rt-2004-878	(Videopptak)
Rt-2006-626	(Normarc)
Rt-2009-125	
Rt-2009-1689	(Testament)
Rt-2010-1404	
Rt-2010-1409	
Rt-2010-774	(Altibox)
Rt-2011-753	(Bokhandleren i Kabul)
Rt-2011-837	
RG-2004-347	
RG-2007-736	(Tom&Jerry)
RG-2011-321	(GPS)
LB-2005-59502	(Normarc)

LB-2009-137376 (Testament)

LB-2010-64856

LB-2010-149042 (Normarc)

TOSLO-2004-42431 (Normarc)

TOSLO-2008-191303 (Testament)

TSTAV-2009-55827 (Altibox)

TOSLO-2009-22961-1(Normarc)

TTONS-2009-126809

TBERG-2011-13681

Asker og Bærum tingretts kjennelse av 30.juni 2008 (Vema)

Aust-Telemark tingretts kjennelse 07-090161TVI-AUTE

Hålogaland lagmannsrett av 10. mars 2011

Oslo tingretts kjennelse av 8. januar 2009 (Testament)

Oslo tingretts kjennelse av 3. november 2009

Sandefjord tingretts kjennelse av 21. februar 2007

Tinn og Heddal tingretts kjennelse av 13. juni 2007

Vesterålen tingretts kjennelse av 14. juli 2005

5.4 Forvaltningspraksis

PVN-2003-02

PVN-2008-02 SSP

PVN-2009-18

PVN-2011-04

ADA-2003-37

5.5 Utenlandske lover og EU-direktiver

Personuppgiftslag	Lov nr 204 av 29. April 1998. Peronuppgiftslagen [Sverige]
Persondataloven	Lov nr 429 af 31. Mai 2000 om behandling av personopplysninger. Persondataloven. [Danmark]
EP/Rdir 95/46/EC	Europa-parlamentets og Rådets direktiv 95/46/EC av 24. oktober 1995 om personvern
EP/Rdir 2006/24/EF	Europa-parlamentets og Rådets direktiv 2006/24/EF av 15. mars 2006 om lagringsplikt for tilbydere av offentlig tilgjengelig elektroniske kommunikasjonstjenester eller elektroniske kommunikasjonsnett

5.6 Litteratur

Bygrave, Dag Lee og Dag Wiese Schartum. *Utredning av behov for endringer i personopplysningsloven*, skrevet etter oppdrag fra Justisdepartementet og Moderniseringsdepartementet, Justis- og politidepartementet, Oslo 2006.

Coll, Line, i samarbeid med Dag Wiese Schartum, *Rettslige spørsmål knyttet til innsamling og bruk av digitale bevis*. På oppdrag fra Norsk Regnesentral, oktober 2004

Farbrot, Sven. *Bevisopptak utenfor rettssak – bevissikring uten varsel til motparten ved bevisforspillelsesfare i sivilretten.* Masteroppgave, UiO 2007

Fredriksen, Halvard Haukeland. *Tvisteloven og EØS-avtalen*. Tidsskrift for rettsvitenskap 2008 side 289-357

Haram, Kristin. *Advokaters plikter etter personopplysningsloven.* Oversikt utarbeidet for Advokatforeningen per 22.2.2008, (online) Advokatforeningens hjemmesider http://advokatforeningen.no/Drift-av-advokatvirksomhet/Klientforholdet/Behandling-av-personopplysninger/Advokaters-plikter-etter-personopplysningsloven-Ved-behandling-av-personopplysninger-om-klienter/

Høgberg, Alf Petter og Njål Høstmelingen. *Grunnlovfesting av retten til privatliv?* Jussens Venner 2010 side 98

Johansen, Michal Wiik, Knut-Brede Kaspersen, Åste Marie Bergseng Skullerud. *Personopplysningsloven Kommentarutgave.* 1.utg. Oslo, 2001

Monsen, Erik, *Bevistilgang til elektronisk lagret material.* Tidskrift for Forretningjus 2007 side 194

Robberstad, Anne. *Sivilprosessen*. Oslo, 2009

Schei, Tore med flere. *Tvisteloven Kommentarutgave.* Bind II, Oslo, 2007

Schartum, Dag Wiese. *Lov om behandling av personopplysninger.* Lov og Rett 2000 side 543

Schartum, Dag Wiese. *Personvern og transportsikkerhet - Personvernmessige spørsmål knyttet til tiltak for å sikre transportmidler mot fiendtlige anslag*. Complex nr. 3/2007

Schartum, Dag Wiese. *Rapport om personvern og trafikksikkerhetsteknologi.* 2010 http://www.vegvesen.no/_attachment/196560/binary/382478

Schartum, Dag Wiese og Lee A. Bygrave. Personvern i informasjonssamfunnet – En innføring i vern av personopplysningsvern. 2.utg. Oslo, 2011

Thorvaldsen, Kjell, Åsmund Skomedal og Trond Ericson. *Bevisverdien av elektronisk informasjon*. Revisjon og Regnskap. 2007 artikkel nr.4

Torgersen, Runar. *Bør adgangen til bevisavskjæring i straffesaker utvides?* Festskrift til Carl August Fleischer 2006 side 533. Universitetsforlaget

5.7 Norsk Lovkommentar

Bernt, Jan Fridthjof. *Kommentar til Forvaltningsloven*(online), note 55 og 56 [sitert 17. november 2011]

Reusch, Christian H.P. med assistanse av flere. *Kommentar til Tvisteloven*. (online) note 1054,1072,1336,1349,1350,1355, 1365 [sitert 17.november 2011]

5.8 Diverse nettdokumenter

Delrapport fra Personvernkommisjonen. *Medier og Personvern.* 10. september 2008 http://folk.uio.no/gisle/pvk/docs/medierogpv.pdf

Høringsbrev fra Justis- og politidepartementet. *Høring - prøveordning med elektronisk kommunikasjon og endring i forskrift om postforkynning.* 30. juni 2011, (online) Regjeringens hjemmesider http://www.regjeringen.no/nb/dep/jd/dok/hoeringer/hoeringsdok/2011/horing---proveordning-med-elektronisk-ko/horingsbrev.html?id=650419

Høringsuttalelse fra Datatilsynet. *Forslag til ny forskrift om prøveordning med elektronisk kommunikasjon med domstolene og forslag om endringer i forskrift om postforkynning.* 14. september 2011, (online) Datatilsynets hjemmesider http://datatilsynet.no/upload/hoering/2011/11-00706-2%20Høringsuttalelse%20-%20Forslag%20til%20ny%20forskrift%20om%20prøveordning%20med%20elektronisk%20kommunikasjon%20med%20domsto%20466216_8_0.pdf

Definisjon ”informasjons- og kommunikasjonsteknologi”. (sitert 2011-11-08) I *Store norske leksikon*. Hentet fra http://snl.no/informasjons-_og_kommunikasjonsteknologi

5.9 Personlig meddelelse

Haram, Kristin. E-post. 24.oktober 2011

Schartum, Dag Wiese. E-post. 26.oktober 2011

A