Adgangen til overføring av personopplysninger til utlandet

Kandidatnummer: 129

Antall ord: 14827

JUS399 Masteroppgave

Det juridiske fakultet

UNIVERSITETET I BERGEN

31.5.2016

Innholdsfortegnelse

1 Innledning

1.1 Problemstillingen

Avhandlingens tema er personopplysningslovens (pol.) regler om adgangen til å overføre personopplysninger til andre land. Dette knytter seg i hovedsak til § 29, med hovedvilkår om at mottaker må sikre "*forsvarlig behandling*", og unntaksbestemmelsen i § 30. Det vil fremgå at reguleringen etterlater betydelig tolkningstvil. Avhandlingens formål er derfor å redegjøre nærmere for bestemmelsenes innhold.

Lovgivningens uskarpe grenser harmonerer dårlig med at det i praksis kan tenkes atskillige formål for overføring av personopplysninger til utlandet, og de skadevirkninger dette kan ha. For å belyse problemets størrelse er det derfor innledningsvis nødvendig å anlegge et bredt rettskilde- og samfunnsmessig perspektiv.

Gjennom de siste tiårene har digitalisering av flere livsområder skutt fart, og Norge er verdensledende på området, foran Island og Korea.[1] IKT-bruken har bidratt til sterk produktivitetsvekst i forretningslivet,[2] og til nye former for sosial interaksjon i privatlivet.

I Europa estimerer EU-kommisjonen ("Kommisjonen") at harmonisering av et indre digitalt marked kan medføre opp mot 4000 milliarder koner i årlige inntjeninger og besparelser, og skape hundretusener av nye jobber.[3]

Ved siden av fordelene innebærer digitaliseringen to hovedutfordringer for personvernet: Økt fare for overvåkning fra personer, virksomheter og myndigheter, og økt fare for utilsiktet spredning og anvendelse av personopplysninger. Dette gjelder så vel innad i Norge som på tvers av landegrenser, ettersom telenett, internett og GPS ikke påvirkes nevneverdig av territorielle skillelinjer.

Dette utfordrer selvbestemmelsesretten; særlig råderetten over hvilke personlige opplysninger en ønsker å dele med andre, og retten til å leve uten at noen konstant følger med på hva en gjør. Med kommersialiseringen av personopplysninger som har funnet sted de siste årene er

[1] Lysneutvalget 2014-2015: <https://www.difi.no/sites/difino/files/olav_lysne.pdf>, innhentet 13.5.2016, s. 6; med videre henvisning til Booz & Company 2012.
[2] Finansdepartementet, Meld. St. 12 (2012-2013): *Perspektivmeldingen 2013*, s. 55.
[3] EU-kommisjonen: *Why we need a Digital Single Market* <http://ec.europa.eu/priorities/sites/beta-political/files/dsm-factsheet_en.pdf>, innhentet 6.4.2016.

det ikke bare tale om vern mot myndighetenes konstante blikk, men også mot private virksomheters overvåkning.[4]

1.2 Temaets historikk og aktualitet

"Personvern" er et vidt begrep som er utfordrende å avgrense presist. Et kjent utgangspunkt er likevel å knytte det til EMK artikkel 8 nr. 1, som stadfester retten til respekt for "[*s*]*itt privatliv og familieliv, sitt hjem og sin korrespondanse.*" Dette fremgår også av Grunnloven § 102. I tillegg angår personvernet tanke-, samvittighets- og religionsfrihet, jf. EMK art. 9.

Personvern dreier seg altså om retten til å verne om opplysninger knyttet til ens person og private anliggender i vid forstand. I offentlig debatt benyttes ordet gjerne synonymt med "*privatlivets fred*" og "*personlig integritet*".

I norsk juridisk teori dukket begrepet først opp på begynnelsen av 1970-tallet, da Erik Samuelsen skrev om "personlighetsvern".[5] Etterhvert fikk vi "personvern", som ble anvendt i forbindelse med utredningene til personopplysningslovens forgjenger, personregisterloven av 1978.[6]

Hva gjelder rettspraksis er To mistenkelige personer-dommen (Rt. 1952 s. 1217) og Sykejournaldommen (Rt. 1977 s. 1035) særlig viktige på personvernområdet, som for øvrig ikke har hatt spesielt mange dommer.[7] Her kan også nevnes Høyesteretts kjennelse Rt. 1915 s. 32, som er en av våre første personvernrettslige domstolsavgjørelser. I kjennelsen fastslås at offentliggjøring av arbeidsstilling kan utgjøre krenkelse av "*personlige forhold*", etter den gamle straffelovens (strl. 1902) § 390.[8]

[4] Datatilsynet: *Det store datakappløpet: Rapport om hvordan kommersiell bruk av personopplysninger utfordrer personvernet*, november 2015, s. 42.
[5] Samuelsen, Erik: *Statlige databanker og personlighetsvern: Rapport fra et forskningsprosjekt*, Universitetsforlaget, Oslo 1972.
[6] For en nærmere gjennomgang og kritikk av personvernbegrepet, se Kvam, Bjarne: *Politiets persondatarett: En studie av hjemmels- og formålskrav ved politiets utlevering av personopplysninger til utlandet*, Universitetet i Bergen 2013, s. 56-61.
[7] Rettspraksis omtales videre under pkt. 2.3 nedenfor.
[8] Se videre Bing, Jon: *Personvern i faresonen*, Cappelen, Oslo 1991, s. 21-22.

Senere på 1900-tallet ble det også debatt rundt opprettelsen og bruken av fødselsnumre. Oslo skolestyres utlevering av personopplysninger om unge gutter til *Metropolittundersøkelsen*[9] ble også sterkt kritisert, bl.a. av høyesterettsadvokat Knut Tvedt og professor Knut S. Selmer.[10]

Til forskjell fra de spredte problemstillingene gjennom det siste århundret, har vi aldri hatt så mange og store personvernsmessige utfordringer som i dag. Grunnen til dette ligger hovedsakelig i den teknologiske utviklingen, som har gjort det mulig å samle inn og sammenstille massive mengder data mer effektivt, og lettere gi et detaljert bilde av en person.

Digitaliseringen har bidratt til at offentlige og private bransjer og virksomheter nå baserer seg på personopplysninger i et omfang som savner sidestykke. Dette gjelder bl.a. skatteetaten, banker, offentlige og private helsetjenesteytere, utdanningsinstitusjoner, forsikringsselskaper, statlige og private sikkerhetsvirksomheter, og reisebyråer og andre virksomheter som selger varer og tjenester via internettet.

Særlig stor bruk av personopplysninger ses i annonseindustrien, hvor Schibsted er Norges største aktør. Denne industrien baserer seg bl.a. på annonsebørser, som har vokst hurtig siden oppstarten i 2007.[11]

På annonsebørsene byr annonsebedrifter på pakker av personopplysninger om enkeltindivider (unntatt navn) som er innhentet gjennom deres internettbruk. Prisen avhenger av mengde og type informasjon; f.eks. øker snittprisen betraktelig, fra ca. 0,004 kr til nesten 1 kr, dersom det er tale om en kvinne som er gravid i sjette måned, og med det dobbelte om pakken inneholder opplysninger om en persons medisinbruk.[12]

Budrunden skjer i løpet av millisekunder, og nettbrukere ser vinnerens annonser på nettstedet en besøker. Til grunn for denne målrettede annonseringen ligger kartlegging av massive mengder informasjon om personers nettvaner, preferanser og behov generelt. En av de største aktørene er amerikanske Acxiom, som lagrer opplysninger om 700 millioner registrerte individer verden over, med i snitt 3000 opplysninger om hver person.[13]

Selv om opplysningene ikke knyttes til navn gjør mengden av informasjon (som antatt alder, kjønn og bosted) det ofte fullt mulig å identifisere enkeltindivider. Til tross for at de fleste internettbrukere ikke kjenner til at

---

[9] En større folkeundersøkelse på 1960-tallet, rettet mot bedre yrkesveiledning og sosialhjelp. I undersøkelsen ble det samlet inn opplysninger om unge gutter, som navn, bolig, forsørgers yrke, karakterer og IQ, jf. <https://www.etikkom.no/fbib/introduksjon/systematiske-og-historiske-perspektiver/forskningsetikkens-historie/>, innhentet 16.5.2016.

[10] Johansen, Michal Wiik og Kaspersen, Knut-Brede m.fl.: *Personopplysningsloven kommentarutgave*, Universitetsforlaget, Oslo 2011, s. 33-36.

[11] Datatilsynet: *Det store datakappløpet*, op.cit., s. 9.

[12] Datatilsynet: *Det store datakappløpet*, op.cit., s. 25; med videre henvisning til Financial Times: *How much is your personal data worth?* <http://www.ft.com/intl/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html#axzz3lAaLdwax>, innhentet 30.3.2016.

[13] Federal Trade Commission: *Data Brokers: A Call for Transparency and Accountability*, Washington D.C., mai 2014 <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>, innhentet 30.3.2016, s. 8.

denne omsetningen av deres personopplysninger skjer ved samtlige kommersielle nettsteder en besøker, foregår kartleggingen på en så omfattende skala at Datatilsynet omtaler det som en ren "innhøsting".[14]

At hundretalls av virksomheter vet svært mye om den enkelte av oss, uten at vi hverken vet hvem de er eller hva de vet, viser noe av problemet med digitaliseringen. Dette forholdet kan sammenlignes med temaet for 1970-tallets debatter om kontraktsfriheten, som førte til begrensninger i form av forbrukervern.

Det finnes gode grunner for å hevde at tilbydere av nettbaserte tjenester og programvare på tilsvarende måte burde begrenses i å stille uomgjengelige vilkår for bruk av sine tjenester, som tilgang til og rett til distribuering av brukerens personopplysninger.

Innstramming av regelverket er imidlertid ingen endelig løsning. Offentlige og private virksomheter har allerede et omfattende regelverk å forholde seg til, bl.a. ved personopplysningsloven som er tema for denne avhandlingen. Likevel er etterlevelsen for dårlig hos mange. Illustrerende er at fem offentlige organer i fjor ble ilagt overtredelsesgebyr, på grunn av alvorlige brudd på personopplysningslovens bestemmelser om internkontroll og informasjonssikkerhet.[15]

Også i privat sektor finnes problemer, bl.a. ved stadig økende lagring av personopplysninger uten at den registrerte er godt nok informert.[16] Dette er mest problematisk når det gjelder de mobile enhetene vi bærer med oss, som avgir trafikkdata og signaleringsdata mer eller mindre kontinuerlig gjennom døgnet. Som Datatilsynet påpeker er det ikke bare problematisk at disse opplysningene er uforholdsmessig omfattende i forhold til lovlige formål som kundeoversikt og fakturering – det er også svært utfordrende for personvernvernet at opplysningene typisk lagres i 1-3 måneder.[17] Situasjonen ser ikke bedre ut når en vet at bransjestandardene ofte henger etter den teknologiske utviklingen, og at disse personopplysningene i stor grad overføres via ukrypterte datalinjer.[18]

I tillegg til våre mobile enheter står vi i økende grad overfor et personvernsrettslig problem ved utbredelsen av såkalt "*smarte hjem*" og "*smarte bedriftslokaler*". Dette kan dreie seg om alt fra husalarmer, kjøleskap og strømmålere som er tilkoblet internett og servere hos

[14] Datatilsynet: *Det store datakappløpet*, op.cit., s. 5 og 41.
[15] Datatilsynet: *Årsmelding for 2015 – Hva rører seg på personvernfeltet?*, s. 36-37.
[16] For eksempel ble det i fjor kjent at BankID samlet inn biometri basert på hvordan bankkunder tastet sine passord under pålogging, uten at tilfredsstillende informasjon ble gitt, jf. Datatilsynets årsmelding 2015, op.cit., s. 47.
[17] Datatilsynets årsmelding 2015, op.cit., s. 46-47.
[18] Datatilsynets årsmelding 2015, op.cit., s. 46-47.

tjenesteleverandøren. Disse enhetene høster informasjon som kan overføres til andre aktører innenlands og utenlands, enten tilsiktet og informert eller ei. Disse utfordringene vil utvilsomt øke i omfang i årene fremover, blant annet ved utbredelsen av nettbaserte og "intelligente" tjenester og transportnettverk[19] i byer, også kalt "*smarte byer*"[20].

I tillegg til private og offentlige virksomheters innsamling og overvåkning er personvernet under press fra utøvende myndigheter. Politiets omfattende bruk av signaleringsdata fra mobiltrafikk som etterforskningsverktøy kan nevnes, all den tid dette bygger på et uavklart hjemmelsgrunnlag og ikke er lovregulert som særskilt tvangsmiddel.[21]

Gjennom de siste årene er det også avdekket enda mer alvorlige mangler på respekt for personvernet; det fremste eksempelet er Edward Joseph Snowdens avsløringer om europeiske og amerikanske myndigheters utstrakte etterretnings- og overvåkningsvirksomhet, og særlig amerikanske *National Security Agency* sitt uttalte mål om å kartlegge og samle inn *all* elektronisk kommunikasjon.[22]

Selv om avsløringer på samme skala ikke har kommet for Norges del, ville det være naivt å tro at personvernet ikke trues også av våre egne myndigheter. Det er i alle fall alt annet enn betryggende når Datatilsynet i fjor uttalte at "[*m*]*esteparten av sosial og individuell adferd, blir registrert og kontrollert.*"[23]

1.3 Rettskildebildet og dets særegenheter

I tillegg til personopplysningsloven fra år 2000, som kan anses som *lex generalis* hva gjelder anvendelse av personopplysninger, finnes det flere spesifikke regelsett. Her kan nevnes forvaltningslovens regler om taushetsplikt, helseregisterloven, pasientjournalloven, helsepersonelloven, ekomloven, reglene i straffeloven[24], politiregisterloven og øvrig rettspleielovgivning.

På sine områder er disse lovene *lex specialis* og går foran personopplysningsloven. For avhandlingens tema, som er overføring av personopplysninger til utlandet, er det likevel i all hovedsak personopplysningsloven som gjelder. Det redegjøres nærmere for

[19] Se lov om intelligente transportsystemer innenfor vegtransport m.m. (ITS-loven) 11. desember 2015.
[20] Se f.eks. <http://www.smartcities.info/>, innhentet 30.3.2016.
[21] NOU 2015:13, s. 118.
[22] Greenwald, Glenn: *Overvåket: Edward Snowden, NSA og overvåkningsstaten*, Cappelen Damm, Oslo 2014, s. 105-107.
[23] Datatilsynets årsmelding 2015, op.cit., s. 46-47.
[24] Se særlig strl. §§ 204 Innbrudd i datasystem, 205 Krenkelse av retten til privat kommunikasjon og 267 Krenkelse av privatlivets fred.

personopplysningsloven og den utfyllende personopplysningsforskriften (pof.) i neste underkapittel.

Personopplysningsloven bygger på EUs personverndirektiv[25] ("personverndirektivet") fra 1995, og en ser bl.a. at personopplysningslovens §§ 29 og 30 er ment å implementere direktivets art. 25 og 26.[26] Dette aktualiserer direktivet og relevant rettspraksis fra EU-domstolen, som rettskilder.

Av direktivets fortale nr. 3, 7, 8 og 10, samt art. 1, fremgår dets formål om å bygge ned hindringer for EUs frie marked og felles forvaltningstjenester gjennom regelharmonisering, i tillegg til dets idealistiske begrunnelse som bygger på synet om at personvern er en grunnleggende rettighet.[27]

Videre finnes en rekke andre internasjonale kilder på området. Dette er i hovedsak Europarådets konvensjon nr. 108 ("108-konvensjonen")[28], ulike rekommandasjoner[29] som bygger på denne, OECDs retningslinjer[30], FNs retningslinjer[31], EMK og FNs verdenserklæring om menneskerettigheter av 1948, og konvensjonen om sivile og politiske rettigheter ("SP") av 1966.

Noen av disse, som SP og EMK, er ratifisert eller inkorporert i norsk rett. Andre, som FNs retningslinjer, fungerer som viktige ikke-rettslige retningslinjer, med et langt bredere nedslagsfelt enn EUs direktiv. Disse vil ikke behandles særskilt i avhandlingen.

Det foreligger imidlertid en ny forordning som må omtales nærmere; *Europaparlamentets- og rådsforordning om beskyttelse av individer ved behandling av personopplysninger og om fri flyt av slike opplysninger* ("personvernforordningen").[32]

Personvernforordningen erstatter personverndirektivet, og vil innlemmes i EØS-avtalens vedlegg slik at Norge er forpliktet til å gjennomføre den. Personvernforordningen får ikke direkte virkning etter sin ordlyd for andre enn EU-landene, men skal etter EØS-avtalens art. 7 bokstav a "[*g*]*jøres til del av avtalepartenes interne rettsorden.*" Norge gjennomfører vanligvis forordninger i form av egne forskrifter, men med denne forordningen, som erstatter

[25] Europaparlamentets- og rådsforordning 95/46/EC 24.10.1995 (personverndirektivet).
[26] Ot.prp.nr.92, s. 125-126.
[27] NOU 1997:19, s. 38.
[28] Europarådets konvensjon 28.1.1981 nr. 108 (108-konvensjonen).
[29] Se f.eks. Europarådets rekommandasjon nr. R (87) 15 17.9.1987 (politirekommandasjonen).
[30] OECDs retningslinjer for personvern og utveksling av personopplysninger over landegrenser 1980.
[31] FNs resolusjon 45/95 14.12.1990.
[32] Europaparlamentets- og rådsforordning 2016/679 27.4.2016 (personvernforordningen).

rettsakten som vår personopplysningslov bygger på, vil det nok kreves omfattende lovendringer, primært i personopplysningsloven. Forordningen ble vedtatt og publisert 4. mai i år, og trer i kraft 25. mai 2018.[33]

Det nye med personvernforordningen er i svært korte trekk at den vil gjelde også for virksomheter utenfor EU som tilbyr varer og tjenester til eller overvåker EU-borgere, tydeligere vurderingsmomenter vedrørende anvendelse av personopplysninger til et nytt formål og nye rettigheter (bl.a. til å motsette seg profilering og automatiserte avgjørelser). I tillegg forflytter den en del av de nasjonale datatilsynenes ansvar over til den enkelte bedrift hva gjelder å vurdere personvernkonsekvenser, og den innfører pliktig personvernombud for visse offentlige og større private virksomheter.[34]

Som nevnt eksisterer det ikke mange dommer fra norsk rett angående personvernspørsmål. De mest sentrale norske dommene omtales nærmere nedenfor i kapittel 2. Fra EU-domstolen foreligger noen sentrale avgjørelser som kan omtales allerede her.

Den første er *Schrems*-dommen (C-362/14 6. oktober 2015), hvor den østerrikske jusstudenten Maximillian Schrems i etterdønningene av Snowden-avsløringene gikk til sak mot Facebook Ireland Ltd. for brudd på personverndirektivet, som følge av overføring av personopplysninger til USA i tråd med den såkalte *Safe Harbor*-avtalen[35].

Safe Harbor er navnet på EU-kommisjonens godkjennelse av USA som et trygt land å overføre til utenfor EU/EØS, så lenge mottakerbedriften i landet erklærer etterlevelse av visse rettslige prinsipper. Etter denne kunne personopplysninger overføres etter personverndirektivet art. 25. EU-kommisjonens beslutning hadde tilsvarende betydning for overførsel fra norske bedrifter, jf. pof. § 6-1, slik at vedkommende amerikanske virksomhet også ble ansett å "[*s*]*ikre en forsvarlig behandling*" etter pol. § 29 første ledd. Behovet for avtalen skyldes at USA ikke har lovfestede personopplysningsregler som antas å tilfredsstille kravene i art. 25 / § 29.[36]

EU-domstolen konkluderte i storkammer med at *Safe Harbor* var ugyldig på grunn av store sikkerhetshull i form av amerikanske myndigheters innsynsadgang, med den virkning at den massive overføringen av personopplysninger fra virksomheter i EU og EØS ikke lenger er lovlig.

---

[33] EU-kommisjonen: *Protection of personal data* <http://ec.europa.eu/justice/data-protection/>, innhentet 13.5.2016.
[34] Datatilsynet: *Hva blir nytt med forordningen?* <https://Datatilsynet.no/Regelverk/EUs-personvernreform/hva-blir-nytt-med-forordningen/>, innhentet 31.3.2016.
[35] EU-kommisjonen avgjørelse 20/520/EC 26.7.2000 (Safe Harbor-avtalen).
[36] Se videre på Datatilsynets nettsider: <https://www.Datatilsynet.no/Regelverk/Internasjonalt/Overfoering/Safe-Harbor-prinsippene/>, innhentet 13.5.2016.

I etterkant har det på høyeste politiske nivå vært jobbet for å få i stand en ny avtale hvor det tas høyde for de personvernsrettslige prinsippene EU-domstolen oppstilte i dommen. Den nye avtalen har samme formål som *Safe Harbor*, og har fått navnet *Privacy Shield*[37].

Avtalen ble presentert 29. februar i år, men etter uttalelse fra det sentrale europeiske rådgivningsorganet på området, Artikkel 29-arbeidsgruppen ("Working Party 29", forkortes "WP29")[38], ble det klart at avtalen anses som et betydelig, men ikke tilstrekkelig, skritt i riktig retning, bl.a. på grunn av fravær av vesentlige sikkerhetsmekanismer og uklart språk.[39] Dermed gjenstår bl.a. ny revisjon fra EU-kommisjonen, og det er uklart når avtalen vil tre i kraft.

I tillegg til *Schrems* viser avgjørelsene om retten til å bli glemt i *Google*-avgjørelsen (C-131/12 13.5.2014)[40] og annulleringen av datalagringsdirektivet[41] at EU-domstolen har posisjonert seg som vaktbikkje for personvernet.

Disse avgjørelsene er viktige i seg selv, og særlig er *Schrems* viktig også fordi EU-domstolens krav til ivaretakelsen av personvernet er blitt innarbeidet i den kommende personvernforordningen, og fordi alle fremtidige avtaler med land utenfor EU/EØS om overføring nå må tilfredsstille disse kravene om de skal overleve potensiell prøving hos EU-domstolen.[42]

Av avgjørelser fra andre land må *Microsoft*-kjennelsen (*Microsoft Corp. v. The United States*: S.D.N.Y. 25. april 2014, 13 Mag. 2814)[43] nevnes. Den kommer fra USA, som er et av landene som utøver desidert størst press på nordmenns personverninteresser, ved at det både innhenter og får overført svært store mengder personopplysninger fra Norge.[44]

I kjennelsen slås det fast at amerikanske myndigheter hadde rett til å beslaglegge innholdet i en Microsoft-kundes e-post, selv når informasjonen er lagret i et annet land, i kraft av at

---

[37] Privacy Shield (foreløpig tekst): <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf>, innhentet 30.5.2016.
[38] Gruppen er opprettet i tråd med personverndirektivets art. 29 som et uavhengig organ, bestående av representanter fra EU-landenes respektive datatilsynsorganer, representanter for de sentrale EU-organene og én representant fra EU-kommisjonen.
[39] WP29: *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, Brüssel 13.4.2016.
[40] Se videre under pkt. 2.3.
[41] EU-domstolens prejudisielle og forente avgjørelse i sakene C-293/12 og C-594/12 8.4.2014.
[42] Se videre Loidean, Nora Ni: *The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law*, Journal of Internet Law, vol. 19 no. 18, februar 2016 s. 1 og 8-14, på s. 12-13.
[43] Se videre under pkt. 2.4.
[44] Datatilsynet: *Det store datakappløpet*, op.cit., s. 41.

Microsoft er et amerikanskregistrert firma og at e-posten dermed var tilgjengelig fra deres amerikanske lokaler.

Kjennelsen er urovekkende idet den gir uttrykk for ensidig vekt på pragmatiske hensyn i favør statens innhenting av informasjon, lite øyensynlig uavhengighet hos dommeren og manglende vektlegging av personvernhensyn. Saken er imidlertid ikke avsluttet, og står for tiden under behandling hos *the United States Court of Appeals for the Second Circuit*.[45] I mellomtiden har Microsoft gått i gang med sine planer om å opprette datasenter i Tyskland for å unngå lignende problemstillinger, blant annet med tanke på sikkerhet vedrørende *skytjenester*, som blir stadig mer utbredt.[46]

"Skytjenester" er en samlebetegnelse på databehandling som via internett foregår på store, eksterne servere som kan være plassert hvor som helst i verden. Dette knytter seg i hovedsak til lagring av datafiler og til behandling av disse – f.eks. kan en lagre dokumenter, bilder og videoer på Microsofts skytjeneste OneDrive, og via Google Docs kan en opprette og behandle tekstfiler direkte på Googles servere.

Skytjenester kan anvendes av virksomheter og privatpersoner, og fordelene er i hovedsak at filene er tilgjengelig fra hvilken som helst datamaskin eller smarttelefon med internettilgang, og at behandlingen ikke beslaglegger lagringsplass eller nevneverdig prosessorkraft på egen maskin. Selv om det kreves et unikt brukernavn og passord for å få tilgang på filene, innebærer ekstern lagring på tilbyderselskapets server åpenbart at det fysiske hinderet for innsyn som ligger i lagring på egen harddisk er fjernet.[47]

Det sentrale norske tilsynsorganet er Datatilsynet, som blant annet skal behandle konsesjonssøknader, gi pålegg eller andre sanksjoner, overvåke og kontrollere virksomheter, drive opplysningsvirksomhet og avgjøre klager i første instans, jf. pol. § 42. Tilsynet skal også fungere som veileder for virksomheter som behandler personopplysninger.[48] Andre- og sisteinstans for klager er Personvernnemnda, jf. pol. § 43.

Med så mange ulike roller samlet hos Datatilsynet kan dette over tid medføre prioriteringsutfordringer. Det kan f.eks. se ut til at tilsynet har lagt uforholdsmessig stor vekt på tilsynsvirksomhet, uavhengig av om faktiske skadevirkninger faktisk foreligger, jf. PVN-2015-11, med den konsekvens at den preventive veiledningsplikten overfor enkeltvirksomheter og håndtering av klager er blitt begrenset.

Hva gjelder klagebehandlingen er det heller ikke uproblematisk at dette ansvaret er plassert hos Datatilsynet, øyensynlig uten at det er oppstilt noen absolutt inndeling i forhold til øvrige

[45] Microsoft Corp. v. The United States, 15 F. Supp. 3d 466, S.D.N.Y 2014.
[46] Moody, Glyn: *Microsoft building data centers in Germany that US government can't touch* <http://arstechnica.com/information-technology/2015/11/microsoft-is-building-data-centres-in-germany-that-the-us-government-cant-touch/>, innhentet 31.3.2016.
[47] Mer om skytjenester: <https://www.Datatilsynet.no/Teknologi/Skytjenester---Cloud-Computing/Hva-er-nettskytjenester/>, innhentet 30.5.2016.
[48] Ot.prp.nr.92, s. 75.

ansvarsområder, som opplysningsvirksomhet.[49] Dette kan påvirke rollen som klagebehandler i første instans, hvor tilsynets øvrige virksomhet står i fare for å virke inn på avgjørelsene.

Dette skaper en vesentlig institusjonell forskjell til andreinstans, som utelukkende driver med klagebehandling. Dette innebærer igjen risiko for redusert forutberegnelighet. Mellom "dømmende" instanser er identiske ansvarsområder å foretrekke, f.eks. slik som i det norske rettssystemet, som består av tre domstolsnivåer hvor samtlige instanser utelukkende behandler og avgjør enkeltsaker.

På nasjonalt nivå har vi også Sivilombudsmannen, som kan avgi uttalelser om forvaltningens praksis. Disse ikke er rettslig bindende for forvaltningen. Det er likevel en normalforventning om at disse etterleves, selv om praksis viser at anbefalingene ikke alltid tas til følge.[50] Sivilombudsmannen uttaler seg ikke ofte om personvernrettslige spørsmål.

På EU-nivå er det allerede nevnte WP29 det sentrale rådgivende organ. Dets mandat er å utrede spørsmål angående nasjonale tiltak som er gjennomført på bakgrunn av direktivet, og å gi rådgivende uttalelser til EU-kommisjonen om land utenfor EØS, endringer i direktivet og *codes of conduct* som er utviklet på EU-nivå, jf. personverndirektivet art. 30 nr. 1. Datatilsynet har bare rolle som observatør i WP29.[51]

Til tross for dette omfattende systemet av regler, tilsyns- og klageorganer, er den generelle kunnskapen om regelverket fortsatt dårlig, bl.a. ved virksomheters internkontroll og informasjonssikkerhet.[52] Dette viser at utviklingen på området har skjedd så raskt at ikke bare lovgiver sliter med å henge med; rettssubjektene og rettighetssubjektene har enda dårligere oversikt over sine plikter og rettigheter.

1.4 Nærmere om personopplysningsloven og -forskriften

I forhold til personregisterloven er personopplysningsloven en videreutvikling og oppdatering, med et langt bredere nedslagsfelt, flere rettigheter for den enkelte registrerte og betydelig redusert konsesjonsplikt, samtidig som vurderingsansvaret i større grad er plassert hos den enkelte virksomhet.

[49] Datatilsynets organisering: <https://Datatilsynet.no/Om-Datatilsynet/organisering/>, innhentet 31.3.2016.
[50] Se Sivilombudsmannens *dok. nr. 4:2 30. oktober 2015* til Stortinget, om at kommunal- og moderniseringsdepartementet ikke følger Sivilombudsmannens uttalelser.
[51] Se pkt. 2.2 om WP29-uttalelsers rettskildemessige vekt.
[52] Datatilsynets årsmelding 2015, op.cit., s. 59.

I tillegg ble Personvernnemnda opprettet som klageinstans over Datatilsynets vedtak. Dette har vist seg å være en viktig rettssikkerhetsgaranti, da det har omgjort Datatilsynets vedtak i nærmere 50 % av klagesakene.[53]

Formålet med personopplysningsloven er å gi beskyttelse til den registrerte, altså individet som personopplysningene kan knyttes til, jf. pol. § 2 nr. 6. Beskyttelsen består av vilkår for og krav til bruk av personopplysninger, bl.a. ved å fastslå at hensyn som kan begrunne behandling av personopplysninger skal veies opp mot personvernhensynet. Dette er utformet som en kombinasjon av plikter for de som tar personopplysninger i bruk og rettigheter for den registrerte.

Ettersom loven bygger på et direktiv, som for vår del er innført via EØS-avtalen, er det ikke full harmoni mellom de ulike landenes personopplysningslover. Sammenlignet med direktivet og andre europeiske lands lovgivning har personopplysningsloven blitt kritisert for å være for streng på noen punkter, også ved måten den praktiseres på. Dette gjelder bl.a. kriteriet om at personopplysninger bare kan anvendes til nye formål dersom de er forenlige med det opprinnelige formålet for innsamlingen.[54] Samtidig kan loven, i likhet med direktivet, kritiseres for mangel på tilstrekkelig klare vurderingsnormer.

Personopplysningslovens saklige virkeområde knytter seg til "*behandling av personopplysninger*", jf. pol. § 1 første ledd, i motsetning til personregisterloven som hovedsakelig knyttet seg til opprettelse og bruk av personregistre, jf. personregisterloven § 1. "Behandling" skal ifølge loven forstås som "[*e*]*nhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter*", jf. pol. § 2 nr. 2.

Loven kommer videre til anvendelse på all elektronisk behandling, alle former for kameraovervåkning og all annen behandling av personopplysninger som inngår eller skal inngå i et personregister, jf. pol. § 3 først ledd.[55] Med dette er loven gitt et vidt saklig virkeområde.

Den gjelder imidlertid ikke "[*b*]*ehandling av personopplysninger som den enkelte foretar for rent personlige eller andre private formål*", jf. pol. § 3 annet ledd. Lovens pliktsubjekter er

[53] I 2014 ble 11 av 26 behandlede saker omgjort av Personvernnemnda, jf. Personvernnemndas årsmelding, Oslo 19. februar 2015.
[54] Se Bjarne Kvams kritikk: <http://www.nrk.no/hordaland/_-personvernregler-er-for-strenge-1.11382370>, innhentet 1.4.2016.
[55] NOU 1997:19, s. 98.

altså virksomheter. Dette omfatter private og offentlige foretak, enten de har kommersielle, forvaltningsmessige eller andre formål, som behandler personopplysninger til annet enn "[*r*]*ent personlige eller andre private formål*".[56]

Av hensyn til ytringsfriheten er loven også betydelig begrenset når behandling skjer "*Utelukkende for kunstneriske, litterære eller journalistiske formål*", jf. pol. § 7.

For avhandlingen er det nyttig å se pliktsubjektene, virksomhetene, slik at de består av *behandlingsansvarlige* og *databehandlere*, som er lovens terminologi. Dette er henholdsvis den som bestemmer formålet og fremgangsmåten for den konkrete behandlingen av personopplysningene, og den som utfører den tekniske behandlingen på vegne av den behandlingsansvarlige, jf. pol. § 2 nr. 4 og 5.

Personopplysninger er i loven gitt en bred definisjon: "[*o*]*pplysninger og vurderinger som kan knyttes til en enkeltperson*", jf. pol. § 2 nr. 1. Det er utfordrende å foreta en nærmere konkretisering av personopplysningsbegrepet. Kort sagt dreier det seg om opplysninger som enten eksplisitt tilkjennegir eller gjør det mulig å finne ut av hvem personen som opplysningene knytter seg til er (den "registrerte", jf. pol. § 2 nr. 6). Her skal det tas høyde for alle hjelpemidler som det er rimelig å tro at noen kan komme til å bruke.[57] I forarbeidene eksemplifiseres dette med opplysninger som "[*b*]*ilde, personens stemme, fingeravtrykk eller genetiske kjennetegn*", uten at denne listen er uttømmende.[58]

Det kreves ikke at opplysningen, ved bruk av kurante hjelpemidler, vil gjøre det kjent for enhver hvem den registrerte er; det er tilstrekkelig at tilknytningen mellom opplysningen og den registrerte bare er kjent av et fåtall personer.[59]

Personopplysninger knytter seg i hovedsak til *fysiske* personer,[60] men opplysninger om juridiske personer som samtidig sier noe om fysiske personer omfattes også.[61] I tillegg er alle kredittopplysninger omfattet, også slike som knytter seg til juridiske personer, jf. pof. § 4-1.[62]

---

[56] Ot.prp.nr.92, s. 105.
[57] Personverndirektivet, op.cit., fortalen nr. 26.
[58] Ot.prp.nr.92, s. 101.
[59] Ot.prp.nr.92, s. 101.
[60] Se bl.a. den danske tittelen på Personverndirektivet: *Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger*.
[61] Schartum, Dag Wiese og Bygrave, Lee A.: *Personvern i informasjonssamfunnet*, 2. utgave, Fagbokforlaget, Bergen 2011, s. 117.
[62] Videre om personopplysningsbegrepet: Schartum og Bygrave, 2. utgave, op.cit., s. 117-135.

Loven begrenser seg geografisk til behandlingsansvarlige som er "[*e*]*tablert i Norge*", jf. pol. § 4 første ledd. Etableringskriteriet er i juridisk teori spaltet opp i tre sentrale kumulative kriterier om at det (1) krever utøvelse av aktivitet på norsk territorium, (2) gjennom en fast organisatorisk struktur og (3) over et ubestemt tidsrom.[63] Etableringskravet er klart nok oppfylt for utenlandske virksomheters datterselskaper eller filialer på norsk territorium, mens det på den andre siden ikke vil være oppfylt for en utenlandsk person på forretningsreise i Norge som behandler personopplysninger.[64]

For øvrig reiser direktivet, personopplysningsloven og den kommende forordningen uavklarte spørsmål hva gjelder jurisdiksjon. Det er bl.a. klart at overføring av personopplysninger til et annet land vil innebære tap av kontroll og sanksjonsmuligheter, hva gjelder innsynsretten til mottakerstatens myndigheter og beslagleggelse etter nasjonal lovgivning.[65] I tillegg vil sanksjonsmulighetene en kan ha overfor mottakeren, f.eks. på grunnlag av avtalebrudd,[66] hjelpe lite for den registrerte, dersom personopplysningene er videreført til et tredje land.[67]

Det er også et spørsmål om nasjonal lovgivning eller europeisk felleslovgivning kan håndheves overfor virksomheter i andre deler av verden, som baserer seg på personopplysninger og retter sin virksomhet mot personer som befinner seg i EØS-området. Nytt i den kommende personvernforordningen er at den eksplisitt pretenderer å gjelde også for slike virksomheter, jf. dens art. 3 nr. 2. Hvorvidt dette kan håndheves er usikkert.

I tillegg til personopplysningsloven har vi som nevnt personopplysningsforskriften som utfyller loven, bl.a. angående unntakene fra melde- og konsesjonsplikt. Forskriftens bestemmelser gis ikke generell behandling, men trekkes inn der de er relevante.

1.5 Struktur og mål

I avhandlingens første hoveddel, kapittel 2, gjennomgås personvernrettslige hensyn, verdier og interesser som har blitt vektlagt i teori, og i norsk og europeisk rettspraksis. Amerikansk rettspraksis og vedtak fra Personvernnemnda trekkes også inn.

I den andre hoveddelen, kapittel 3, redegjøres det for reglene for utenlandsoverføring i §§ 29 og 30, i et *de lege lata*-perspektiv.

---

[63] Schartum og Bygrave, 2. utgave, op.cit., s. 158; smh. personverndirektivets fortale nr. 19.
[64] Ot.prp.nr.92, s. 105.
[65] Dette var problemet i både Microsoft-kjennelsen og Schrems-dommen, jf. pkt. 1.3, 2.3 og 2.4.
[66] Jf. bruk av standardkontrakt i pkt. 3.3.3.3.
[67] Jf. pkt. 3.2.3 om 108-konvensjonen, som utløser en slik problemstilling.

Gjennomgangen i avhandlingens hoveddeler legger grunnlaget for å diskutere om personopplysningslovens regler for utenlandsoverføring ivaretar verdiene og interessene som gjør seg gjeldende, i et *de lege ferenda*-perspektiv i kapittel 4.

2 Personvernhensyn i et interesse- og verdiperspektiv

2.1 Innledning

Det fremgår av personopplysningslovens § 29 at personopplysninger bare kan overføres til stater som sikrer "*forsvarlig behandling*" av opplysningene. Dette kan selvsagt knyttes til tekniske forholdsregler og andre sikkerhetsmekanismer, men i utgangspunktet beror spørsmålet om hva som er "forsvarlig" på en avveining av brede, personvernrettslige hensyn, interesser og verdier.

Her er det typisk en fordel med lovgivers avklaring av hva som er relevante vurderingsmomenter. Men som det vil fremgå har avklaringer av personvernets nærmere innhold i stor grad blitt overlatt til teori og rettspraksis. Det må derfor foretas en redegjørelse for personvernrelevante hensyn, interesser og verdier, slik dette har fremgått i disse rettskildene.

2.2 Personvernsteori

Personvern har for det første vært forklart via tre innfallsvinkler: Det integritetsfokuserte, det maktfokuserte, og det beslutningsfokuserte personvernet.[68] Disse gjennomgås nedenfor. I tillegg finnes flere andre innfallsvinkler, med varierende grad av rettslig forankring.[69] Dette understreker personvernbegrepets kompleksitet.

Under *integritetsperspektivet* vektlegges enkeltindividets herredømme over egne personopplysninger, hvor herredømmets eksklusivitet varierer ut fra de enkelte livsområders ulike sensitivitetsgrader. En taler f.eks. om stedlig, kroppslig og psykisk integritet, kommunikasjonsintegritet og informasjonsintegritet. Det spesielle med den teknologiske utviklingen er at denne påvirker alle disse integritetsområdene, og "[*f*]*orstørrer og forverrer virkningene av integritetskrenkelsen*."[70]

---

[68] NOU 1997:19, s. 21-24; Ot.prp.nr.92, s. 19, og; Schartum og Bygrave, 2. utgave, op.cit., s. 27-36.
[69] Nærmere om ulike syn på personvernets rettslige karakter og forankring: Se Rasmussen, Ørnulf: *Kommunikasjonsrett og taushetsplikt i helsevesenet* (A.S. Borgund, Ålesund 1997) kap. 2.2.3.3 og 2.2.3.4. I boken konkluderes det med at en "systematisk relativisering" av personverninteressene er nødvendig i hvert enkelttilfelle, og at *interessemodellen* er best egnet til dette.
[70] Schartum og Bygrave, 2. utgave, op.cit., s. 28-31.

Under *beslutningsperspektivet* betraktes personopplysninger som beslutningsgrunnlag, gjerne i forvaltningens enkeltvedtak. Generelt kan det sies at "*Desto større betydning en avgjørelse har for den enkelte, desto viktigere kan de tilknyttede personvernspørsmålene være*".[71]

Til slutt betraktes personvern i lys av hvilken innvirkning personopplysninger har på *maktforholdet* mellom virksomheter/organer og enkeltindivid. Dette knytter seg bl.a. til enkeltindividets rettssikkerhet ved offentlige myndigheters maktbruk. Her kan det spørres om utbredelsen av ny teknologi og internett har gitt den enkelte bedre muligheter til å ivareta egne interesser overfor offentlige organer, eller om den stadig mer automatiserte saksbehandlingen har økt følelsen av avmakt blant borgerne.[72]

For det andre utformet Dag Blekeli og Knut S. Selmer personvernets *interessemodell* (også kjent som "interesseteorien") på 70-tallet,[73] som siden den tid har vært brukt som referansepunkt for mange nordiske personvernsdiskusjoner, blant annet i forarbeidene til personopplysningsloven.[74] Modellen har også vært grunnlag for videreutvikling over årene.[75]

I interessemodellen beskrives personvernet gjennom syv interesser, kategorisert som *individuelle* og *kollektive* interesser.

De individuelle, individbaserte, interessene er *innsyn*, *fullstendighet*, *diskresjon* og *privatlivets fred*. Dette knytter seg kort sagt til kunnskap om hvem som har hvilke opplysninger om deg, medbestemmelsesrett, formålsbestemthet, rettmessighet, opplysningskvalitet og at ens privatliv registreres i minst mulig grad.

De kollektive interessene er *borgervennlig forvaltning*, *robust samfunn* og *begrenset overvåkning*. Dette går ut på at forvaltningens automatisering ikke skal gå for langt, krav til nødvendighet og proporsjonalitet, krav til sikker informasjonsbehandling og at samfunnet er tjent med tillit mellom forvaltning og den enkelte. Med dette tar modellen høyde for individets behov for å kontrollere opplysninger om seg selv, og samfunnets interesse i opplysninger om dets medlemmer.[76]

[71] Schartum & Bygrave, 2. utgave, op.cit., s. 33.
[72] Schartum & Bygrave, 2. utgave, op.cit., s. 34.
[73] Blekeli, Dag Ragnar og Selmer, Knut S.: *Data og personvern*, Universitetet i Oslo 1977; se også Samuelsen, op.cit.
[74] Ot.prp.nr.92, s. 19, og; NOU 1997:19, s. 24-26.
[75] Schartum og Bygrave, 2. utgave, op.cit., s. 41-80, og; Rasmussen, op.cit., kap. 2.2.3.4.4.
[76] Johansen og Kaspersen, op.cit., s. 23-25.

Av internasjonale teorikilder finnes det mange. Jeg skal nøye meg med å vise til WP29s *Working Document* WP12[77], hvor det oppstilles seks *core principles* for utenlandsoverføring av personopplysninger.

For øvrig kan den rettskildemessige vekten av WP29s uttalelser diskuteres, da disse ikke kan tillegges autoritativ betydning. I lys av rettsområdets betydelige behov for utfyllende kilder, kan det trekkes frem at organet består av medlemmer fra EU-landenes respektive kontrollorganer ("datatilsyn"), at dets vurderinger er representative for EU-landenes spesialorganer på området, og er resultatet av diskusjoner som forutsetningsvis ligger på et høyt faglig og juridisk nivå. Dette tilsier at WP29s uttalelser tillegges en viss rettskildemessig vekt, også her til lands. Dette støttes av Personvernnemndas praksis, jf. PVN-2005-1.

Prinsippene fra WP12 kan ses som et vektig forslag til "minstekrav" for hva som skal anses å være "*adequate level of protection*" for overføring etter personverndirektivets art. 25 og 26,[78] som pol. §§ 29 og 30 bygger på.

I WP12 oppstilles på side 6 følgende grunnleggende prinsipper:

(1) the purpose limitation principle;
(2) the data quality and proportionality principle;
(3) the transparency principle;
(4) the security principle;
(5) the rights of access, rectification and opposition, og;
(6) restrictions on onward transfers.

De fem første prinsippene har åpenbare likhetstrekk til det som er gjennomgått av interessemodellen ovenfor. Det sjette og siste, om begrensning av mottakerlandets rett til videre overføring til andre land, knytter seg spesifikt til problematikken ved utenlandsoverføringer, og søker å begrense en av de største risikoene for tap av kontroll over personopplysninger som utenlandsoverføring innebærer.[79]

Til forskjell fra interessene som er oppstilt ovenfor, er WP12s prinsipper mer håndgripelige; de gir uttrykk for praktiske prinsipper som vurderingen av "*forsvarlig behandling*" kan bygges på, og kan ses som bindeleddet mellom de interessene og det endelige regelverket.

[77] EU-kommisjonen: *Working Party on the Protection of Individuals with regard to the Processing of Personal data*, DG XV D/5025/98 WP12, 24.7.1998 (WP12).
[78] Til tross for språklige nyanseforskjeller mellom "adequate level of protection" i personverndirektivets art. 25 og 26 og "forsvarlig behandling" i pol. §§ 29 og 30, knytter dette seg til de samme vurderingsmomenter, hvilket fremgår av bestemmelsenes øvrige ordlyd og at de norske bestemmelsene bygger på direktivets bestemmelser.
[79] Jf. den omtalte jurisdiksjonsproblematikken i pkt. 1.4.

2.3 Typeargumenter fra rettspraksis

Rettspraksis bidrar dessverre i liten grad til avklaring av personopplysningslovens ordlyd. Til gjengjeld gir avgjørelsene uttrykk for typeargumenter som tillegges vekt når personvernspørsmål må avgjøres, enten på lovfestet eller ulovfestet grunnlag.

At det eksisterer alminnelige, ulovfestede personvernregler fremgikk så tidlig som i Aars-dommen (Rt. 1896 s. 530). Dette fremgår også av dissensdommen To mistenkelige personer (Rt. 1952 s. 1217), som bygger på "[*d*]*et alminnelige rettsvern for personligheten*". Sistnevnte dom gir også uttrykk for at brede etiske, rettspolitiske, økonomiske og teknologiske hensyn er relevante vurderingsmomenter. Dette fremgår også av Datatilsynet og Personvernnemndas saker, se f.eks. PVN-2005-1 og PVN-2014-23.

Liv og helse kan også ha direkte tilknytning til personvern. I moderne samfunn knytter dette seg gjerne til individets rett til innsyn i andres opplysninger om en selv, som i Sykejournaldommen (Rt. 1977 s. 1035). I dommen knyttes dette også til opplysningenes fullstendighet og kvalitet, som fremholdes som særlig viktig når det gjelder sensitive opplysninger. På den andre siden påpekes det at taushetsplikt kan utgjøre en saklig begrensning av innsynsretten, i likhet med hensynet til ens egen helse eller forhold til nærstående, jf. pol. § 23 første ledd bokstav c, sml. forvaltningslovens § 19.

Et annet hensyn som kan begrense personvernet er rettssikkerhetsgarantier, som opplysning av straffesaker ved bevisførsel, jf. Fotobokskjennelsen (Rt. 1990 s. 1008) og Gatekjøkkenkjennelsen (Rt. 1991 s. 616). Dommene, som gikk i hver sin retning, viser at personvernet kan begrenses av hensynet til sakens opplysning, dersom man etter en objektiv og konkret vurdering kommer til at opplysningene ikke krenker tiltaltes integritet.

I likhet med Gatekjøkkenkjennelsen, kom en i Løgndetektorkjennelsen (Rt. 1996 s. 1114) til at den omdiskuterte opplysningen ikke kunne anvendes som bevis. Det fremgår av sistnevnte at potensielle integritetskrenkelser må tillegges tung vekt, uavhengig av tiltaltes konkrete ønsker i saken.

Dette beror gjerne på konkrete rimelighetsvurderinger av hvor nært en trår vedkommendes privatliv. Her legges det bl.a. vekt på om personopplysningene i hovedsak eller utelukkende knytter seg til vedkommendes arbeidsforhold. Som det fremgår av både E-postkjennelsen (Rt. 2002 s. 1500) og Avfallsservice-dommen (Rt. 2013 s. 143) vil slike opplysninger ofte anses å være uten verneverdig tilknytning til vedkommendes privatliv, i møte med andre tungtveiende interesser.

Av Avfallsservice-dommen ser en også at Høyesterett støtter seg til uttalelser i Personvernnemndas vedtak når det gjelder tolkning av personopplysningsloven.

Kommersielle hensyn og hensyn til samfunnets opplysning kan også begrense personvernhensynet. I en av de viktigste personvernavgjørelsene av nyere tid, *Google*-avgjørelsen, slås det likevel fast som den klare hovedregel at retten til privatliv veier tyngre enn selskapers økonomiske interesser i anvendelsen av personopplysninger og samfunnets interesse for enkeltpersoner.

Google-avgjørelsen (C-131/12 13. mai 2014) er en prejudisiell avgjørelse av spørsmål fra et privat søksmål mot Google i Spania, hvor saksøkeren krevde sletting av visse treff ved Google-søk på hans navn. EU-domstolen bekreftet at sletting kan kreves, og etablerte en "*rett til å glemmes*", basert på innsynretten og kravet til informasjonskvalitet, og retten til å motsette seg behandling av ens personopplysninger, jf. hhv. personverndirektivets art. 12 b og 14. Dommen bygger i hovedsak på prinsippet om rett til privatliv, jf. EMK art. 8, og har klare likhetstrekk med To mistenkelige personer-dommen, som omtaler "*glemselens slør*".

Vern mot myndigheters innsyn er også et anerkjent argument, som bl.a. ble tungt vektlagt i den nevnte *Schrems*-dommen[80]. Dette knytter seg i stor grad til integritetsperspektivet og beslutningsperspektivet som er omtalt ovenfor, og i avgjørelsen slås det fast at individers herredømme over egne personopplysninger skal tillegges betydelig vekt, også i møte med storsamfunnets behov; myndigheter skal bare ha rett til å skaffe seg tilgang eller anvende personopplysninger dersom det oppfyller strenge krav til formålsmessighet, nødvendighet og proporsjonalitet.

2.4 Oppsummering og forholdet til amerikansk rett

Av det gjennomgåtte ser en at retten til privatliv, informasjonskvalitet, innsyn og frihet fra integritetskrenkelser ofte blir tillagt avgjørende vekt i møte med motstående interesser.

Hvor motstående interesser, som rettssikkerhetsgarantien som ligger i fri bevisførsel, ivaretakelsen av lovbestemt taushetsplikt og arbeidsgivers innsyns- og styringsrett, har blitt tillagt avgjørende vekt, skjer dette først og fremst når det ikke er tungtveiende personvernhensyn på spill.

Av den nyere europeiske rettspraksisen ser en at personvernet vektes like tungt, om ikke tyngre. Her er det synlig forskjell på europeisk rettspraksis og rettspraksis hos et av de landene som mottar og innhenter flest personopplysninger fra Europa, nemlig USA.

[80] Se omtale under pkt. 1.3.

Blant annet gir *Microsoft*-kjennelsen[81] fra USA uttrykk for en mindre prinsipiell tilnærming til personvernet enn *Google*-avgjørelsen og *Schrems*-dommen. Dette gir bl.a. rom for tyngre vekting av nasjonale sikkerhetsinteresser, og kjennelsen viser en klar tendens til at det heller kreves begrunnelse for *ikke å overvåke*, i stedet for å kreve begrunnelse *for* overvåkning. Det finnes selvsagt amerikanske dommer i motsatt retning, f.eks. *Riley v. California* (573 S. Ct. 2014). Synet i Microsoft-kjennelsen synes likevel å være fremtredende, jf. bl.a. *r DoubleClick Inc. Privacy Litigation* (154 F. Supp. 2d 497, S.D.N.Y. 2001).

I *Riley v. California* ble det for første gang slått fast at politiet ikke kan gjennomsøke pågrepne personers mobiltelefon for elektronisk informasjon uten ransakelsesordre, selv om telefonen finnes under ransakelse av personen og kan beslaglegges. Dommen bygger på at gjennomsøk av telefonen uten ransakelsesordre ikke kan forsvares som et *warrantless search*, både fordi dette bare tar sikte på å avverge fysiske trusler mot politibetjenten som gjennomfører pågripelsen, og fordi moderne mobiltelefoner ofte inneholder betydelige mengder informasjon som dekkes av retten til privatliv.

I *r DoubleClick Inc. Privacy Litigation* slås det fast at selskapet *DoubleClick*s plassering av informasjonskapsler (*cookies*) på nettbrukeres harddisker når de besøkte samarbeidsselskapers nettsider ikke var ulovlig. Dommen bygger på samtykket som nettstedene, ikke nettbrukerne, hadde avgitt til *DoubleClick*s informasjonsinnhenting, og at det ikke kunne påvises tilstrekkelig høye økonomiske tap for nettbrukerne.

Det er også verdt å merke seg at USA har et personopplysningsbegrep som bare omfatter *direkte* identifiserende opplysninger, til forskjell fra i europeisk personvernlovgivning, som også omfatter *indirekte* identifiserende opplysninger. Dette innskrenker personvernets anvendelsesområde, og innebærer blant annet at IP-adresser ikke anses som en personopplysning i USA, i motsetning til i EØS-området.

3 Adgangen til overføring til utlandet

3.1 Innledning

Før det nærmere innholdet i §§ 29 og 30 undersøkes, er det viktig å kjenne til lovens grunnvilkår som gjelder for all form for behandling av personopplysninger.

Særlig viktig er §§ 8, 9, 11 og 13, som oppstiller generelle formål og vilkår som må være oppfylt for å kunne behandle personopplysninger. Først og fremst går dette ut på at behandling bare kan skje dersom det foreligger samtykke fra den opplysningene gjelder, er tillatt ved lov, eller er nødvendig for å ivareta bestemte formål, jf. § 8. I § 9 oppstilles ytterligere behandlingsvilkår for sensitive personopplysninger. I tillegg knesetter §§ 11 og 13 bl.a. vilkår angående formålsbestemthet, informasjonskvalitet og -sikkerhet. Enhver som vil

[81] Se omtale under pkt. 1.3.

overføre personopplysninger til utlandet må altså først vurdere om vilkårene i disse bestemmelsene er oppfylt, jf. Avfallsservice-dommen.[82]

I tillegg vil overføring ofte knytte seg til elektronisk behandling. Her slår § 31 første ledd bokstav a fast at den behandlingsansvarlige skal avgi melding til Datatilsynet, før virksomheten igangsetter elektronisk behandling for første gang.[83] Meldeplikten utgjør en viss praktisk terskel for den behandlingsansvarlige, og gir mulighet for Datatilsynets kontroll.

For behandling av sensitive personopplysninger, jf. pol. §§ 9 og § 2 nr. 8, utløses også konsesjonsplikten etter § 33, utenom for slike som er avgitt uoppfordret. Konsesjon gis av Datatilsynet, som også kan bestemme at dette ikke kreves, og at behandling av ikke-sensitive opplysninger krever konsesjon dersom behandlingen "[*å*]*penbart vil krenke tungtveiende personverninteresser*". Sistnevnte kompetanse er anvendt på behandling av personopplysninger i telesektoren, i forsikringsbransjen og ved banker og finansinstitusjoner, jf. personopplysningsforskriften §§ 7-1, 7-2 og 7-3.

3.2 Kravene i § 29

3.2.1 Innledning

I sin helhet lyder § 29 om *grunnleggende vilkår* som følger:

> *Personopplysninger kan bare overføres til stater som sikrer en forsvarlig behandling av opplysningene. Stater som har gjennomført direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, oppfyller kravet til forsvarlig behandling.*
>
> *I vurderingen av om behandlingen sikres på forsvarlig måte, skal det bl.a. legges vekt på opplysningenes art, den planlagte behandlingens formål og varighet samt de rettsregler, regler for god forretningsskikk og sikkerhetstiltak som gjelder i vedkommende stat. Det skal også legges vekt på om staten har tiltrådt Europarådets konvensjon 28. januar 1981 nr. 108 om personvern i forbindelse med elektronisk behandling av personopplysninger.*

Bestemmelsen tolkes med utgangspunkt i en naturlig forståelse av ordlyden, supplert med rettspraksis, forarbeider, juridisk teori og reelle hensyn. Som nevnt under pkt. 2.3 har også Personvernnemndas uttalelser rettskildemessig vekt. Ettersom personopplysningsloven

[82] Se også Ot.prp.nr.92, s. 126.
[83] Ot.prp.nr.92, s. 127.

implementerer et EU-direktiv er også dette, og tilhørende rettspraksis fra EU-domstolen, av betydning.[84]

Som det fremgår av ordlyden, er det sentrale vilkåret at mottakerstaten "[*s*]*ikrer en forsvarlig behandling av opplysningene*". Før det redegjøres for dette vil de øvrige begrepene i bestemmelsen gjennomgås. Dette gjelder "personopplysning", "behandling", "overføres", "stater som sikrer" og "fri utveksling".

Rettspraksis bidrar ikke i særlig grad til avklaring av begrepene i §§ 29 og 30, og heller ikke til lovens øvrige ordlyd; domstolene har, som vist i kapittel 2, hovedsakelig utviklet ulovfestet rett. Det vil også fremgå at personopplysningsloven, i tillegg til sin tidvis vage ordlyd, lider under manglende avklaringer i forarbeidene.

For begrepet "personopplysninger" vises det til lovens vide definisjon i § 2 nr. 1,[85] og det som allerede er sagt i pkt. 1.4 og 2.4. Generelt er det positivt for personvernet jo videre begrepet tolkes, samtidig som dette vil gå på bekostning av motstående hensyn.

Også for begrepet "behandling" vises det til lovens vide definisjon av begrepet i § 2 nr. 2 som omfatter "*enhver bruk av personopplysninger*",[86] og til det som er sagt i pkt. 1.4.

Uttrykket "*fri utveksling*" finnes i den norske tittelen på personverndirektivet, både i § 29 og i forarbeidene[87]. Begrepet må, i samsvar med personverndirektivets anvendelsesområde, antas å gjelde utveksling innad i EU og EØS-området, jf. personverndirektivets art. 1 nr. 2.[88]

Ordet *fri* er noe villedende. Det kan ikke være tale om ubegrenset utveksling;[89] f.eks. vil norske regler om taushetsplikt begrense muligheten for enhver utenlandsoverføring. For EU-rettsakter gjelder også en saklig avgrensning i form av "*de fire frihetene*" (fri flyt av varer, tjenester, arbeid og kapital), som f.eks. ikke berører påtalemyndighetens registre.[90] Det enkelte EØS-land står videre fritt til å stille krav til overføringsmåten, så lenge dette ikke avviker fra de krav som stilles til overføringer innenlands.[91]

[84] Se Europaparlamentets- og rådsdirektiv 2013/37/EU, 26. juni 2013 (EØS-avtalen), vedlegg XI nr. 5e., og; Ot.prp.nr.92, s. 15.
[85] NOU 1997:19, s. 52-53.
[86] Ot.prp.nr.92, s. 102.
[87] Ot.prp.nr.92 og NOU 1997:19.
[88] Ot.prp.nr.92, s. 14.
[89] NOU 1997:19, s. 100
[90] Dette er imidlertid særskilt regulert via *Eurojust*-samarbeidet.
[91] NOU 1997:19, s. 100.

3.2.1.1 Overføringsbegrepet

Begrepet "overføring" er av sentral betydning, da dette rettsvilkåret er en viktig markør for § 29s saklige virkeområde. Ordet er en oversettelse av direktivets "transfer", men som påpekt i *Lindqvist*-avgjørelsen (EU-domstolen sak nr. C-101/01 6.november 2003) er det ikke definert i direktivet.

Lindqvist-avgjørelsen omhandler en kirkemedarbeider i Sverige, Bodil Lindqvist, som hadde lastet opp personopplysninger om sine kollegaer på internett, som navn, adresse, stilling og (for én kollega) medisinske opplysninger. Det fastslås at det innebar "transfer" da Lindqvist delte internettsiden med server-leverandøren som skulle drifte siden. Dette var imidlertid ikke et brudd på direktivets bestemmelser, ettersom server-leverandøren lå innenfor EU-området, jf. art. 25. I *obiter dicta* ble det også gitt uttrykk for at "transfer" mellom server-leverandør og nettbrukere neppe er direktivstridig, hovedsakelig basert på de praktiske vanskeligheter det ville medføre i dagens samfunn.

Overføringsbegrepet er heller ikke definert i personopplysningsloven, og forarbeidene retter seg mer mot sammenhenger og formål enn begrepsavklaring.[92]

Forarbeidene slår imidlertid fast at overføring mellom to parter i Norge faller utenfor lovens begrep, selv hvor de optimaliserende trafikkfordelingsprotokollene som internettet bygger på gjør at opplysningene er innom utenlandske servere.[93] Språklig skulle derimot midlertidige overføringer være omfattet, f.eks. ved at en norsk person på forretningsreise i utlandet har med seg sin bærbare datamaskin, som inneholder personopplysninger.

Om dette skulle legges til grunn vil lovens anvendelsesområde utvides utover det som er hensiktsmessig ifht. hensynene loven skal ivareta, jf. pol. § 1 annet ledd. Forarbeidene tyder på at dette ikke har vært meningen, da begrepet "videregivelse" lenge ble brukt før loven var endelig utformet.[94] Rent språklig tar dette begrepet sikte på mer permanente forflytninger mellom personer. Uttrykket ble, før lovens endelige vedtak, byttet til "overføring" uten at det fremgår at den språklige begrensningen skulle falle bort. Dette kan skyldes at problemstillingen ble oversett, men formåls- og konsekvensbetraktninger taler som nevnt for å tolke "overføring" noe innskrenkende, som i *Lindqvist*-avgjørelsen.

Uavhengig av ordlydstolkningen kan det nevnes at det i dagens digitale samfunn som oftest vil være tale om forflytning av en *kopi* av opplysningen; mao. slik at avsender ikke taper fysisk rådighet. Personopplysningsloven synes ikke å avgrense mot dette. Overføring av slike

[92] Ot.prp.nr.92, s. 75-76.
[93] Ot.prp.nr.92, s. 126.
[94] NOU 1997:19.

duplikat kan for øvrig samtidig antas å innebære en fordobling av potensiell risiko vedrørende personopplysningene.

Overføringsbegrepet har i rettsteorien vært tolket på ulike måter, og det har særlig blitt satt på prøve av internettet, bl.a. ved den senere tids massive økning i bruk av skytjenester. Som nevnt slår *Lindqvist*-avgjørelsen fast at opplasting til internett ikke innebærer "transfer" i direktivets forstand. Via et noe annet resonnement fremgår dette også av personopplysningslovens forarbeider.[95]

Hverken i rettspraksis, teori eller andre rettskilder har det vært argumentert overbevisende for at denne avgrensningen kan forankres i mer autoritative kilder enn ønsket om å unngå de store, praktiske vanskelighetene motsatt løsning ville innebære. Behovet for lovgivers avklaring er derfor stort hva gjelder internettet. Overraskende nok avklarer heller ikke den kommende personvernforordningen *transfer*-begrepet.

Jon Bing tok til orde for å ta utgangspunkt i den behandlingsansvarliges instruksjonsmyndighet når det skal avgjøres om "overføring" foreligger; dersom behandlingen av personopplysningen skjer innenfor den behandlingsansvarliges rom for instruksjonsmyndighet skal det ikke sies å foreligge en overføring, heller ikke hvor mottaker befinner seg i et annet land.[96] Dette er bl.a. praktisk mtp. kostnadsnivå og *outsourcing*.

Bings definisjon synes å stemme med kravene som stilles i personopplysningsforskriften vedrørende standardkontrakter,[97] og later derfor til å gi uttrykk for gjeldende rett, i den grad denne er avklart.[98]

3.2.1.2 "Forsvarlig" behandling

For § 29s hovedvilkår om at mottakerstaten må "*sikre forsvarlig behandling*", gjenstår det å avklare hva som ligger i ordet "forsvarlig". Dette er ubetinget avhengig av kontekst, da dets innhold ikke kan avklares uten å spørre "*forsvarlig i forhold til hva?*".

Dette illustrerer at vilkåret er en rettslig standard. Denne lovgivningsteknikken har både fordeler og ulemper, og som det vil fremgå gjør slike seg gjeldende også for personopplysningslovens bestemmelse. Et sentralt aspekt ved rettslige standarder er at de

[95] Ot.prp.nr.92, s. 76.
[96] Bing, Jon: *Overføring av personopplysninger til utlandet – noen grunnleggende problemstillinger*, Lov og Rett, vol. 53, 3, s. 127-146, 2014.
[97] Se pkt. 3.3.3.3.
[98] Se kap. 4 for videre omtale av de problematiske sidene ved overføringsbegrepet.

burde være så klare som mulig, og at innholdet i standarden burde bygge på bruk av presiserende "understandarder".[99]

I forarbeidene fremgår det at forsvarlighetskravet tar sikte på at "[*o*]*verføringen av personopplysninger ikke må medføre noen vesentlig forringelse av det vernet som lovforslaget her skal sikre*."[100] Utover vurderingsnormen "*vesentlig forringelse*", som ikke er lovfestet, gir ikke dette særlig mye mer enn en henvisning til personopplysningslovens øvrige regler.

Spørsmålet må et stykke på vei kunne besvares med de grunnleggende personvernhensynene som er angitt i personopplysningslovens formålsbestemmelse § 1 annet ledd, som uttrykk for den relevante kontekst, eller "understandard". Formålsbestemmelsen nevner "[*b*]*ehovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger*", som en ikke uttømmende liste av personvernhensyn.

Dette er presiserende til en viss grad, men kan fortsatt hevdes å være så skjønnsmessig at interesseavveiningen står i fare for å bli uforholdsmessig påvirket av den enkelte rettsanvenderens personlige oppfatninger.

Samtidig fremgår det av § 29 første ledd at stater som har gjennomført personverndirektivet uten videre skal anses å sikre forsvarlig behandling. Her er det gitt et konkret vilkår, og dette bidrar i det minste til forutberegnelighet hva gjelder stater som har gjennomført direktivet.

Av bestemmelsens andre ledd fremgår en ikke uttømmende liste over momenter som kan anvendes "*I vurderingen av om behandlingen sikres på forsvarlig måte*" for stater som ikke har gjennomført direktivet, jf. lovsitatet ovenfor.[101]

Videre gir forarbeidene støtte for å trekke inn bredere, samfunnsmessige hensyn, da det står at det også bør vektlegges om det er "[*m*]*ulig å få kontrollert og overprøvd for domstolene om reglene overholdes*".[102] Å trekke inn slike momenter i helhetsvurderingen vil ofte kunne være sentralt for ivaretakelsen av personvernet, jf. de nevnte dommene *Aars* og *To mistenkelige personer*.

Bing angir forskjellige spesifikke og generelle momenter som kan vektlegges, som "[*d*]*en generelle informasjonssikkerheten, som tar hensyn til tekniske løsninger, stabilitet av de*

[99] For en nærmere gjennomgang av begrepets utvikling, innhold og utfordringer, se Nygaard, Nils: *Rettsgrunnlag og standpunkt*, 2. utgave, Universitetsforlaget, Bergen 2004, s. 390-393, med henvisninger til Knoph og Augdahl.
[100] Ot.prp.nr.92, s. 126.
[101] Ot.prp.nr.92, s. 126.
[102] Ot.prp.nr.92, s. 126.

valgte løsninger, personalforhold og organisasjonen rundt databehandlingen". Han mener at en også burde gå lenger, og vektlegge forhold som "[*m*]*anglende politisk stabilitet, risiko for angrep rettet mot systemet mv.*"[103] Disse vurderingsmomentene kan bidra til ytterligere avklaring av hva som etter loven kan anses å være "forsvarlig" behandling.

I lys av det gjennomgåtte, kan forsvarlighetsvilkåret tolkes slik at det normalt vil være innfridd dersom behandlingen bygger på nødvendighet, formålsbestemthet, tidsbegrensning, tekniske løsninger som gir lav risiko for urettmessig spredning av personopplysningene, et generelt akseptabelt trusselnivå i mottakersamfunnet og at terskelen heves dersom det er tale om sensitive opplysninger.

Slike vurderingsmomenter gjør det mulig å gjennomføre en forsvarlighetsvurdering som kan fremstå betryggende, selv om den langt på vei baseres på skjønn. En kommer likevel ikke utenom at lovteksten og de øvrige rettskildene ikke gir et særlig godt grunnlag for å oppstille mer konkrete vurderingsmomenter for forsvarlighetsvilkåret for land hvor personverndirektivet ikke er gjennomført.[104]

Samtidig er ikke loven fri for konkrete rettigheter og plikter: Den enkelte virksomhet plikter f.eks. å gjennomføre risikovurderinger før behandling tiltar, jf. pof. § 2-4. Dette går bl.a. ut på å klarlegge sannsynligheten for, og konsekvenser av, sikkerhetsbrudd. Av personopplysningsloven og personverndirektivet fremgår også rettigheter og plikter vedrørende opprettelse av kontrollorgan med ankemulighet og retten til innsyn, retting og sletting.[105]

En forsvarlighetsvurdering kunne tenkes å oppstille disse elementene som minimumskrav til lovgivningen i mottakerstaten. Dette ville hjulpet den enkelte rettsanvender og bidratt til å sikre lovens personvernhensyn. Men, som problematisert i *Schrems*-dommen, slår ikke direktivet fast at dette er rettigheter og plikter som *må* være på plass for at en mottakerstat skal kunne anses for å sikre forsvarlig behandling – og det samme må kunne sies for personopplysningsloven.

For å komme nærmere inn på forsvarlighetsvilkåret må en etter dette se til lovens typetilfeller.

[103] Bing: *Overføring av personopplysninger til utlandet*, op.cit., s. 145.
[104] Videre omtale i kapittel 4.
[105] Jf. Google-avgjørelsen.

3.2.2 Overføring til EØS-land

Som nevnt slår § 29 entydig fast at stater som har gjennomført direktivet "[*o*]*ppfyller kravet til forsvarlig behandling*", smh. personverndirektivets art. 1 nr. 2 og art. 25, jf. fortalens pkt. 53-60.[106]

Dette tilsier for det første at også stater utenfor EØS-området, som frivillig har valgt å gjennomføre direktivet, skal anses å sikre forsvarlig behandling etter § 29. For det andre tilsier det at en stat i EØS-området som ikke har gjennomført direktivet i tilstrekkelig grad, ikke uten videre anses å oppfylle kravet til forsvarlig behandling.[107]

Da det ikke eksisterer faktiske eksempler på disse to ytterpunktene er det likevel mest praktisk å trekke skillet mellom overføring til EØS-land og til andre land, som etter personverndirektivets terminologi omtales som "tredjeland".

Det er betimelig å stille spørsmål ved automatikken i at EØS-land uten videre anses å sikre forsvarlig behandling. På den ene siden er det nødvendig og effektiviserende med et likelydende regelverk for flere land, ettersom teknologien sjeldent er begrenset av fysiske landegrenser.[108]

På den andre siden stiller løsningen store krav til det nevnte regelverket, og generelt kan det sies å innebære risiko for personvernet til den enkelte registrerte at det ikke foretas en konkret vurdering av den enkelte mottaker (normalt virksomheter). Hos EØS-virksomheter vil det, på samme måte som i tredjeland, være varierende sikkerhetstiltak og bransjepraksis, som kan ha stor betydning for personvernet.

Forarbeidene tar ikke stilling til dette, utover å legge til grunn at direktivet "[*f*]*orutsetter* […] *et rammeverk som bør tilfredsstille kravet til forsvarlig personvernregulering*" og at "*det legges opp til* […] *et nært samarbeid*" mellom både EU- og EØS-landene hva gjelder de nasjonale reglene som gis i medhold av direktivet.[109]

Løsningen fører altså til nasjonale regelverk med større eller mindre forskjeller. Dette undergraver direktivets egen forutsetning om homogenitet, jf. dets art. 25 og fortalens pkt. 8, og gjør automatikken betenkelig. Her kan det likevel minnes om den kommende personvernforordningen, som vil demme opp for disse innvendingene. Behovet for en

[106] Jf. også ot.prp.nr.92, s. 126.
[107] NOU 1997:19, s. 152.
[108] NOU 1997:19, s. 38.
[109] Ot.prp.nr.92, s. 75.

oppdatering av reglene og at dette skjer via forordning, er imidlertid i seg selv innsigelser mot automatikken i direktivet.[110]

3.2.3 Overføring til tredjeland

Overføring til tredjeland avhenger av at mottakerstaten "[*s*]*ikrer en forsvarlig behandling av opplysningene*", jf. pol. § 29 første ledd. Vurderingsmomentene i annet ledd, som er omtalt ovenfor, skal legges til grunn i en konkret og helhetlig vurdering av det enkelte tredjeland, Jf. *Lindqvist*-avgjørelsens avsnitt 64.

Vurderingen foretas i første rekke av den enkelte behandlingsansvarlige. Datatilsynet vil likevel kunne bidra til avklaringen, da det bl.a. ved elektronisk behandling skal gis melding til Datatilsynet minst 30 dager i forveien, jf. pol. § 31. Dette gir Datatilsynet anledning til å uttale seg og veilede dersom det mener at overføringen vil være lovstridig, eller ilegge sanksjoner[111] i etterkant.

For den enkelte behandlingsansvarlige som skal foreta disse vurderingene ville det vært til stor hjelp dersom "forsvarlighetsterskelen" var enklere å klarlegge. Som vist ovenfor lar dette seg ikke gjøre ut fra bestemmelsene i personopplysningsloven, personverndirektivet eller tilhørende rettskilder.

En kan likevel spørre om det er mulig å oppstille en nedre terskel for den rettslige standarden, som i alle tilfeller må være oversteget for at mottakerstaten skal anses å sikre *forsvarlig behandling*. Dette er hovedtema i Schrems-dommen, som gir uttrykk for noen generelle retningslinjer om utenlandsoverføring etter personverndirektivet som etter EU-domstolens syn må overholdes.

WP29 har utledet fire sentrale prinsipper fra *Schrems*-dommen, som fremgår av arbeidsgruppens *Statement on the Consequences of the Schrems Judgement*:

> *A. Processing should be based on clear, precise and accessible rules: this means that anyone who is reasonably informed should be able to foresee what might happen with her/his data where they are transferred;*
>
> *B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated: a balance needs to be found between the objective for which the*

[110] Kuner, Christopher: *Reality and Illusion in EU Data Transfer Regulations Post Schrems*, Legal Studies Research Paper Series, University of Cambridge 2016, s. 30.
[111] Se pkt. 3.4 om personopplysningslovens sanksjoner.

data are collected and accessed (generally national security) and the rights of the individual;

C. An independent oversight mechanism should exist, that is both effective and impartial: this can either be a judge or another independent body, as long as it has sufficient ability to carry out the necessary checks;

D. Effective remedies need to be available to the individual: anyone should have the right to defend her/his rights before an independent body.[112]

Selv om dette i utgangspunktet knyttes til "*intelligence activities*", understreker WP29 på første side i uttalelsen at prinsippene burde respekteres "[*w*]*henever personal data are transferred*". Ved å være utledet fra *Schrems* er prinsippene vektige vurderingsmomenter som rettsanvendere har all grunn til å forholde seg til dersom en ikke vil komme i konflikt med EU-domstolens vurdering.

Med disse fire prinsippene er det gjort et forsøk på å fastslå visse minstekrav til en "*adequate level of protection*". Dette er et steg i retning av bedret forutberegnelighet, men i likhet med lovteksten er også disse prinsippene svært skjønnsmessige, hvilket utfordrer de registrertes rettsstilling.[113]

Videre er det relevant hva direktivet og personopplysningslovens øvrige regler sier om sikkerhetstiltak, når det skal vurderes hva som ligger i kravet om forsvarlig behandling av personopplysninger etter art. 25 og § 29, jf. *Schrems*-dommen.

For direktivet kan det vises til art. 17 nr. 1 om *security of processing*:

Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

---

[112] WP29: *Statement of the Article 29 Working Party on the Consequenes of the Schrems Judgement*, Brüssel, 3.2.2016, s. 1.
[113] Kuner, op.cit., s. 18.

I bestemmelsens første avsnitt kreves ikke bare "*appropriate measures*", men det slås også fast hva tiltakene mer konkret skal sikre. Dette gjør det lettere å etterleve regelverket. I tråd med den helhetlige vurderingen som skal foretas etter art. 25, jf. *Schrems*-dommen avsnitt 75, kan disse rettighetene trekkes inn under vurderingen av tredjeland.

Personopplysningslovens § 13 om *informasjonssikkerhet* er ment å gjennomføre art. 17 nr. 1.[114] Denne vil på tilsvarende måte være av relevans ved vurderingen av tredjeland etter § 29. Selv om forarbeidene gir anvisning på proporsjonale sikkerhetstiltak i forhold til de aktuelle truslene,[115] har konkretiseringen i art. 17 nr. 1 uteblitt i § 13s ordlyd; det kreves "*tilfredsstillende informasjonssikkerhet*", uten at de spesifikke formålene for sikkerhetstiltak nevnes.

Her er rettsanvenderen åpenbart ikke gitt samme hjelp i personopplysningsloven som i direktivet. Dette avhjelpes likevel til en viss grad av sikkerhetstiltakene som nevnes i pof. §§ 2-10 – 2-13.

For de nærmere vurderingsmomentene i § 29 annet ledd fremgår det ovenfor at disse i stor grad bygger på skjønn, og at dette svekker forutberegneligheten. Dette skjer både ved at det er vanskelig for rettsanvendere å vite hvilke nærmere krav til forsvarlighet som gjelder for overføring til tredjeland, og ved at de registrerte vil ha vanskelig for å finne ut hvilket vern de har mot at deres opplysninger overføres til utlandet.

Problemet skyldes en lovregulering tuftet på rettslige standarder, som i stor grad nøyer seg med å fastslå generelle prinsipper og henvise til øvrig lovgivning. Dette er kjent lovgivningsmetode, men svikter når det henviste regelverket ikke bidrar til ytterligere konkretisering.

Illustrerende er at tiltredelse av 108-konvensjonen[116] er skilt ut som eget vurderingsmoment i § 29 annet ledd. Konvensjonen gir imidlertid ikke andre konkrete rettigheter enn de som fremgår eller kan utledes av personverndirektivet, jf. dens art. 5 og 8. Og i likhet med direktivet ligger konvensjonen på prinsippnivå, bl.a. ved at en har nøyd seg med henvisninger til slikt som "*appropriate safeguards*" uten å utdype dette kravet, jf. konvensjonens art. 6. Den er dermed ikke presiserende i nevneverdig grad.

[114] Ot.prp.nr.92, s. 114.
[115] Ot.prp.nr.92, s. 114.
[116] Se pkt. 1.3.

I WP12 gis også en viktig påpekning om at 108-konvensjonen hverken forbyr eller begrenser adgangen til overføring av personopplysninger til land som ikke har tiltrådt konvensjonen. Av denne grunn risikeres det, ved vektleggelse av et tredjelands tiltredelse av 108-konvensjonen, at staten anvendes som en "mellomlanding" for personopplysningene, hvis endelige mottaker er et tredjeland som ikke ville bestått forsvarlighetsvurderingen.[117]

Om en på bakgrunn av helhetsvurderingen som skal foretas etter § 29 kommer til at forsvarlig behandling *ikke* sikres av vedkommende stat, er overføring av personopplysning i utgangspunktet ikke tillatt. Om overføringen likevel skal være lovlig må den oppfylle unntaksvilkårene i § 30.[118]

3.3 Overføring til tredjeland som ikke sikrer forsvarlig behandling – pol. § 30

3.3.1 Innledning

I pol. § 30 gjennomføres direktivets art. 26. Bestemmelsen oppstiller i likhet med denne unntak fra hovedregelen om at "*forsvarlig behandling*" kreves for å kunne overføre personopplysninger til et annet land.[119]

Til forskjell fra § 29 åpner noen av unntakene i § 30 for å vurdere den enkelte mottaker og overføring. I bestemmelsen skilles det videre mellom unntakene i bokstavene a-h i første ledd, og overføring etter særskilt godkjenning etter annet ledd.

3.3.2 Unntaksvilkårene i § 30 første ledd

Bestemmelsen i § 30 første ledd oppstiller flere unntak:

> *Personopplysninger kan også overføres til stater som ikke sikrer en forsvarlig behandling av opplysningene dersom*
>
> *a) den registrerte har samtykket i overføringen,*
>
> *b) det foreligger plikt til å overføre opplysningene etter folkerettslig avtale eller som følge av medlemskap i internasjonal organisasjon,*
>
> *c) overføringen er nødvendig for å oppfylle en avtale med den registrerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås,*

[117] Jf. WP12, op.cit., s. 8-9.
[118] Ot.prp.nr.92, s. 126.
[119] Ot.prp.nr.92, s. 126.

d) *overføringen er nødvendig for å inngå eller oppfylle en avtale med en tredjeperson i den registrertes interesse,*

e) *overføringen er nødvendig for å vareta den registrertes vitale interesser,*

f) *overføringen er nødvendig for å fastsette, gjøre gjeldende eller forsvare et rettskrav,*

g) *overføringen er nødvendig eller følger av lov for å beskytte en viktig samfunnsinteresse, eller*

h) *det er fastsatt i lov at det er adgang til å kreve opplysninger fra et offentlig register.*

Hverken i lovteksten eller i forarbeidene oppstilles generelle retningslinjer til disse unntaksbestemmelser. Imidlertid legger WP29 til grunn, som fremholdt av Datatilsynet, at "[*u*]*nntaksbestemmelsene i § 30 første ledd ikke anses for å gi tilstrekkelig overføringsgrunnlag annet enn i meget begrensede tilfeller*".[120] Dette trekker i retning av en streng ordlydstolkning av unntaksbestemmelsene, smh. formålsbestemmelsen i § 1 annet ledd.

Rent språklig gir noen av unntakene anvisning på relativt klare vurderinger, f.eks. bokstavene b og h. Utenom bokstav a, knytter imidlertid de andre unntakene seg til vurderinger av hva som er "nødvendig". Dette byr normalt på større utfordringer.

Av disse kan det sies at størst tolkningstvil er knyttet til bokstav g. Denne gjør unntak for "*viktige samfunnsinteresser*", og omfatter etter sin ordlyd ikke den registrertes hensyn, behov eller interesser, i motsetning til de andre nødvendighetsunntakene. Av denne grunn behandles bokstav g særskilt nærmere nedenfor.

Først drøftes likevel bokstav a, om samtykke som grunnlag for unntaksmessig overføring.

3.3.2.1 Samtykkevilkåret § 30 første ledd bokstav a

Med samtykkevilkåret gjennomføres direktivets art. 26 nr. 1 bokstav a.[121] Vilkåret reiser hovedsakelig spørsmål om hva som kreves av et samtykke.

[120] Datatilsynet: *Hvordan overføre personopplysninger til utlandet etter Safe Harbor*, 23.10.2015 <https://www.Datatilsynet.no/Regelverk/Internasjonalt/Hvordan-overfore-personopplysninger-til-utlandet-etter-Safe-Harbor/>, innhentet 11.4.2016.
[121] Ot.prp.nr.92, s. 126.

I følge personopplysningsloven § 2 nr. 7 må et samtykke være "[*e*]*n frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandlingen av opplysninger om seg selv*".

Dette innebærer ifølge forarbeidene krav om tilstrekkelig informasjon om opplysningenes innhold, formål og mottaker, slik at den registrerte kan vurdere fordeler og ulemper/risikoer før overføring skjer. Uttrykkelighetskravet innebærer at stilltiende eller passivt samtykke, eller samtykke bygget på konkludent atferd, ikke vil være tilstrekkelig.[122]

Det kan bemerkes at dette tilsier at personopplysningslovens samtykkebegrep er noe snevrere enn det legalitetsprinsippet etter loven har gitt rom for i offentlig rett, jf. bl.a. pasient- og brukerrettighetslovens kapittel 4 om helsehjelp til pasienter uten samtykkekompetanse som motsetter seg hjelpen.

Med frivillighet er det oppstilt krav om fravær av tvang.[123] Hvorvidt noe er frivillig kan imidlertid by på betydelig tvil, selv når det klart nok ikke er tvang etter alminnelig språkbruk. Dette kan f.eks. komme på spissen i arbeidsforhold. Her er det i juridisk teori tatt til orde for at arbeidstakers samtykke til behandling av egne personopplysninger ikke er tilstrekkelig, på grunn av arbeidsgivers makt i form av instruksjonsmyndigheten, og at samtykke derfor burde suppleres eller erstattes av nødvendighetsbegrunnelsene i pol. § 8.[124] Dette fremgår imidlertid ikke av lovteksten eller forarbeidene.[125]

Forholdet mellom samtykkevilkåret og nødvendighetsvilkårene i bokstavene c-e, som tar utgangspunkt i den registrerte, er også uklart og avklares ikke i bestemmelsens forarbeider. Vilkårene har imidlertid en klar parallell til personopplysningslovens § 8, som på tilsvarende måte oppstiller samtykkevilkår og nødvendighetsvilkår, uten at det innbyrdes forholdet mellom disse er avklart i lovteksten.

Til § 8 fremgår det imidlertid av forarbeidene at behandling "[*b*]*ør i størst mulig grad*" baseres på samtykke fra den registrerte, for å styrke dennes råderett over egne

[122] NOU 1997:19, s. 133.
[123] Ot.prp.nr.92, s. 103-104.
[124] Bing, Jon: *Samtykke til behandling av personopplysninger i arbeidsforhold*, FEST-2009-hj-45, Cappelen Akademisk Forlag 2009, s. 63.
[125] Sml. likevel pof. § 7-16 annet ledd angående sensitive personopplysninger.

opplysninger.[126] Dette kan tale for at samtykke skal ses som et hovedvilkår også etter § 30 første ledd – hvilket har støtte i Personvernnemnda i PVN-2004-1 og rettslig teori.[127]

3.3.2.2 Viktige samfunnsinteresser § 30 første ledd bokstav g

Unntaket gir adgang til overføring når det er "[*n*]*ødvendig eller følger av lov for å beskytte en viktig samfunnsinteresse*". I forarbeidene og i direktivets fortale nr. 58 eksemplifiseres dette med tilfeller hvor personopplysningsutveksling er nødvendig for skatte-, toll- eller trygdemyndigheter.[128]

Uttrykket "*viktig samfunnsinteresse*" er ikke nærmere definert, hverken i loven, forarbeidene eller direktivet, og er enda en rettslig standard. Det er uklart i hvilken grad det skiller seg fra "*allmenn interesse*" i § 8 bokstav d, "*samfunnets interesse*" i § 9 bokstav h og "[*r*]*ikets sikkerhet, landets forsvar eller forholdet til fremmede makter eller internasjonale organisasjoner*" i § 23 bokstav a. Retts- og nemndspraksis avgjør heller ikke spørsmålet, ei heller juridisk teori.

Rent språklig kan det legges til grunn at "*viktig samfunnsinteresse*" knytter seg til nasjonens territorielle integritet og borgernes fysiske sikkerhet, og andre kollektive interesser, som økonomisk og digital sikkerhet. Uttrykket er et eksempel på fordelen med rettslige standarder, som gjør at en kan ta høyde for samfunnsutviklingen.[129]

Unntaksvilkåret tillegger altså hensynet til samfunnsordenen betydelig vekt i møte med individets personvern, som en slags avveining av flertallets interesser mot enkeltindividets, sml. § 23 bokstav a om unntak fra retten til innsyn.

At flertallets interesser skal veie tungt mot enkeltindividets, er i utgangspunktet logisk. Men ikke sjelden vil det være vanskelig å skille mellom den enkeltes og fellesskapets interesser, og i slike regler ligger en stor del av myndighetenes muligheter til å krenke enkeltindividers rettigheter.

Her finnes et godt eksempel i *Schrems*-dommen. Der ble det bl.a. slått ned på *Safe Harbor*-avtalens vide unntaksbestemmelser knyttet til *national security*. Det finnes altså en rettslig grense for hvor tungt samfunnsinteresser kan vektlegges i forhold til enkeltindividets

[126] Ot.prp.nr. 92, s. 108.
[127] Schartum, Dag Wiese og Bygrave, Lee A.: *Personvern i informasjonssamfunnet*, 3. utgave, Fagbokforlaget, Bergen 2016, s. 201.
[128] Ot.prp.nr.92, s. 127.
[129] Jf. pkt. 3.2.1.2 ovenfor.

personvern. Grensen er i ytterste fall trukket ved de grunnleggende menneskerettighetene, jf. bl.a. EMK og SP.

Videre er det uklart *hvem* sine samfunnsinteresser som skal vurderes; avsenderstatens, mottakerstatens eller begges? Spørsmålet er hverken reist eller avklart i lovens forarbeider, i direktivet eller i retts- eller nemndspraksis.

Rent språklig finnes det ikke holdepunkter for å avgrense til avsenderstatens samfunnsinteresser. Ut fra et grunnleggende jurisdiksjonsperspektiv, er det likevel ikke unaturlig å legge til grunn at bestemmelsen sikter til avsenderstatens samfunnsinteresser. En potensiell løsning er å legge til grunn at bestemmelsen ikke tillater overføring hvor dette vil skade viktige samfunnsinteresser i Norge.

Dette byr uansett på utfordrende avveininger, og av hensyn til lovens plikt- og rettssubjekter burde lovgiver avklare også disse tvilsmomentene.

3.3.3 Unntaksvilkåret i § 30 annet ledd

3.3.3.1 Innledning

Unntaket i § 30 annet ledd lyder:

> *Datatilsynet kan tillate overføring selv om vilkårene i første ledd ikke er oppfylt dersom den behandlingsansvarlige gir tilstrekkelige garantier for vern av den registrertes rettigheter. Datatilsynet kan sette vilkår for overføringen.*

Datatilsynet er gitt denne kompetansen uavhengig av om vilkårene i første ledd er oppfylt eller ikke.[130] Rettsanvendere kan altså gå rett til annet ledd.

Vilkåret for overføring er at den behandlingsansvarlige "[*g*]*ir tilstrekkelige garantier for vern av den registrertes rettigheter*." Hva som ligger i "[*v*]*ern av den registrertes rettigheter*" er ikke klarlagt i forarbeidene. Lovens system og formål tilsier at uttrykket tilsvarer "*forsvarlig behandling*" i § 29.[131]

Forskjellen til de øvrige overførings- og unntaksvilkårene, ligger for det første i at den behandlingsansvarlige avsenderen må stille "*tilstrekkelig garantier*" for at vernet er ivaretatt. Uten rettskildemessige holdepunkter for annet, legges det til grunn en naturlig tolkning av ordlyden, som etter mitt syn tilsier at bestemmelsen stiller krav til forsikringer om at

[130] Ot.prp.nr.92, s. 127.
[131] Se pkt. 3.2 om begrepet.

behandlingen er forsvarlig etter avsenderstatens regler, både under overføringen og ved den senere behandlingen i tredjelandet.

Kravet om at garantiene må være "*tilstrekkelige*" er heller ikke avklart i rettskildene, men antas å knytte seg til sannsynlighetsgraden for at forsvarlig behandling gjennomføres. Hva som anses *tilstrekkelig* må nok bl.a. avhenge av hvilke rettslige forpliktelser som hviler på mottaker. Dette kan ta ulike former, som gjennomgås i de følgende underkapitlene.

Kravet om garantier retter seg ifølge ordlyden mot "*den behandlingsansvarlige*". Dette tilsier at ansvaret for den registrertes rettigheter ikke forflyttes til mottaker ved overføringen, selv om han er en selvstendig behandlingsansvarlig, sml. PVN-2014-23. Dette innebærer at avsender kan holdes ansvarlig for mottakers eventuelle overtredelser.[132]

På den andre siden vil overføring normalt innebære økt risiko for uintendert spredning.[133] Selv om avsender stadig er ansvarlig, vil ikke dét nødvendigvis avhjelpe de faktiske konsekvenser overføringen kan få. I tillegg kan det være vanskelig å få avdekket mottakerens overtredelser.

Datatilsynets tillatelse retter seg i utgangspunktet mot den enkelte overføring, og det kan stille "*vilkår for overføringen*". Vilkårene vil i praksis være tilpasset de konkrete forhold og relevante interesser, sml. pol. § 1 annet ledd og den ulovfestede vilkårslæren, jf. Rt. 2003 s. 764 avsnitt 61.

Ettersom det er snakk om store mengder personopplysninger som overføres mellom et stort antall aktører, er det praktisk med effektiviseringstiltak. Derfor er EU-kommisjonen bl.a. gitt kompetanse til å "forhåndsgodkjenne" tredjeland og utforme godkjente standardkontrakter, jf. personverndirektivet art. 25 nr. 6, jf. art. 31 nr. 2.

De alternative overføringsgrunnlagene er ikke nevnt i personopplysningsloven, men gjelder også for Norge, jf. pof. §§ 6-1 og 6-3. Disse overføringsgrunnlagene gjennomgås i det følgende.

3.3.3.2 Forhåndsgodkjente tredjeland

EU-kommisjonen kan forhåndsgodkjenne eller -avslå tredjeland som mottakere på generelt grunnlag, eller for visse typer opplysninger. Det ligger selvsagt til nasjonal skjønnskompetanse å avgjøre om det kan overføres til et tredjeland eller ikke, jf. pof. § 6-2,

[132] Om sanksjoner se pkt. 3.4.
[133] Jf. det som er sagt om jurisdiksjonsproblematikken ovenfor under pkt. 1.4.

og hvilken myndighet som skal avgjøre dette, men i praksis vil Kommisjonens avgjørelser følges også av EØS-landene som ikke er EU-medlemmer,[134] jf. pof. §§ 6-1 og 6-3.

For øvrig kan nok overføring til forhåndsgodkjente tredjeland foretas allerede etter hovedregelen art. 25 / § 29, ettersom Kommisjonen med sin forhåndsgodkjenning har slått fast at staten "*sikrer forsvarlig behandling*".

Pr. i dag er 12 tredjeland forhåndsgodkjent av Kommisjonen.[135] Dette gjelder bl.a. USA, som i motsetning til de 11 andre landene, kun har godkjennelse innenfor *Privacy Shield*-avtalens anvendelsesområde.

Listen oppdateres når Kommisjonen enten forhåndsgodkjenner flere tredjeland, eller finner at et godkjent tredjeland ikke lenger oppfyller kravene til en "*adequate level of protection*", jf. art. 25. Land fjernes også dersom EU-domstolen finner at en forhåndsgodkjenning er ugyldig, slik som ved *Safe Harbor*.

I grove trekk vurderer Kommisjonen landets rettssystem generelt, om menneskerettigheter respekteres og er implementert, og landets personvernlovgivning og relevant rettspraksis, fortrinnsvis gjennom en sammenligning med direktivet og de nevnte prinsippene fra WP12. I tillegg avgir WP29 en grundig vurdering og rådgivende forhåndsuttalelse, som normalt tillegges betydelig vekt. Dette publiseres sammen med Kommisjonens avgjørelse.[136]

3.3.3.3 Standardkontrakt

Behovet for effektivisering ble forutsett i arbeidet med personverndirektivet, og førte til at Kommisjonen også ble gitt kompetanse til å forhåndsgodkjenne "*certain standard contract clauses*", jf. direktivets art. 26 nr. 4.

Kommisjonen har utarbeidet tre kontrakter: To for overføring fra behandlingsansvarlig til annen behandlingsansvarlig,[137] og én for overføring fra *behandlingsansvarlig* til *databehandler*.[138] Overføring mellom behandlingsansvarlige skal likevel alltid godkjennes

---

[134] EØS-komiteens beslutning nr. 83/1999 25.6.1999, art. 2 pkt. 5e bokstav b.
[135] Tredjelandslisten med oversikt over godkjente tredjeland: <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm>, innhentet 20.5.2016.
[136] Tredjelandslisten, op.cit.
[137] Se <https://www.Datatilsynet.no/globalassets/global/04_skjema_maler/eus-standardkontrakter1_eng.pdf> og <https://www.Datatilsynet.no/globalassets/global/04_skjema_maler/eus-standardkontrakter2_eng.pdf>, innhentet 11.4.2016.
[138] Se <https://www.Datatilsynet.no/globalassets/global/04_skjema_maler/kontraktsvilkaar_overforing_eng.pdf>, innhentet 11.4.2016.

ved forhåndstillatelse fra Datatilsynet, mens overføring mellom *ansvarlig* til underordnet *behandler* bare krever varsling, jf. pof. § 6-3.

Standardkontraktene knesetter bl.a. sikkerhetstiltak hos avsender og mottaker. Faktisk tok Maximillian Schrems under sin sak til orde for at standardkontraktene var sikrere enn *Safe Harbor*, ettersom slike overføringer, i motsetning til overføring etter forhåndsgodkjenning av stater eller særskilte overføringavtaler, er "*under supervision by DPAs* [de nasjonale datatilsynene]"[139].

Imidlertid følger ikke dette av personopplysningslovverket i alle EØS-landene. De nasjonale datatilsynene har i utgangspunktet heller ikke håndhevingskompetanse utover statens grenser.[140] Dette er så betydelige innvendinger at Schrems' synspunkt har blitt omtalt som "*legal fiction*".[141]

Disse poengene fremholdes også i WP12, hvor det uttales at kontrakter i noen tilfeller uansett vil være utilstrekkelige instrumenter for å sikre forsvarlig behandling etter overføringen.[142] Det kan bl.a. være store ulikheter mellom ulike lands kontraktslovgivning, som forskjeller i reglene for lovvalg og for om tredjeparts rettigheter kan etableres på rettskraftig måte i avtale mellom to parter.[143]

3.3.3.4 Bindende konsernregler

Ved siden av godkjente kontrakter er det bare bindende konsernregler ("*Binding Corporate Rules*") som er anerkjent som tilstrekkelig overføringsgrunnlag til tredjeland som hverken sikrer forsvarlig behandling etter § 29 eller er forhåndsgodkjent av Kommisjonen.

Bindende konsernregler er ikke nevnt spesifikt hverken i personverndirektivet eller i personopplysningsloven, men har i praksis blitt akseptert som grunnlag for overføring når reglene gir tilstrekkelige garantier for den registrertes personvern. I den nye personvernforordningen er dette kodifisert i art. 47.

Bindende konsernregler er regelverk som virksomheter har pålagt seg selv og alle sine datterselskaper eller filialer, uavhengig global plassering. Et slikt enhetlig regelverk kan mer presist omtales som "*bindende konserninterne regler*", og må på samme måte som

[139] Kuner, op.cit., s. 27-28.
[140] Se pkt. 1.3 om jurisdiksjonsproblematikken.
[141] Kuner, op.cit., s. 27-28.
[142] WP12, op.cit., s. 21-23.
[143] WP12, op.cit., s. 18.

Kommisjonens standardkontrakter og forhåndsgodkjente land ivareta personvernet på en tilstrekkelig god måte for å få Kommisjonens godkjennelse, jf. personverndirektivet art. 25.

Den friere overføringen som oppnås med slik godkjennelse utgjør et betydelig effektiviseringstiltak for mange multinasjonale selskaper. Samtidig gjør de samme tungtveiende innvendingene som er anført mot standardkontraktene seg gjeldende, da konserninterne regler ikke står i posisjon til å begrense myndighetene i tredjeland, hva gjelder inngripende myndighetsutøvelse som overvåkning og beslag.[144]

3.4 Sanksjoner

Utgangspunktet for personopplysningslovens sanksjonsmuligheter er pålegg om opphør eller retting av ulovlig behandling, jf. § 46 og PVN-2015-11.[145] For tilfeller hvor pålegg ikke etterleves, oppstiller loven økonomiske og strafferettslige sanksjoner.

Den første av de økonomiske sanksjonene er overtredelsesgebyr inntil 10G, jf. pol. § 46. Det hører til Datatilsynets kompetanse å gi slike pålegg ut fra en skjønnsmessig vurdering, jf. den ikke uttømmende momentlisten i bestemmelsens annet ledd. Ettersom gebyr er en sanksjon av pønal karakter, kreves noe mer enn ordinær sannsynlighetsovervekt, jf. Rt. 2007 s. 1217.[146]

Den andre økonomiske sanksjonen er tvangsmulkt, jf. pol. § 47. Mulkten knyttes til fristen som Datatilsynet kan sette for bestemte pålegg det kan gi virksomheter, f.eks. tvungen bruk av fødselsnummer for å sikre personopplysningers kvalitet etter § 12 annet ledd.

Den tredje økonomiske sanksjonen er erstatningsansvaret, jf. pol. § 49. Dette er det klassiske erstatningsansvaret hvor skadevolder er ansvarlig for tap på skadelidtes side. Ansvarsgrunnlaget er imidlertid avgrenset til å gjelde skade som følger av at "[*p*]*ersonopplysninger er behandlet i strid med bestemmelser i eller i medhold av loven*". Som i personverndirektivets art. 23 nr. 1 gjelder erstatningsansvaret for enhver som blir skadelidende som følge av ulovlig behandling av personopplysninger – ikke bare den registrerte.[147]

Erstatningsansvaret i personopplysningsloven er spesielt, ved at det inntrer "[*m*]*ed mindre det godtgjøres at skaden ikke skyldes feil eller forsømmelse på den behandlingsansvarliges side*". Med dette er det oppstilt omvendt bevisbyrde, som gjør at ansvaret ligger hos den påståtte

[144] Kuner, op.cit., s. 26-27.
[145] Ot.prp.nr.92, s. 134.
[146] Ot.prp.nr.71, s. 12.
[147] Ot.prp.nr.92, s. 135.

skadevolderen for å fri seg fra anklagene,[148] som i personverndirektivets art. 23 nr. 2. Dette gjelder generelt for overtredelser av personopplysningslovens bestemmelser, ikke bare for §§ 29 og 30.

Bestemmelsen oppstiller i annet ledd også et rent objektivt erstatningsansvar for kredittopplysningsforetak som har meddelt uriktige eller åpenbart misvisende personopplysninger.[149]

Bestemmelsen om erstatning gir i tredje ledd adgang til å pålegge den behandlingsansvarlige oppreisningsansvar for skade av ikke-økonomisk art, etter en rimelighetsvurdering. Her er det bl.a. relevant hvilken berikelse den behandlingsansvarlige har oppnådd ved krenkelsen, hvilket kan være særlig praktisk når personopplysninger behandles for kommersielle formål,[150] som ofte ligger til grunn for utenlandsoverføring. Terskelen for oppreisning ligger noe høyere enn for det alminnelige erstatningsansvaret, jf. Avfallsservice-dommen.

Den siste sanksjonen er det alminnelige straffansvaret, som kan medføre bøter eller fengsel inntil ett år eller begge deler, eller fengsel inntil tre år ved særdeles skjerpende omstendigheter, jf. pol. § 48, jf. pof. § 10-3. Her er inngangsvilkåret at nærmere bestemte overtredelser i bestemmelsens første ledd bokstavene a-f er foretatt "*forsettlig eller grovt uaktsomt*".

Også for sanksjonsmulighetene gjør den nevnte jurisdiksjonsproblematikken som følger med utenlandsoverføring seg gjeldende.[151] Det er bl.a. uklart om også mottakerens lovstridige behandling av personopplysningene kan utløse sanksjonene, og hvorvidt manglende retting kan innebære sanksjoner mot den norske virksomheten som har overført opplysningene, herunder også i tilfeller hvor sistnevnte har opptrådt i samsvar med loven, f.eks. ved å ha gitt "*tilstrekkelige garantier*" etter § 30 annet ledd.[152]

Som nevnt under pkt. 2.3 om *Schrems*-dommen vil det, i vurderingen av tredjeland som mottakere av personopplysninger, være sentralt om mottakerstaten finnes å gi en tilsvarende "*level of protection*" som personverndirektivet. I dette henseende bidrar det til den registrertes

[148] Ot.prp.nr.92, s. 135.
[149] Ot.prp.nr.92, s. 135.
[150] Ot.prp.nr.92, s. 135.
[151] Se pkt. 1.4.
[152] Se pkt. 3.3.3.1

rettssikkerhet ved utenlandsoverføring at sanksjonsmulighetene er kodifisert i personverndirektivet.[153]

Både av denne grunn, og av hensynet til rettsanvenderne, er det fordelaktig at sanksjonene fremgår tydelig av nasjonal personopplysningslovgivning og at lovens øvrige bestemmelser bidrar til enkel etterlevelse. Som påpekt er ordlyden i personopplysningsloven tidvis vagt utformet. Dette gjør at det syndes en del mot regelverket.[154] Med det store antall virksomheter som i dag behandler personopplysninger, og herunder overfører slike til utlandet, er det liten grunn til å tro at mørketallene ikke er store.

Det kan se ut til at en på EU-nivå har innsett og tatt følgene av dette, både ved å forsøke å lage et tydeligere regelverk og ved å innføre strengere økonomiske sanksjoner. Etter den nye personvernforordningen har de nasjonale tilsynsorganene, ved brudd på sentrale bestemmelser i forordningen, som art. 8 om behandling av barns personopplysninger uten foreldrenes samtykke, kompetanse til å ilegge bøter på inntil 10 millioner euro eller 2 % av virksomhetens globale omsetning, hvor det høyeste av disse to beløpene skal legges til grunn, jf. personvernforordningen art. 83 nr. 4.

4 Rettspolitisk vurdering

Med den uoversiktlige risikoen som den tiltakende teknologiske utviklingen innebærer for personvernet, er det bedre å velge en "*føre var*"-fremgangsmåte, ved heller å regulere for mye enn for lite, inntil en har oversikt over potensielle konsekvenser. Dette fremgår også av den omtalte *Google*-avgjørelsen[155].

Her har personverndirektivet vist seg å bygge på et for snevert utgangspunkt når det gjelder overføring av personopplysninger – f.eks. reguleres ikke oppbygging av kundeprofiler hos bedrifter på bakgrunn av deres kunders valg og kjøp på internettet, det har lite fokus på overvåkning, og det passer dårlig på den stadige automatiseringen av tjenester. Det er heller ikke tilpasset utfordringen som ligger i at behandlingsansvarlige i tredjeland retter sin virksomhet mot EØS-borgere. Akkurat disse problemene rettes imidlertid opp med reglene i den nye personvernforordningen. Samtidig er det flere andre problematiske forhold i direktivet som ikke rettes opp ved forordningen.

[153] Se personverndirektivet, op.cit., kap. 3 om *Judicial remedies, liability and sanctions*.
[154] Se pkt. 1.2 og 1.4.
[155] Se pkt. 2.3.

Blant annet påpekes det ovenfor at direktivet i sin karakter er svært prinsipiell, og anvender en lite presiserende henvisningsteknikk og et tidvis vagt språk. Dette påvirker ikke bare forutberegneligheten og personvernet, men det kan også tenkes å være i strid med grunnleggende prinsipper for lovgivning; eksempelvis anførte Bodil Lindqvist at "[*t*]*he definition of 'processing of personal data wholly or partly by automatic means' does not fulfill the criteria of predicatbility and accuracy*", jf. avgjørelsens avsnitt 73. Dette understreker noen av de store utfordringene som ligger i å skulle lovgi for et livsområde som stadig er i hurtig utvikling og som er hevet over territorielle landegrenser.

I den norske gjennomføringen av personverndirektivet ved personopplysningsloven, ser en at en ikke har tatt konsekvensen av disse utfordringene på alvor, men i stor grad taklet problemene på samme måte som i direktivet. Blant annet ble det i forarbeidene reist en innvending om at direktivet oppstiller for lav terskel for overføring til utlandet.[156] På samme side fremgår det at innvendingen løses ved å se bort fra den, ut fra en betraktning om at ulike sikkerhetsnivåer vil innebære en åpenbar omgåelsesmulighet. Løsningen fremstår ikke som betryggende for lovens rettssubjekter.

Det samme kan bl.a. sies om at personopplysningsloven tilsynelatende ikke rammer overføringer av personopplysninger mellom en behandlingsansvarlig og hans underordnede databehandler, heller ikke hvor sistnevnte er plassert i utlandet.[157]

Om dette skal legges til grunn er det svært problematisk, da det som nevnt er klart at personopplysninger som overføres til et annet land samtidig underlegges en ny jurisdiksjon. Dette tapet av kontroll over egne personopplysninger var hovedbegrunnelsen for at *Safe Harbor* ble opphevet i *Schrems*-dommen.

Her kreves altså en bedre rettslig avklaring, og for nordmenns personvern ville det klart nok være mest fordelaktig om § 29s overføringsbegrep også omfattet overføring til underordnede databehandlere i utlandet.

Personvernnemnda har løst lignende problemstillinger ved å supplere lovtekst med ulovfestede personvernprinsipper, jf. PVN-2014-23 om pol. § 19, med videre henvisninger til tidligere vedtak. På denne måten kan lovgivningens mangler avhjelpes, men rettssikkerhets-

[156] NOU 1997:19, s. 102.
[157] Se pkt. 3.2.1.1.

og forutberegnelighetshensyn tilsier uansett at lovteksten gis bedre avklaring, særlig for saker som ikke havner på Datatilsynets eller Personvernnemndas bord.

På den andre siden er det visse positive rettspolitiske sider ved personverndirektivet, herunder dets bidrag til regelharmonisering. Som påpekt i Kommersialiseringsrapporten er internasjonalt samarbeid "[*a*]*vgjørende for å utvikle regler som virker i en global verden.*"[158] På personvernområdet gjelder ikke dette bare et felles regelverk, men også et utstrakt og effektivt samarbeid mellom de europeiske datatilsynene. Dette tar personvernforordningen høyde for, og omgjør WP29 til *European Data Protection Board*, jf. dens art. 68-71. Dette skal bl.a. styrke samkjøringen mellom de ulike nasjonale datatilsynene. Økt fellesskap kan imidlertid gi redusert handlingsrom for den enkelte, og det gjenstår å se hvilken effekt dette vil ha for de nasjonale datatilsynene.

Som omtalt, er en av Datatilsynets viktigste roller å motta og etterspørre informasjon om sikkerhetstiltak hos virksomheter som behandler personopplysninger, jf. pol. § 13. Her er det altså oppstilt et dokumentasjonskrav, som skal gjøre det mulig for Datatilsynet å fylle sin rolle som kontrollorgan, både for å vite om virksomhetene faktisk etterlever regelverket og om deres konkrete sikkerhetstiltak er tilstrekkelige. For personvernet er denne kontrollfunksjonen svært viktig. Da kreves det at Datatilsynet har tilstrekkelig kapasitet til å faktisk gjennomføre kontroller i et betryggende omfang. En organisasjon på rundt 40 ansatte, som i tillegg til kontrollfunksjon skal tjene opplysnings-, rådgivnings- og klagebehandlingsfunksjoner, synes å være utilstrekkelig.

Som tilsynsorgan avgir Datatilsynet også innspill i debatter og til lovforslag som berører personvernhensyn. Et av dets seneste innspill var i høringsuttalelse[159] til NOU 2015:13 *Digital Sårbarhet – sikkert samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden*. I utredningen gikk det Digitale Sårbarhetsutvalget *mot* å forby kryptering, som har stått på personvernagendaen de seneste årene. I sin høringsuttalelse gav Datatilsynet sin tilslutning til utvalgets standpunkt.

Spørsmålet om å forby kryptering eller ikke, viser at diskusjonen allerede er på avveie – personvernhensyn tilsier at kryptering burde påbys, i det minste for digitale offentlige

[158] Datatilsynet: *Det store datakappløpet*, op.cit., s. 42.
[159] Høringsuttalelse fra Datatilsynet, 15.3.2016: <https://Datatilsynet.no/globalassets/global/05_hoeringer/2016/horingsuttalelse-digital-sarbarhet.pdf>, innhentet 13.4.2016.

tjenester hvor personopplysninger samles inn og føres ut av landet. Da hadde man samtidig fått gjennomført en nyttig konkretisering av rettsområdets regelverk.

Det finnes flere måter å utbedre regelverket på, utover det personvernforordningen vil bidra med om to år. Blant annet kan det ses til tiltakene som har vært foreslått for å møte utfordringene angående kjøpsvilkår og forbrukervern på forbrukerkjøpsområdet. Det viser seg at mange av problemene på forbrukerkjøpsområdet har sine paralleller til personvernutfordringer. For eksempel kan *dårlig kvalitet på varer* og *høy pris* sies å tilsvare problemene med henholdsvis dårlig ivaretakelse av personvernet og innsamlingen av store mengder personopplysninger, som ofte er dårlig opplyst. Grovt sagt er problemet på begge områder *informasjonsasymmetri*, som økonomiprofessor Lars Sørgard har kalt det på forbrukerkjøpsområdet.[160]

I Sørgards avhandling presenteres løsningsforslag som lar seg låne til utfordringene en står overfor på personvernområdet. Dette går ut på konkurransepolitiske tiltak som innføring av erstatningsansvar, innføring av minstestandarder, informasjonsspredning om god og dårlig kvalitet på bestemte varer, utforming av standardkontrakter, pålegg om minstekrav til opplysninger før avtalebinding, og minstevilkår som må oppfylles for å kunne drive en virksomhet (utdanning, sertifisering, m.m.).[161]

På personvernområdet har en med personverndirektivet allerede gjennomført en del tiltak som tilsvarer noen av disse løsningsforslagene, som utforming av standardkontrakter, informasjons- og innsynskrav, og innføring av erstatningsansvar (som skjerpes vesentlig med den nye personvernforordningen). Samtidig gjenstår en del – det ville f.eks. være hensiktsmessig å innføre minstestandarder for sikkerhetstiltak (som nevnt kan bestemte former for kryptering være gode alternativ) og økt offentlig informasjonsspredning om store markedsaktørers gode eller dårlige ivaretakelse av personvernhensyn.

Andre mulige utbedringer av lovverket kan ligge i det som kalles *innebygd personvern*[162]: Ettersom lovverket i stor grad knytter seg til elektroniske verktøy kan etterlevelse sikres ved integrering i slikt som datamaskiner, smarttelefoner, programvare til slike enheter og nettlesere. For eksempel kan det stilles krav om sikker kryptering, tydelig mulighet til å velge

[160] Sørgard, Lars: *Informasjonsasymmetri og konkurransepolitikk*, Stortingsmelding nr. 15 (2004-2005): Om konkurransepolitikken, vedl. 1, s. 95-109.
[161] Sørgard, op.cit., pkt. 3.3.
[162] For en nærmere gjennomgang av begrepet og anvendelsesområder, se Schartum, Dag Wiese: *Automatisk virkende rettsregler – om pling-juss og systemrettssikkerhet i elektronisk forvaltning*, FEST-2013-emb-253.

bort sporingsmuligheter på internett og ved lokasjonsdata,[163] jevnlig opplysning om innsamling og personvernrettigheter, og aktive samtykker.

Slike praktiske løsninger kan, om ikke på lovsnivå, i alle fall gjennomføres i forskrifts form. Dette kan et stykke på vei avhjelpe problemet som ligger i at dagens lovgivning og øvrige rettskilder ikke synes å være tilstrekkelige for å løse de personvernsrettslige utfordringene som ligger i stadig økende bruk av avanserte elektroniske kommunikasjonsverktøy.[164]

I påvente av personvernforordningen ville det bidratt til økt personopplysningssikkerhet om både interesseorganisasjoner og sentrale bransjeaktører i større grad engasjerte seg som pådrivere for utvikling av minstestandarder hva gjelder sikkerhetstiltak og personvern. Dette kan gjøres gjennom såkalte *Best Practices Guidelines*, slik som den internasjonale handelsorganisasjonen *The Wireless Association* har gjort for både teleselskapsbransjen og programvareutviklere.[165]

Bransjeskapte minstestandarder har visse fordeler over lovtekst og forskrift, ved at de kan utformes og innføres raskere enn lovgivning, og at en står i bedre stilling til å omtale helt konkrete tiltak som de nevnt ovenfor. Dette kan også virke presiserende for personopplysningslovens rettslige standard i § 29.

På dette livsområdet er det likevel ikke sikkert at rettslige garantier eller bransjestandarder er tilstrekkelige, da det er svært lav terskel for å bevege seg på området, aktivitetskontrollen er og burde være lav av hensyn til tankefriheten, og hverken rettighets- eller pliktsubjektene forholder seg til geografiske grenser. I tillegg er det klart at de lovbaserte virkemidlene som hittil har vært brukt for å ivareta personvernhensynet, ikke innebærer et nevneverdig vern mot utenlandske myndigheters berettigede eller uberettigede innsyn i elektronisk lagrede personopplysninger.

Dette kan tyde på at det faktiske problemet ikke ligger i regelverket, men heller hos de som sitter ved makten. Hvordan en slik utfordring kan løses burde være gjenstand for en løpende, offentlig debatt på tvers av landegrenser, hvor grunnleggende menneskerettigheter respekteres og prioriteres over politiske agendaer.

---

[163] Whitten, Matthew: *Attacking Analogies: The need for Independent Standards for Mobile Privacy*, UCLA Journal of Law and Technology, vol. 19 utgivelse nr. 2, 2015, s. 26-29.
[164] Videre om denne problemstillingen i Johnson, David R. og Post, David: *Law and Borders – The Rise of Law in Cyberspace*, 48 Stanford Law Review 1367, 1995-1996.
[165] Whitten, op.cit., s. 13.

Litteraturliste

Norske lover og forskrifter

1814 Kongeriket Noregs Grunnlov (Grunnloven) 17. mai 1814

1902 Almindelig borgerlig Straffelov 22. mai 1902 nr. 10 (opphevet)

1967 Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) 10. februar 1967

1978 Lov om personregistre m.m. 9. juni 1978 nr. 48 (opphevet)

1992 Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområdet (EØS) m.v. (EØS-loven) 27. november 1992 nr. 109

1999 Lov om pasient- og brukerrettigheter (pasient- og brukerrettighetsloven) 2. juli 1999 nr. 63

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

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

2003 Lov om elektronisk kommunikasjon (ekomloven) 4. juli 2003 nr. 83

2005 Lov om straff (straffeloven) 20. mai 2005 nr. 28

2010 Lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) 28. mai 2010 nr. 16

2015 Lov om intelligente transportsystemer innenfor vegtransport m.m. (ITS-loven) 11. desember 2015 nr. 101

Internasjonale lover og avtaler

1950 Den europeiske menneskerettighetskonvensjonen (EMK) 4. november 1950

1948 FNs verdenserklæring om menneskerettigheter 10. desember 1948

1966 FNs internasjonale konvensjon om sivile og politiske rettigheter (SP) 16. desember 1966

1980 OECDs retningslinjer for beskyttelse av personopplysninger over landegrenser

1981 Europarådets konvensjon om personvern i forbindelse med elektronisk databehandling av personopplysninger (personvernkonvensjonen) 28. januar 1981 nr. 108

1987 Europarådets rekommandasjon 17. september 1987 nr. R (87) 15 om behandling av personopplysninger i politiet (politirekommandasjonen)

1990 FN-resolusjon 45/95: *Guidelines Concerning Computerized Personal Data Files* 14. desember 1990

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

2000 EU-kommisjonen 2000/520/EC: *Commission decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce* (Safe Harbor-avtalen)

2013 Direktiv 2013/37/EU: Europaparlamentets- og rådsdirektiv av 26. juni 2013 som endrer direktiv 2003/98/EF om viderebruk av den offentlige sektors informasjon (EØS-avtalens vedlegg XI)

2016 Forordning 2016/679: Europaparlamentets- og rådsforordning av 27. april 2016 om beskyttelse av individer ved behandling av personopplysninger og om fri flyt av slike opplysninger og om oppheving av direktiv 95/46/EF (personvernforordningen)

EU-kommisjonen: *Commission implementing decision of* [ikke vedtatt: ingen dato] *pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield,* <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf>, (Privacy Shield-avtalens foreløpige tekst, pr. 30. mai 2016)

Forarbeider

NOU 1997:19 *Et bedre personvern – forslag til lov om behandling av personopplysninger*

Ot.prp.nr.92 (1998-1999) *Om lov om behandling av personopplysninger (personopplysningsloven)*

Ot.prp.nr.71 (2007-2008) *Om lov om endringer i personopplysningsloven mv. (forskriftshjemmel, overtredelsesgebyr og innkreving av tvangsmulkt)*

NOU 2015:13 *Digital sårbarhet – sikkert samfunn: Beskytte enkeltmennesker og samfunn i en digitalisert verden*

Domsregister Høyesterett

Rt. 1896 s. 530 (Aars-dommen)

Rt. 1915 s. 32

Rt. 1952 s. 1217 (To mistenkelige personer-dommen)

Rt. 1977 s. 1035 (Sykejournaldommen)

Rt. 1990 s. 1008 (Fotobokskjennelsen)

Rt. 1991 s. 616 (Gatekjøkkenkjennelsen)

Rt. 1996 s. 1114 (Løgndetektorkjennelsen)

Rt. 2002 s. 1500 (E-postkjennelsen)

Rt. 2003 s. 764

Rt. 2007 s. 1217

Rt. 2013 s. 143 (Avfallsservice-dommen)

Domsregister EU-domstolen

Sak C-101/01, 6. november 2003 (Lindqvist- avgjørelsen)

Digital Rights Ireland Ltd. v Minister for Communications, Marine and natural Resources; Minister for Justice, Equality and Law Reform; Commissioner of the Garda Síochána; Ireland, The Attorney General; Irish Human Rights commission (intervener); Kärntner Landesregierung; Michael Seitlinger, and; Christof Tschohl and others, forente saker C-293/12 og C-594/12, 8. april 2014 (Datalagringsdirektivavgjørelsen)

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, sak 131/12, 13. mai 2014 (Google-avgjørelsen)

Maximillian Schrems v Data Protection Commissioner, sak C-362/14, 6. oktober 2015 (Schrems-dommen)

Domsregister amerikansk rett

re DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, U.S. District Court for the Southern District of New York, 28. mars 2001 (DoubleClick-dommen)

Microsoft Corp. v. The United States, 15 F. Supp. 3d 466, U.S. District Court for the Southern District of New York, 25. april 2014 (Microsoft-kjennelsen)

Riley v. California, 573 U.S. Supreme Court, 25. juni 2014

Avgjørelser fra personvernnemnda

PVN-2004-1

PVN-2005-1

PVN-2014-23

PVN-2015-11 (ikke publisert)

Andre beslutninger

EØS-komiteen: Beslutning nr. 83/1999 av 25. juni 1999 om endring av EØS-avtalens protokoll 37 og vedlegg XI (Telekommunikasjonstjenester)

Litteratur

Bing, Jon: *Personvern i faresonen*, Cappelen, Oslo 1991

Blekeli, Dag Ragnar og Selmer, Knut S.: *Data og personvern*, Universitetet i Oslo 1977

Greenwald, Glenn: *Overvåket: Edwards Snowden, NSA og overvåkningsstaten*, Cappelen Damm, Oslo 2014

Johansen, Michal Wiik; Kaspersen, Knut-Brede, og; Skullerud, Åste Marie Bergseng: *Personopplysningslovens kommentarutgave*, Universitetsforlaget, Oslo 2011

Kvam, Bjarne: *Politiets persondatarett: En studie av hjemmels- og formålskrav ved politiets utlevering av personopplysninger til utlandet*, Universitetet i Bergen 2013

Nygaard, Nils: *Rettsgrunnlag og standpunkt*, 2. utgave, Universitetsforlaget, Bergen 2004

Rasmussen, Ørnulf: *Kommunikasjonsrett og taushetsplikt i helsevesenet*, A.S. Borgund, Ålesund 1997

Samuelsen, Erik: *Statlige databanker og personlighetsvern: Rapport fra et forskningsprosjekt*, Universitetsforlaget, Oslo 1972

Schartum, Dag Wiese og Bygrave, Lee A.: *Personvern i informasjonssamfunnet – En innføring i vern av personopplysninger*, 2. utgave, Fagbokforlaget, Bergen 2011

Schartum, Dag Wiese og Bygrave, Lee A.: *Personvern i informasjonssamfunnet – En innføring i vern av personopplysninger*, 3. utgave, Fagbokforlaget, Bergen 2016

Artikler, uttalelser og meldinger

Bing, Jon: *Overføring av personopplysninger til utlandet – noen grunnleggende problemstillinger*, Lov og Rett, vol. 53, 3, s. 127-146, 2014

Bing, Jon: *Samtykke til behandling av personopplysninger i arbeidsforhold*, publisert i *Arbeid og rett: Festskrift til Henning Jakhellns 70-årsdag 2009*, s. 45-64, Cappelen Akademisk Forlag, Oslo 2009

Datatilsynet: *Det store datakappløpet – Rapport om hvordan kommersiell bruk av personopplysninger utfordrer personvernet*, november 2015, <https://www.datatilsynet.no/globalassets/global/04_planer_rapporter/kommersialisering-norsk-endelig.pdf> (Kommersialiseringsrapporten), innhentet 30. mai 2016

Datatilsynet: *Hva blir nytt med forordningen?*, 18. februar 2016, <https://datatilsynet.no/Regelverk/EUs-personvernreform/hva-blir-nytt-med-forordningen/>, innhentet 31. mars 2016

Datatilsynet: *Hvordan overføre personopplysninger til utlandet etter Safe Harbor*, 23. oktober 2015, <https://www.datatilsynet.no/Regelverk/Internasjonalt/Hvordan-overfore-personopplysninger-til-utlandet-etter-Safe-Harbor/>, innhentet 11. april 2016

Datatilsynet: *Høringsuttalelse – Digital sårbarhet – NOU 2015:13*, 15. mars 2016, <https://datatilsynet.no/globalassets/global/05_hoeringer/2016/horingsuttalelse-digital-sarbarhet.pdf>, innhentet 13. april 2016

Datatilsynet: *Organiseringa av datatilsynet*, < https://datatilsynet.no/Om-Datatilsynet/organisering/>, innhentet 31. mars 2016

Datatilsynet: *Safe Harbor – prinsipper om overføring av opplysninger til USA*, sist endret 16. oktober 2015, <https://www.datatilsynet.no/Regelverk/Internasjonalt/Overfoering/Safe-Harbor-prinsippene/>, innhentet 13. mai 2016

Datatilsynet: *Årsmelding for 2015 – Hva rører seg på personvernfeltet?* <https://www.datatilsynet.no/globalassets/global/04_planer_rapporter/aarsmelding/arsmeldingen_2015.pdf>, innhentet 30. mai 2016

EU-kommisjonen: *Protection of personal data*, <http://ec.europa.eu/justice/data-protection/>, innhentet 13. mai 2016

EU-kommisjonen: *Statement of the Article 29 Working Part on the Consequences of the Schrems Judgement*, Brüssel 3. februar 2016, <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf>, innhentet 30. mai 2016

EU-kommisjonen: *Why we need a Digital Single Market*, <http://ec.europa.eu/priorities/sites/beta-political/files/dsm-factsheet_en.pdf>, innhentet 6. april 2016

EU-kommisjonen: *Working Party on the Protection of Individuals with regard to the Processing of Personal Data*, DG XV D/5025/98 WP 12, 24. juli 1998 (WP12)

Federal Trade Commission: *Data Brokers: A Call for Transparency and Accountability*, Washington D.C., mai 2014, <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>, innhentet 30. mars 2016

Finansdepartementet: *Perspektivmeldingen 2013*, Stortingsmelding 12 (2012-2013)

Johnson, David R. og Post, David: *Law and Borders – The Rise of Law in Cyberspace*, 48 Stanford Law Review 1367, 1995-1996

Kuner, Christopher: *Reality and Illusion in EU Data Transfer Regulations Post Schrems*, Legal Studies Research Paper Series, University of Cambridge 2016

Loidean, Dr. Nora Ni: *The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law*, Journal of Internet Law, vol. 19 no. 8, 19. februar 2016

Lysne, Olav: *Lysneutvalget 2014-2015: Digitalt sårbarhetsutvalg*, <https://www.difi.no/sites/difino/files/olav_lysne.pdf >, innhentet 13. mai 2016

Moody, Glyn: *Microsoft building data centers in Germany that US government can't touch*, Ars Technica, 12. november 2015, <http://arstechnica.com/information-technology/2015/11/microsoft-is-building-data-centres-in-germany-that-the-us-government-cant-touch/>, innhentet 31. mars 2016

Oldeide, Adalheidur Audardottir: *Mener personvernregler er for strenge*, NRK 29. november 2013, <http://www.nrk.no/hordaland/_-personvernregler-er-for-strenge-1.11382370>, innhentet 1. april 2016

Personvernnemnda: *Årsmelding for 2014*, Oslo 19. februar 2015, <http://www.personvernnemnda.no/vedtak/2014_arsmeld.htm>, innhentet 7. april 2016

Ruyter, Knut W.: *Forskningsetikkens historie*, sist endret 18. mai 2015, <https://www.etikkom.no/fbib/introduksjon/systematiske-og-historiske-perspektiver/forskningsetikkens-historie/>, innhentet 16. mai 2016

Schartum, Dag Wiese: *Automatisk virkende rettsregler – om pling-juss og systemsikkerhet i elektronisk forvaltning*, publisert i *Forsker og formidler: Festskrift til Erik Magnus Boe*, s. 253-266, Universitetsforlaget, Oslo 2013

Sørgard, Lars: *Informasjonsasymmetri og konkurransepolitikk*, publisert i Stortingsmelding nr. 14 (2004-2005) *Om konkurransepolitikken*, s. 95-109

Sivilombudsmannen: *Særskilt melding – Kommunal- og moderniseringsdepartementet følger ikke Sivilombudsmannens uttalelser*, dokument nr. 4:2 2015-2016, 30. oktober 2015

Steel, Emily; Locke, Callum; Cadman, Emily, og; Freese, Ben: *How much is your personal data worth?*, Financial Times 12. juni 2013, <http://www.ft.com/intl/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html#axzz3lAaLdwax>, innhentet 30. mars 2016

Whitten, Matthew: *Attacking Analogies: The Need for Independent Standards for Mobile Privacy*, UCLA Journal of Law & Technology, vol. 19 utgivelse nr. 2, 2015

Working Party 29: *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, 16/EN WO 238, Brüssel 13. april 2016

Annet

EU-kommisjonens oversikt over godkjente tredjeland: <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm>, innhentet 20. mai 2016

EUs standardkontrakter for overføring mellom behandlingsansvarlige: <https://www.datatilsynet.no/globalassets/global/04_skjema_maler/eus-standardkontrakter1_eng.pdf> og <https://www.datatilsynet.no/globalassets/global/04_skjema_maler/eus-standardkontrakter2_eng.pdf>, innhentet 11. april 2016

EUs standardkontrakt for overføring fra behandlingsansvarlig til databehandler: <https://www.datatilsynet.no/globalassets/global/04_skjema_maler/kontraktsvilkaar_overforing_eng.pdf>, innhentet 11. april 2016