I hvilken grad sikrer Privacy Shield at europeiske personopplysninger lagret i USA er tilstrekkelig beskyttet fra overvåking utført av amerikanske myndigheter?

En komparativ analyse av amerikansk og europeisk personvernrett

Kandidatnummer: 69

Antall ord: 14 419

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10.desember 2018

Innholdsfortegnelse

1 Innledning

1.1 Tema og problemstilling

I 2016 vedtok EU-kommisjonen et nytt rammeverk som er ment å sikre vern av fysiske personer i forbindelse med behandling av personopplysninger lagret i USA. Avtalen har fått navnet The EU-U. S Privacy Shield, og er en avtale inngått mellom EU og amerikanske kommersielle selskaper. Det vern av personopplysninger som Privacy Shield-avtalen gir, skal sikre et personvernnivå som langt på vei er sammenfallende med det vernet opplysningene ville fått dersom de var lagret i EU/EØS. Rammeverket fremgår av Kommisjonens gjennomføringsbeslutning (EU) 2016/1250, og trådte i kraft 12. juli 2017.[1] Den godkjenner ikke USA som sådan som en trygg mottakerstat, men den innebærer at selskaper i USA, etter nærmere vilkår fastsatt i avtalen, vurderes å ha et tilfredsstillende vernenivå for personopplysninger i forhold til de krav som fulgte av dagjeldende personverndirektiv.[2] Personverndirektivet ble i mai 2018 erstattet av personvernforordningen. [3]

Privacy Shield er en anerkjennelse av at transatlantiske overføringer er helt nødvendig for forholdet mellom Europa og USA, og et utslag av at europeisk lovgivning krever at europeiske personopplysninger nyter et tilstrekkelig personvern også etter at opplysningene har forlatt europeisk jurisdiksjon. Avtalen har imidlertid vært gjenstand for kritikk om at den ikke i tilstrekkelig grad sikrer europeiske forbrukeres personvern. The European Data Protection Supervisor, Giovanni Buttarelli, uttalte i en pressemelding i mai 2016 at

> «Privacy Shield as it stands is not robust enough to withstand future legal scrutiny before the Court. Significant improvements are needed […]»[4]

[1] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 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 (notified under document **C(2016) 4176**) (Text with EEA relevance) (Videre: "Commission implementing decision")
[2] Europaparlaments- og rådsdirektiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (personverndirektivet)
[3] Europaparlaments – og rådsforordning (EU) 2016/679 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt oppheving av direktiv 95/46/EF (personvernforordningen)
[4] EDPS *«Privacy Shield: more robust and sustainable solution needed"* (2016)

Tema for oppgaven er om EU-kommisjonens beslutning i tilstrekkelig grad sikrer det vernet personopplysningene hadde hatt dersom de var lagret i EU/EØS, og problemstillingen er:

> I hvilken grad sikrer Privacy Shield at norske personopplysninger lagret i USA er tilstrekkelig beskyttet fra overvåking utført av amerikanske myndigheter?

Problemstillingen er et utslag av to fundamentalt ulike perspektiver i personverndebatten, med retten til å råde over egne personopplysninger på den ene siden, og ideen om at myndighetene bør få tilgang til flest mulige personopplysninger for å beskytte samfunnet og dets individer på den andre.[5]

1.2 Aktualitet

Digitale overvåkingsmetoder har vist seg å være et effektivt hjelpemiddel i kampen mot terror og bekjempelse av annen alvorlig kriminalitet. I lys av Snowden-avsløringene i 2013 er det imidlertid ikke tvilsomt at metodene kan bryte med flere grunnleggende menneskerettigheter, blant annet retten til privatliv. Særlig problematisk er det at de største kommersielle aktørene som Facebook, Google og Microsoft har europeiske forbrukere og holder til og lagrer dataene i USA – en stat hvis personvern i mange europeiske øyne gir forbrukerne et svakere vern enn de har etter europeisk lovgivning.

Overføring av personopplysninger fra EU/EØS til USA har i lang tid vært gjenstand for debatt. Tredjestatsproblematikken har kommet på spissen i blant annet Irland i en sak personvernaktivisten Maximillian Schrems har anlagt mot det irske datatilsynet (Data Protection Commissioner) i anledning dennes manglende inngripen mot Facebook Ireland. Den 9. mai 2018 ble saken henvist til en prejudisiell avgjørelse i EU-domstolen.[6] Saken ventes å bli behandlet i 2019.

Bakgrunnen for saken er at Facebook Ireland Ltd. er en del av Facebook-gruppen og datterselskap av Facebook Inc. som er etablert og har sine servere i California, USA. Personopplysningene til europeiske facebook-brukere lagres hos Facebook Ireland Ltd. Schrems søksmål går i all hovedsak ut på at Facebook Inc. gjennom denne selskapsmodellen får overført all data fra Facebook Ireland Ltd., og behandler disse personopplysningene under

[5] NOU 2015: 13 s. 28
[6] C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems

amerikansk lovgivning.[7] Det forventes at EU-domstolen blir nødt til å ta stilling til amerikansk overvåkingslovgivning for å vurdere om overføringen er gyldig. Dommen vil derfor – i alle fall indirekte – få betydning for gyldigheten av Privacy Shield.

1.3 Gjennomføring av EØS-relevante rettsakter i nasjonal rett

Norge er en EFTA-stat og har forpliktet seg til en rekke EU-rettsakter gjennom EØS-avtalen. EØS-avtalens hoveddel er gjennomført i norsk lov gjennom EØS-loven.[8] Det følger av EØS-avtalen artikkel 3 at avtalepartene skal treffe tiltak som er egnet til å oppfylle forpliktelsene etter avtalen, hvilket innebærer at EU-rettsakter som er EØS-relevante må gjennomføres i norsk rett.

Privacy Shield er en EU-rettsakt i form av en kommisjonsbeslutning. EØS-avtalen omtaler ikke særskilt hvordan beslutninger skal gjennomføres i nasjonal rett. På bakgrunn av EØS-avtalen artikkel 3 og lojalitetsprinsippet har Privacy Shield-beslutningen blitt vurdert EØS-relevant og ble innlemmet i EØS-avtalens vedlegg XI 7. juli 2017.[9] Dette innebærer at Privacy Shield er en del av EØS-retten, og overføringer av norske personopplysninger til USA kan skje til de selskapene som forplikter seg til avtalen.

Homogenitetsprinsippet innebærer at EØS-regelverk som er hentet fra EU-retten må fortolkes og anvendes slik at rettstilstanden blir den samme i EØS som i EU.[10] Prinsippet kommer til uttrykk gjennom EØS-avtalens fortale hvor det heter at

> «avtalepartenes formål […] er å nå frem til og opprettholde en lik fortolkning og anvendelse av denne avtale og de bestemmelser i Fellesskapets regelverk som i det vesentlige er gjengitt i denne avtale»[11]

[7] Ireland, High Court, 2016 4809 P Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems avsnitt 4 (Videre: "Schrems II")
[8] Lov 27.november 1992 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) (EØS-loven)
[9] EØS-KOMITEENS BESLUTNING nr. 144/2017 av 7.juli 2017 om endring av EØS-avtalens vedlegg XI (Elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunnstjenester)
[10] Fredriksen og Mathisen (2018) s. 50
[11] EØS-avtalens fortale, femtende betraktning

Homogenitetsprinsippet tilsier således at EUs vurdering av Privacy Shield vil få betydning for EFTA-staten Norge, og det skal ikke være noen forskjell på EU og EØS-retten på dette området.

I mai 2018 trådte personvernforordningen i kraft. Det følger av EØS-avtalen artikkel 7 bokstav a at en rettsakt som tilsvarer en forordning

> «skal som sådan gjøres til en del av avtalepartenes interne rettsorden»

I dette ligger at forordningen ikke bare skal gjennomføres ordrett og i sin helhet, men den må gjennomføres ved inkorporasjon. De strenge gjennomføringsforpliktelsene som følger av EØS-avtalen er ment å sikre at EU-retten og EØS-retten langt på vei er så sammenfallende som mulig. Personvernforordningen er i dag gjennomført i norsk lov gjennom inkorporasjon ved en henvisningsbestemmelse i personopplysningsloven § 1.[12] Den ble gjeldende norsk rett den 20. juli 2018.

1.4 EU/EØS-rettens forhold til EMK

Norge er folkerettslig forpliktet til Den europeiske menneskerettskonvensjon (EMK) og FNs konvensjon om sivile og politiske rettigheter (SP). EMK er inkorporert i norsk lov gjennom menneskerettsloven. [13] I 2007 innlemmet EUs medlemsstater en bestemmelse i Traktaten om den europeiske union (TEU) art 6 (2) som slår fast at EU som organisasjon skal tiltre EMK. Innlemmelsen av menneskerettigheter i EU-retten innebærer at menneskerettighetene gjøres til gjeldende rett i medlemsstatene i alle tilfeller hvor de gjennomfører EU-rett.

Det følger av EMK artikkel 8 (1) at

> «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse»

og av SP artikkel 17 (1) at

> «Ingen må utsettes for vilkårlige eller ulovlige inngrep i privat – eller familieliv, hjem eller korrespondanse, eller ulovlige inngrep på ære eller omdømme»

[12] Lov 15.juni 2018 om behandling av personopplysninger (personopplysningsloven)
[13] Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven)

Praksis fra de to konvensjonenes overvåkingsorganer viser at vurderingstemaene i EMK artikkel 8 og SP artikkel 17 er sammenfallende, og oppgaven vil derfor kun forholde seg til EMK artikkel 8.

Et sentralt spørsmål i denne sammenheng er hvordan forholdet mellom EU/EØS og EMK utspiller seg. EU-domstolen har tradisjonelt vært opptatt av å markere avstand til folkeretten, fordi EU-retten skal være mer forpliktende enn alminnelig folkerett. [14] På noen områder har imidlertid EU-retten latt seg inspirere av folkeretten. EU utviklet sine «egne» menneskerettigheter, nå kodifisert i EUs charter om grunnleggende rettigheter (EU-charteret), og det er ikke tvilsomt at en rekke bestemmelser i EU-charteret er hentet fra, eller i hvert fall klart inspirert av, EMK. Charteret inneholder to bestemmelser med særlig relevans for personvern og personopplysningsvern, herunder artikkel 7 og 8. Det heter i artikkel 7 at

> «Everyone has the right to respect for his or her private and family life, home and communications»,

og i artikkel 8 (1) at

> «Everyone has the right to the protection of personal data concerning him or her»

Spørsmålet er således hvilken betydning EMK skal ha for rettsanvendelsen og tolkingen av EU-charteret.

I tilfeller hvor EU-domstolen trekker inn bestemmelser fra charteret som er hentet fra EMK, synes det klart at EU/EØS-statenes forpliktelser til EMK må trekkes inn i vurderingen. Til illustrasjon refererer EU-domstolen i Digital Rights Ireland[15] til EMK flere steder i vurdereringen av hvorvidt oppbevaring av personopplysninger utgjør et proporsjonalt inngrep i retten til privatliv i charteret artikkel 7 og 8, og bruker denne henvisningen:

> «see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *S and Marper v United Kingdom*» [16]

Dette innebærer at der rettighetene i charteret og EMK er sammenfallende, kan EMK og medfølgende rettspraksis fra EMD utgjøre en sentral rettskilde for tolkingen av EU-retten.

[14] Sejersted (2011) s. 58
[15] Forente saker C-293/12 og C-594/12 Digital Rights Ireland and others v Ireland
[16] Digital Rights Ireland avsnitt 47 og 54

1.5 Metodiske utfordringer knyttet til forståelsen av amerikansk rett

Det er ikke mulig å vurdere om europeiske personvernrettigheter er ivaretatt under Privacy Shield uten å gjøre seg opp en mening om rettstilstanden i USA. Det er imidlertid en stor metodisk utfordring å vurdere hvor grundig en må gå til verks før man har et forsvarlig grunnlag for å vurdere hva fremmed rett går ut på. Oppgaven blir lite hensiktsmessig om det avgrenses mot forståelsen av amerikansk rett, og jeg vil derfor konkret måtte tolke og vurdere enkelte amerikanske bestemmelser som gir myndighetene adgang til overvåking av europeiske personopplysninger for å gjøre meg opp en best mulig underbygd oppfatning av om disse bestemmelsene er i tråd med EU-retten.

På grunn av prosessregler, forskjeller i juridisk metode og andre rettslige forhold kan to regler i ulike jurisdiksjoner som tilsynelatende virker like i praksis ha to forskjellige virkninger. Det er derfor tryggest at tolkingen av amerikansk rett baserer seg på juridisk sekundærlitteratur, herunder juridiske analyser og rapporter utarbeidet av kvalifiserte jurister, og selvstendige og upartiske organer og organisasjoner i EU og USA.

I USA er hovedregelen at lovgivningskompetansen ligger til den enkelte delstat. [17] En rekke personvernspørsmål er imidlertid regulert gjennom føderal lovgivning, og det er disse lovene oppgaven vil ta utgangspunkt i. Det finnes en lang rekke amerikanske overvåkingslover som gir seg utslag i lover, acts, forskjellige programmer, ordre og direktiver. Ulike etterretningsbyråer følger ulike lover avhengig av hvem som overvåkes og hvilke midler som benyttes i overvåkingen. På bakgrunn av Privacy Shield og det EU-kommisjonen har lagt til grunn i sin tilstrekkelighetsbeslutning, er det hensiktsmessig at oppgaven tar utgangspunkt i the Presidental Policy Directive 28[18] (PPD-28) og the Foreign Intelligence Surveillance Act 702 [19] (FISA 702).

[17] Lando (2009) s. 130
[18] Presidental Policy Directive 28, Signals Intelligence Activities (17.01.2014)
[19]Foreign Intelligence Surveillance Act: Section 702, 50 U.S.C. § 1881 a

1.6 Videre fremstilling

Oppgaven består av fem deler. I del II skal det redegjøres for det juridiske grunnlaget for overføring av personopplysninger fra EU/EØS til USA, og hva som ligger i at tredjestaten må kunne sikre et «tilstrekkelig beskyttelsesnivå». EU/EØS og USAs grunnleggende ulike tilnærming til personvern vil også problematiseres.

Oppgavens tredje del tar for seg en kjent problemstilling innen EU-retten; i hvilken grad må EU-statene avstå fra suverenitetsprinsippet i saker som gjelder nasjonal sikkerhet? Problemstillingen er relevant fordi overvåking som regel skjer i nasjonal sikkerhets interesse, og det er bestemmelser i både TEU, Privacy Shield og personvernforordningen som gir uttrykk for at EU-retten i slike saker ikke skal komme til anvendelse. Spørsmålet er dermed hvilken betydning disse nasjonale sikkerhets-unntakene skal få.

I del IV følger det en drøftelse av amerikansk overvåkingslovgivning, og målet med denne delen er å se om amerikansk overvåkingslovgivning lar seg forene med kravene til behandling av personopplysninger i EU-retten, som jo EU-kommisjonen mener det gjør. Dette er den mest utpregede komparative delen av oppgaven.

I oppgavens siste del vil det fremgå noen avsluttende bemerkninger og noen tanker om veien videre og Privacy Shields fremtid.

2 Overføring av personopplysninger fra Europa til USA

2.1 Hovedregler og utgangspunkt for overføring av personopplysninger til en tredjestat

Utgangspunktet er at overføring av personopplysninger til et tredjeland ikke er ansett som trygt. Dette kommer til uttrykk gjennom personvernforordningen artikkel 44 som er utformet som et forbud mot overføring til tredjestater, som bare oppheves dersom ett eller flere vilkår er til stede: [20]

> «Enhver overføring av personopplysninger som behandles […] etter overføring til en tredjestat […] skal bare finne sted dersom den behandlingsansvarlige og databehandleren […] oppfyller vilkårene i dette kapittelet»

Hensynet bak forbudet om overføring til en tredjestat er at det er nødvendig å stille krav til selve overføringen for å sikre at personopplysninger beskyttes også etter at de er sendt ut av EU/EØS, og på den måten forhindre at forordningen omgås gjennom å overføre opplysningene til en annen jurisdiksjon og at det felleseuropeiske beskyttelsesnivået undergraves.[21]

Selv om overføring til tredjestater i utgangspunktet ikke anses som trygt, følger det av fortalen at overføringer mellom stater i dag er uunngåelig for blant annet å kunne utvide internasjonal handel og internasjonalt samarbeid.[22] Forbudet mot overføring til en tredjestat lar seg derfor oppheve under flere omstendigheter. Det følger av personvernforordningen artikkel 45 nr.1 at overføring av personopplysninger til en tredjestat kan skje

> «[…] når Kommisjonen har fastslått at tredjestaten […] sikrer et tilstrekkelig beskyttelsesnivå»

Når en slik beslutning foreligger, kan det fritt overføres personopplysninger til mottakere i den aktuelle staten.[23] Det eksisterer en rekke slike kommisjonsbeslutninger som ble godkjent under

[20] Skullerud, Rønnevik, Skorstad og Pellerud (2018), Personvernforordningen (GDPR) Kommentarutgave, kommentar til art. 44
[21] Skullerud (2018) Kommentar til art. 44
[22] Personvernforordningens fortale pkt. 101
[23] Skullerud (2018) Kommentar til art. 45

det tidligere personverndirektivet, og det følger av forordningen artikkel 45 nr. 9 at disse beslutningene fortsatt skal gjelde under den nye forordningen.

2.2 Nærmere om Privacy Shield-rammeverket

Privacy Shield inneholder krav som legger retningslinjer og begrensninger for hvordan selskaper skal behandle europeiske personopplysninger. Kravene gir seg utslag i en rekke grunnleggende personvernprinsipper blant annet om opplysningsplikt, dataintegritet, formålsbegrensing, sikkerhet og innsyn.[24] Dokumentet er på 130 sider, og avtalens prinsipper og garantier fremgår av beslutningens fortale og i en rekke vedlegg. Artikkel 29-gruppen har i den anledning anbefalt Kommisjonen å gjøre avtalen mer forståelig for både Europa og USA.[25]

Privacy Shield er et overføringsgrunnlag som baserer seg på et selvsertifiseringssystem, og tanken er at selskaper som gjennomgår sertifiseringen etterfølger kravene i personvernforordningen. Kommersielle selskaper som mottar europeiske personopplysninger må registrere sin tilknytning til rammeverket ved det amerikanske handelsdepartementet. Det er også handelsdepartementet som har ansvar for å påse at selskapene lever opp til sine forpliktelser etter avtalen.[26] For at avtalen skal overholdes, kreves det at selskapene tilpasser sin interne behandling av opplysninger og sikrer at disse rutinene er i samsvar med avtalen.

Når det gjelder amerikanske myndigheters adgang til personopplysningene som er lagret hos amerikanske sertifiserte selskaper, vil overholdelse av Privacy Shield i stor grad avhenge av den amerikanske rettsordenen. Amerikanske selskaper er bundet av amerikansk overvåkingslovgivning som for dem har forrang over prinsippene i Privacy Shield. Til tross for at avtalen ble inngått på bakgrunn av en rekke forsikringer fra det amerikanske justisdepartementet om at overvåking skjer i tråd med prinsippene i Privacy Shield, og således EU-retten, er det – særlig på bakgrunn av Schrems II – grunn til å se nærmere på etterretningslovgivningen myndighetene er bundet av.

[24] Commission implementing decision avsnitt 19-29
[25] Artikkel 29-gruppen, *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, Adopted on 13 April 2016, WP 238, s. 2
[26] Datatilsynet (2018)

2.3 Spenninger mellom europeisk og amerikansk personvern

For å forstå bakgrunnen for hvorfor overføring av personopplysninger fra EU/EØS til USA er problematisk, er det påkrevd med et noe overordnet perspektiv på den europeiske og amerikanske tilnærmingen til begrepet «personvern».

«Personvern» er et særnorsk begrep. Det fremgår ikke av hverken EU-lovgivningen eller EMK, og heller ikke av rettspraksis fra domstolene. Selv om forordningen i Norge har fått navnet «personvernforordningen», er det mer nærliggende å omtale vernet av fysiske personer i forbindelse med behandling av personopplysninger som et person*opplysnings*vern (the right to data protection).[27] [28]

«Privatliv» har ikke blitt generelt definert i hverken EU-domstolen eller EMD. Begge domstolene synes imidlertid å legge til grunn at «privatliv» favner vidt, og ikke skal tolkes strengt. EU-domstolen har uttalt at retten til respekt for sitt privatliv etter EU-charteret artikkel 7 og 8

> «concerns any information relating to an identified or identifiable individual» [29]

Uttalelsen er sammenfallende med det som nå er definisjonen av personopplysninger i personvernforordningen artikkel 4 (1), og dermed også norsk rett. EMD har gjennom en rekke avgjørelser fremholdt at begrepet «privatliv» omfatter aspekter knyttet til personlig identitet og fysisk og moralsk integritet, og at EMK artikkel 8 har som formål

> «to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings» [30]

Bakgrunnen for at personvern nyter sterkt vern i Norge og EU, er ideen om at alle mennesker har et behov for en privat sfære der man kan være i fred fra innblanding fra utenforstående, både fra enkeltmennesker og myndigheter. Personvern bygger i tillegg på behovet for å ha kontroll over opplysninger om en selv. Personvern er i EU/EØS en grunnleggende forutsetning

[27] Skullerud (2018) s. 31
[28] Denne forståelsen er langt på vei sammenfallende med de nordiske landene; i Sverige blir kalt forordningen kalt «dataskyddsförordningen» og i Danmark «persondataforordningen»
[29] Forente saker C-92/09 og C-93/09 Volker und Markus Schecke and Eifert v Land Hessen and Bundesanstalt für Landwirtschaft und Ernährung avsnitt 52. Se også domstolens videre henvisning til EMD
[30] Forente saker 40660/08 og 60641/08 Von Hannover v Germany (No. 2) avsnitt 95

for en funksjonell rettstat og et velfungerende demokrati, og vilkårene for inngrep i denne rettigheten er derfor strenge.

Til tross for at USA er en funksjonell rettsstat og et velfungerende demokrati, er presumsjonen der en annen. Her er prinsippet at inngrep er tillatt med mindre det er forbudt. I USA er det heller ingen generell personvernlov, men sektorlovgivning – lovgivning som gjelder på enkelte områder, eksempelvis finanssektoren eller helsesektoren. En annen vesentlig forskjell er at personvern i den private sektoren i stor grad er definert som en forbrukerrettighet,[31] og ikke en menneskerettighet slik som i Norge og mange andre europeiske land.

I mangelen på en overordnet personvernlovgivning kommer den grunnleggende forskjellen mellom amerikansk og europeisk regulatoriske tilnærming til personvernet tydelig frem. US Supreme Court har imidlertid funnet at retten til «privacy», til tross for at det ikke fremgår uttrykkelig av grunnloven, implisitt fremgår av både første, tredje, fjerde og femte grunnlovstillegg. Retten til privatliv har blitt brukt i en rekke dommer som begrunnelse for beslutninger som særlig gjelder sivile rettigheter. Roe v Wade illustrerer dette.[32] Saken handlet i korte trekk om hvorvidt lover som kriminaliserte kvinners rett til å ta abort eller lover som innskrenket denne retten var lovlig, og retten fant at retten til privatliv omfatter kvinners beslutning om å ta abort.

Når det gjelder den lovfestede retten til privatliv, er amerikansk lovgivning normalt mindre vidtrekkende og restriktiv enn den europeiske. [33] Den amerikanske lovgivningen avstår for eksempel fra å pålegge restriksjoner på eksport av personopplysninger til utlandet. Til sammenligning har den europeiske personvernforordningen et helt kapittel om regler som kommer til anvendelse ved overføring av personopplysninger fra EU/EØS til en stat utenfor EU/EØS. Privacy Shield som sådan er også et godt eksempel på at EU ønsker å beskytte europeiske personopplysninger som overføres og eksporteres til USA. I tillegg er det i europeisk personvernlovgivning en rekke sentrale prinsipper som kommer til anvendelse ved behandling av personopplysninger. Det følger for eksempel av personvernforordningen artikkel 5 nr. 1 bokstav b at personopplysninger skal behandles for det formål de er innsamlet for (prinsippet

[31] Thon, Bjørn Erik, "*Personvern i USA – part one"* (2013)
[32] U.S Supreme Court, Jane Roe v Henry Wade 410 U.S 113
[33] Bygrave (2014) s. 110

om formålsbegrensning). Tilsvarende prinsipp om formålsbegrensning finnes ikke i den amerikanske personvernlovgivningen. [34]

Et tilfelle der ulikhetene mellom europeisk og amerikansk personvern kommer tydelig frem, er forståelsen av begrepet «behandling» av personopplysninger. Begrepet har sentral betydning både for vurderingen av om personvernforordningen skal komme til anvendelse og når ansvaret for behandlingen skal avklares.[35]

Det følger av personvernforordningen artikkel 4 nr. 2 at en «behandling» er enhver operasjon som gjøres med personopplysninger, som for eksempel innsamling, registrering, lagring og bruk. Behandlingsbegrepet er etter dette meget vidt, og skal ramme enhver befatning med personopplysninger. Forordningen tilsvarer i stor grad definisjonen av «behandling» i det tidligere personverndirektivet og den tidligere personopplysningsloven § 2 nr. 2. [36] Det er etter EU/EØS-retten derfor klart at det foreligger en behandling av personopplysning allerede på innsamlingsstadiet av opplysningene.

I USA er det forskjellige oppfatninger av personvern med hensyn til når data blir innsamlet. Det ene synspunktet er at en behandling oppstår når data blir innsamlet, uavhengig av hva som skjer med informasjonen i etterkant. [37] Dette tilsvarer den europeiske tilnærmingen. Det andre og ledende synspunktet er at en behandling kun for å avgjøre informasjonens relevans ikke krenker personvernet og heller dermed ikke kan anses som en behandling i utgangspunktet. For å hensiktsmessig og effektivt kunne innsamle enkelte typer etterretning, er det det siste synspunktet som har blitt lagt til grunn i amerikansk etterretning.[38] Dette medfører at EU/EØS-rett og amerikansk rett har to vidt forskjellige synspunkt på når en behandling anses å være startet. Dette kan være problematisk, særlig fordi enkelte amerikanske etterretningslover gir hjemmel til å innsamle enorme mengder data uten at disse er relevante for etterretningen.

---

[34] Bygrave (2014) s. 110

[35] Skullerud (2018) Kommentar til art. 4 nr. 2

[36] Lov 14.april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) [Opphevet]

[37] National Academies, *Committee on responding to section 5(D) of the Presidential Policy Directive 28: The feasibility of software to provide alternatives to bulk signals intelligence collection* (2015) pkt 2.2.1. Rapporten ble skrevet etter forespørsel fra the Office of the Director of National Intelligence (ODNI). National Academies er en uavhengig NGO som bistår en rekke amerikanske organer ved å lage rapporter, gjøre nærmere undersøkelser og tilby rådgivning, se http://national-academies.org/

[38] National Academies, *Committee on responding to section 5(D) of the Presidential Policy Directive 28: The feasibility of software to provide alternatives to bulk signals intelligence collection* (2015) pkt 2.2.1

2.4 Hva er en «overføring» av personopplysninger?

Det følger av personvernforordningen artikkel 44 første pkt. at enhver «overføring» av personopplysninger til en tredjestat bare skal finne sted dersom den behandlingsansvarlige eller databehandleren oppfyller vilkårene som følger av kapittel V. Det nevnes i denne forbindelse at Facebook Inc, for eksempel, opererer både som databehandler og behandlingsansvarlig – avhengig av omstendighetene – jf. forordningen artikkel 4 nr. 7 og 8. Etter ordlyden i artikkel 4 nr. 7 er behandlingsansvarlig den som treffer beslutninger med hensyn til formålet med behandlingen, og hvilke midler som skal benyttes.[39] Det er etter dette klart at Facebook i de aller fleste tilfeller er databehandler ettersom det er de som bestemmer formålene med behandlingen av forbrukernes personopplysninger.

Spørsmålet er således hva som menes med «overføring».

Begrepet er ikke definert i forordningen eller i rettspraksis. Til tross for at begrepet mangler avklaring, har EUs interne datatilsynsmyndighet, European Data Protection Supervisor (EDPS) i et prosjektnotat uttalt at overføringsbegrepet brukes om data som er

> «move[d] or allowed to move between different users» [40]

Enn så lenge er det denne definisjon som er mest nærliggende å forholde seg til, mens vi venter på en etterlengtet mer utførlig definisjon fra EU-domstolen.[41] Når Facebook Ireland overfører europeiske opplysninger til Facebook Inc., er det ikke tvilsomt at disse dataene blir Facebook Inc's eiendom, og de har også råderett over opplysningene i tråd med det som fremgår av forbrukeravtalen alle forbrukere må samtykke til ved registreringen. Det foreligger derfor en «overføring», og reglene i forordningen kapittel V kommer til anvendelse.

[39] Artikkel 29-gruppen, *Opinion 01/2010 on the concept of "controller" and "processor"* Adopted on 16 February 2010, WP 169 s. 21
[40] European Data Protection Supervisor (2014) s. 6
[41] European Data Protection Supervisor (2014) s. 6

2.5 «Tilstrekkelig beskyttelsesnivå»

Som nevnt under punkt 2.1 kan EU-kommisjonen treffe en beslutning om at en tredjestat sikrer et «tilstrekkelig beskyttelsesnivå», jf. personvernforordningen artikkel 45 nr. 1. Dette er således kjernen i Privacy Shield.

Spørsmålet er hva som ligger i kravet til «tilstrekkelig beskyttelsesnivå».

Begrepet er ikke definert i personvernforordningen, og innholdet er ikke avklart i annen lovgivning. EU-domstolen har imidlertid redegjort for at det ikke er slik at nivået av beskyttelse skal være identisk med beskyttelsen som følger av EU-lovgivning. Retten uttalte i Schrems at vilkåret skal forstås slik at det kreves

> « […] a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union […] »[42]

At beskyttelsesnivået skal være «essentially equivalent» innebærer at beskyttelsesnivået i det vesentlige må svare til det nivået som er sikret gjennom personvernforordningen. Tredjestatens vernenivå behøver altså ikke å være helt sammenfallende med det europeiske nivået.[43] Det er i dag fortsatt uklart hvor kvalitativt ulikt tredjestatens personvernregulering kan være før staten ikke oppfyller kravet, men det avgjørende må være at staten i sin helhet, en rekke omstendigheter tatt i betraktning, sikrer det nødvendige nivået av sikkerhet og dekker de sentrale elementene i europeisk personvernrett. Målet er ikke at tredjestaten skal speile den europeiske lovgivningen, men tredjestatens lovgivning må etablere «the core requirements» til den europeiske personvernlovgivningen. [44] Det er ikke tilstrekkelig at tredjestatens rettssystem og dens internasjonale forpliktelser på papiret sikrer et tilstrekkelig beskyttelsesnivå. Personvernet må være effektivt sikret i praksis. [45]

Det følger av forordningen artikkel 45 nr. 2 bokstav a, b og c en rekke omstendigheter som Kommisjonen må ta i betraktning i vurderingen av om en tredjestat sikrer et tilstrekkelig beskyttelsesnivå. I korte trekk dreier det seg om egenskaper ved den aktuelle staten som er relevante for vurderingen.[46] Det heter i bokstav a første pkt. at det skal tas hensyn til

[42] C-362/14 Schrems v Data Protection Commissioner avsnitt 73
[43] Skullerud (2018) Kommentar til art. 45 nr. 1
[44] Artikkel 29-gruppen, *Adequacy Referential,* Adopted on 6 February 2018, WP 245 s. 3
[45] Schrems avsnitt 74
[46] Skullerud (2018) Kommentar til art. 45 nr. 2

> «prinsippet om rettsstaten, respekt for menneskerettighetene og grunnleggende friheter [og] relevant lovgivning»

Bestemmelsen henviser her til rettsstatsprinsippet og menneskerettighetene og de grunnleggende friheter.[47] I den sammenheng er det naturlig å trekke en linje til menneskerettskonvensjonen og EU-charteret. I samsvar med de grunnleggende verdiene som unionsretten bygger på, burde det i tilstrekkelighetsvurderingen tas hensyn til hvordan tredjestaten overholder rettsstatsprinsippet, sikrer klageadgang og domstolsprøving, overholder internasjonale menneskerettighetsstandarder og tredjestatens lovgivning om offentlig sikkerhet, forsvar og nasjonal sikkerhet.[48]

[47] Skullerud (2018) Kommentar til art. 45 nr. 2
[48] Fortalen pkt. 104

3 Behandling av personopplysninger når behandlingen skyldes «national security»

3.1 Betydningen av nasjonale sikkerhets-unntak

Facebook Inc anfører i Schrems II at EU-retten ikke kommer til anvendelse ettersom behandlingen gjelder nasjonal sikkerhet. De hevder at ettersom EU-lovgivning ikke får anvendelse i EU-stater når behandling av personopplysninger skyldes nasjonal sikkerhet, kan det heller ikke kreves at USA, når etterretningstjenester der ønsker å behandle personopplysninger for samme formål, skal anvende EU-lovgivningen.[49]

Anførselen forankres i TEU artikkel 4 (2) som bestemmer at:

> « [The Union] shall respect [the Member States] essential State functions, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member States»

Et lignende unntak følger av Privacy Shield. Det følger av avtalens vedlegg at:

> «Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements» [50]

Dette innebærer at Privacy Shield-prinsippene ikke er absolutte, og at unntak fra anvendelse av disse prinsippene kan være mulig i den grad det er nødvendig for å møte kravene til nasjonal sikkerhet.

I tillegg følger det av personvernforordningen artikkel 2 nr. 2 bokstav d at forordningen ikke får anvendelse ved behandling av personopplysninger som utføres av kompetente myndigheter med henblikk på å

> «forebygge, etterforske, avsløre eller straffeforfølge straffbare forhold, herunder vern mot og forebygging av trusler mot den offentlige sikkerhet»

[49] Schrems II avsnitt 55
[50] Commission implementing decision vedlegg II.5 a

Et eksempel på slik behandling er aktiviteter som gjelder nasjonal sikkerhet.[51] Det følger av forordningens fortale at behandling i dette øyemed skal behandles av annen mer spesifikk lovgivning, herunder direktiv (EU) 2016/680.[52] [53] Direktivet er gjennomført i norsk rett gjennom politiregisterloven – og forskriften.[54] Hensynet bak bestemmelsen er først og fremst at en ønsker å legge forholdene til rette for en effektiv håndhevelse av strafferetten og straffeprosessen, og regelen viser at i enkelte tilfeller tilsier sakens art og alvorlighet at personvernet må vike.

Ettersom både TEU artikkel 4 (2), Privacy Shield vedlegg II og personvernforordningen artikkel 2 nr. 2 bokstav d gir uttrykk for at når en behandling av personopplysninger skyldes nasjonal sikkerhet så gjelder det andre regler, er spørsmålet om behandling av personopplysninger som skyldes nasjonal sikkerhet medfører at EU-retten bortfaller.

Spørsmålet om hvorvidt og i hvilken utstrekning en stats suverenitet gjennom EU og et EU-medlemskap ligger hos EU, har vært en sentral debatt i EU i en årrekke. Suverenitetsprinsippet er et folkerettslig prinsipp som innebærer at hver enkelt stat har den ultimate autoritet og makt over seg selv, og ikke er underkastet noen annen vilje enn sin egen.[55] Unionsrettens natur og EUs forhold til medlemsstatene reiser således spørsmålet om maktbalansen mellom medlemsstatene og EU, og om det finnes tilfeller der statens suverenitet medfører at nasjonal lovgivning får forrang over EU-retten.

TEU artikkel 4 (2) gir isolert sett grunnlag for begrensninger i anvendelsen av EU-retten. «National security» henviser nettopp til *nasjonal* sikkerhet, som jo ligger til den enkelte stat å regulere og utøve. Overvåkingsprogrammer i nasjonale sikkerhetsinteresser vil dermed etter ordlyden som utgangspunkt falle utenfor EU-rettens anvendelse.

En slik rigid forståelse av maktfordelingen mellom EU og medlemsstatene vil imidlertid i praksis medføre at all behandling utført av etterretningstjenester av hensyn til nasjonal sikkerhet alltid vil falle utenfor EU-lovgivningens anvendelsesområde. De nasjonale sikkerhetsunntakene ville dermed representere en omfattende omgåelsesfare ved at man,

[51] Wessel-Aas og Ødegaard (2018) s. 113
[52] Fortalen pkt. 19
[53] Dir. (EU) 2016/680 om vern av fysiske personer i forbindelse med vedkommende myndigheters behandling av personopplysninger med henblikk på å forebygge, etterforske, avsløre eller straffeforfølge straffbare forhold eller iverksette strafferettslige sanksjoner, om fri utveksling av slike opplysninger og om oppheving av Rådets rammebeslutning 2008/977/JIS
[54] Lov 28.mai 2010 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)
[55] Ruud og Ulfstein (2011) s. 21

tilsynelatende enkelt, kan stemple noe som å gjelde nasjonal sikkerhet og dermed slippe unna en rekke europeisk personvernlovgivning. Dette ville umuliggjort ethvert forsøk på et felles forpliktende regelverk. [56]

Læren om EU-rettens forrang over nasjonal rett ble fastslått av EU-domstolen allerede i Costa-saken i 1964, og i dommen peker EU-domstolen særlig på at fellesskapsrettens natur på generelt grunnlag innebærer en suverenitetsavståelse innenfor enkelte områder. [57]

Om saker som gjelder nasjonal sikkerhet har EU-domstolen uttalt i ZZ v Secretary of state Home Department at

> «although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns State security cannot result in European Union law being inapplicable» [58]

og i European Commission v Italy at dersom EU-lovgivningen ikke kommer til anvendelse i saker som gjelder nasjonal sikkerhet, vil unntaket

> «be liable to impair the binding nature of Community law and its uniform application» [59]

Noe av det man ønsket gjennom den nye personvernforordningen var nettopp å forhindre denne omgåelsesfaren og tvert imot styrke EU/EØS-borgernes personvern i tredjestater. Det følger av forordningens fortale at når personopplysninger overføres ut av EU/EØS og til mottakere i tredjestater, bør det beskyttelsesnivået som personer sikres i EU/EØS gjennom forordningen ikke undergraves.[60] De nasjonale sikkerhetsunntakene kan etter dette ikke forstås som generelle unntak fra anvendelsesområdet til EU-retten.

Det vil etter dette heller være mer nærliggende å forstå TEU artikkel 4 (2) som en regel om kompetansefordeling mellom EU og de enkelte medlemsstaters nasjonale rettshåndhevelse. Etter folkeretten og suverenitetsprinsippet er hver medlemsstat suveren når det gjelder nasjonal sikkerhet, men dette må ikke feiltolkes som en generell adgang til å gå bort i fra EU-lovgivningen i saker som gjelder nasjonal sikkerhet. I EU-retten må derfor de grunnleggende

[56] Ruud og Ulfstein (2011) s. 21
[57] C-6/64 Costa v ENEL
[58] C-300/11 ZZ v Secretary of State Home Department avsnitt 38
[59] C-387/05 European Commission v Italy avsnitt 45
[60] Fortalen pkt. 101

prinsippene om behandling av personopplysninger gjelde selv om behandlingen er begrunnet i nasjonal sikkerhet.

Dersom Privacy Shield skal sikre et tilstrekkelig beskyttelsesnivå sammenlignet med det nivået som følger av EU-retten, må det kunne kreves at de grunnleggende prinsippene om behandling av personopplysninger fortsatt blir ivaretatt selv om behandlingen gjelder «national security». Det ville jo ikke vært noe poeng i å regulere myndighetenes adgang til overvåking av europeiske personopplysninger dersom nasjonal sikkerhet uansett hadde trumfet ethvert personvernprinsipp, og det er ikke en akseptabel rettstilstand at nasjonal sikkerhet fungerer som et trumfkort hvor ethvert virkemiddel er tillatt uten hensyn til retten til privatliv.

3.2 Hva er «national security»?

Et nærliggende spørsmål som oppstår når en vurderer betydningen av «national security»-unntak, er hva som faktisk utgjør «national security». Selv om det finnes internasjonale retningslinjer for forståelsen av begrepet, finnes det ingen entydig forståelse av innholdet innad i EU. Det er ikke forsøkt definert nærmere i hverken EU-lovgivning eller rettspraksis.

En rapport utarbeidet av The European Union Agency for Fundamental Rights fra 2017 fremhever behovet for en klar definisjon som medlemsstatene kan forholde seg til. [61] EU-domstolen har tatt til ordet for at unntak som begrunnes i nasjonal sikkerhet skal tolkes snevert, og at en eventuell anvendelse av unntaket må være velbegrunnet.[62] I mangelen på en klar definisjon av «nasjonal sikkerhet» innad i EU, henviser The European Union Agency for Fundamental Rights i sin rapport til EMD og domstolens praksis fra EMK artikkel 8 (2) for veiledning.

Fra EMDs rettspraksis kan det utledes at blant annet spionasje,[63] terrorisme,[64] oppfordring til terrorisme[65] og ekstreme organisasjoner som truer demokratiet[66] anses som adekvate trusler mot nasjonal sikkerhet. Det er derfor slik at det ikke lenger bare er det tradisjonelle forsvar og beskyttelse av eget territorium som faller innenfor begrepet «nasjonal sikkerhet». Dagens

[61] European Union Agency for fundamental rights (2017), *Surveillance by intelligence services: fundamental rights, safeguards and remedies in the EU* Volume II: *field perspectives and legal update* s. 53-54
[62] Se for eksempel C-387/05 European Commission v Italy avsnitt 45
[63] C 47143/06 Roman Zakharov v Russia
[64] C 5029/71 Klass and others v Germany
[65] C18954/91 Zana v Turkey
[66] C 19392/92 United Communist Party of Turkey v Turkey

trusselbilde medfører at andre trusler også må omfattes. Ny teknologi har gitt kriminelle nye verktøy og gjort kriminaliteten internasjonal. I tillegg kommer at en sikkerhetstjeneste skal være forebyggende, hvilket impliserer at en må planlegge for alle forskjellige situasjoner som muligens kan være en trussel mot nasjonal sikkerhet. Det norske forslaget om digitalt grenseforsvar hos E-tjenesten viser at «nasjonal sikkerhet» er et dynamisk begrep og en rettslig standard som forandrer seg med samfunnsutviklingen.[67] Dette kan være noe av grunnen til at både EU-domstolen og EMD har vært tilbakeholdne med en klar definisjon. Også statenes skjønnsmargin tilsier at det er staten som ligger nærmest til å vurdere hva som utgjør en så farlig trussel at det er naturlig å kategorisere den som en trussel mot den nasjonale sikkerhet.

Heller ikke i USA har «national security» blitt klart definert, men US Supreme Court har uttalt at nasjonal sikkerhet

> « […] relates only to those activities which are directly concerned with the nation's safety, as distinguished from the general welfare» [68]

Uttalelsen er langt på vei sammenfallende med den europeiske forståelsen, og tilsier at det kreves en viss terskel før noe er så alvorlig at det anses som en trussel mot den nasjonale sikkerhet.

Til tross for at amerikanske myndighets adgang til europeiske personopplysninger i saker som gjelder nasjonal sikkerhet nå er adressert i Privacy Shield, i motsetning til sin forgjenger Safe Harbour, har unntaket mottatt kritikk fra flere hold. En rekke rapporter fra artikkel 29-gruppen og EDPS har gitt klart uttrykk for at formuleringen «to the extent necessary to meet national security» er for vid og upresis, og at formålene bak inngrep må snevres inn.[69] Det er i den anledning viktig å merke seg at en av årsakene til at Safe Harbour-avtalen ble underkjent av EU-domstolen i Schrems-saken var nettopp fraværet av regler som begrenset amerikanske myndigheters adgang til å gjøre inngrep i de grunnleggende rettighetene til personer hvis data ble overført fra EU til USA.

Det nasjonale sikkerhetsunntaket i Privacy Shield er problematisk også i den forstand at behandling av personopplysninger som skjer i nasjonalt sikkerhetsøyemed er vanskelig å

[67] Digitalt grenseforsvar (DGF) Lysne II-utvalget s. 10
[68] The US Supreme Court Cole v Young, 351 U.S 563 (1956)
[69] Se for eksempel artikkel 29-gruppen *Working Document on surveillance of electronic communication for intelligence and national security purposes* WP 288 s. 14-15 og
EDPS *Opinion 4/2016 on the EU-U.S Privacy Shield draft adequacy decision* s. 7-8

overprøve. I dag synes arbeidet i etterretningstjenestene i stor grad å være sammenflettet med arbeidet til andre rettshåndhevende myndigheter, som jo utfører sine arbeidsoppgaver på bakgrunn av andre formål enn nasjonal sikkerhet.[70] Dette representerer en stor og reell fare for at unntakene som gjelder nasjonal sikkerhet utvides til å dekke behandling av personopplysninger for formål som opplysningene lovlig ikke egentlig kan brukes til, som for eksempel saker om «the general welfare», jf. ovenfor. Artikkel 29-gruppen har uttalt at det ikke foreligger noen automatisk presumsjon om at det nasjonale sikkerhets-argumentet anført av nasjonale myndigheter faktisk er gyldig, og at det ligger til den enkelte stat å godtgjøre at inngrepet faktisk skyldes nasjonal sikkerhet. [71]

3.3 Inngrep i retten til privatliv

3.3.1 Innledning

Når det i EU-retten må konkluderes med at de grunnleggende prinsippene om behandling fortsatt må gjelde selv om behandlingen er begrunnet i nasjonal sikkerhet, er det naturlig å se til EMK 8 (2) da denne gir direkte uttrykk for det samme. Det følger av bestemmelsen at inngrep kan skje

> «når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet […]»

Bestemmelsen er et utslag av en interesseavveining der interessen i å effektivt kunne motvirke og bekjempe trusler må veies opp mot ethvert individs grunnleggende rett til personvern. [72] Den er samtidig en anerkjennelse av at personvernet ikke uten videre settes til side i slike tilfeller – som vi skal se nærme på nedenfor.

[70]Artikkel 29-gruppen *Working Document on surveillance of electronic communication for intelligence and national security purposes* WP 288 s. 14
[71] Artikkel 29-gruppen *Working Document on surveillance of electronic communication for intelligence and national security purposes* WP 288 s. 6
[72] Ot.prp. nr. 49 s. 4

3.3.2 «Nødvendig i et demokratisk samfunn»

EMK art 8 (2) gir hjemmel til inngrep i retten til privatliv hvis det er «nødvendig i et demokratisk samfunn» av hensyn til blant annet den nasjonale sikkerhet. Dette innebærer at selv om inngrepet skjer av hensyn til den nasjonale sikkerhet, må det fremdeles være «nødvendig». Hensynet bak denne begrensningen er at en stat, i kampen mot for eksempel terrorisme, ikke kan ty til hvilket som helst virkemiddel. [73]

Spørsmålet er om overvåkingen av europeiske personopplysninger utført av amerikanske myndigheter begrunnet i nasjonal sikkerhet er «nødvendig i et demokratisk samfunn».

Kravet om at inngrepet må være nødvendig, betyr ikke at det må være uunnværlig.[74] Terskelen er ikke så høy at inngrepet må være det eneste mulige alternativet, men samtidig fremgår det av EMDs rettspraksis at enhver bestemmelse som unntar et individ en grunnleggende rettighet skal tolkes snevert.[75]

I vurderingen av om inngrepet er nødvendig i et demokratisk samfunn, har EMD oppstilt et underliggende vurderingstema av hvorvidt inngrepet svarer til «a pressing social need» - et pressende sosialt behov. [76] Når det gjelder overvåking som sådan, skjer dette i de aller fleste tilfeller med det formål å beskytte nasjonale interesser og sikre nasjonal sikkerhet. Overvåking skjer således i statens og samfunnets interesse. Dagens trusselbilde tatt i betraktning, er det særlig antiterrorarbeid som utgjør det største formålet med overvåking. Vilkåret om at inngrepet må svare til «a pressing social need» synes ikke ha voldt store problemer i rettspraksis når inngrepet gjelder antiterrorarbeid, med mindre staten har handlet i ond tro.[77] Etter dette synes det klart at overvåking med nasjonal sikkerhet for øyet svarer til «a pressing social need», og vilkåret er oppfylt.

I tillegg til at inngrepet må være «nødvendig», ligger det i nødvendighetsvilkåret også et krav om at inngrepet må være proporsjonalt. EMD uttalte i S. and Marper v United Kingdom at

[73] Sak 5029/71 Klass and others v Germany avsnitt 49
[74] Forente saker 947/72, 6205/73, 7052/75, 7061/75, 7107/75 og 7113/75 Silver and others v United Kingdom avsnitt 97
[75] Sak 5029/71 Klass and others v Germany avsnitt 42
[76] Sak 5493/72 Handyside v the United Kingdom avsnitt 48-49
[77] van der Hilst (2013) s. 262

> «The question, however, remains whether such retention is proportionate and strikes a fair balance between the competing public and private interest" [78]

Det må etter dette være en rimelig balanse mellom ethvert individs rett til privatliv og et demokratisk samfunns rett til å beskytte seg mot terrorvirksomhet. Spørsmålet er dermed om overvåkningen utført av amerikanske myndigheter etter PPD-28 og FISA 702 er proporsjonal.

At det må være en rimelig balanse mellom retten til privatliv og overvåking, tilsier at det ene ikke må utelukke det andre. I striden mellom terrorbekjempelse og privatliv må det likevel kunne sies å være allment antatt at konsekvensene av å ikke drive antiterrorarbeid er langt mer alvorlig enn å ikke ha fullstendig rett til sitt privatliv. En ytterste konsekvens av å vektlegge retten til privatliv mer enn behovet for overvåking kan være at liv går tapt, mens overvåking i ytterste konsekvens kan medføre en nedkjølingseffekt. Nedkjølingseffekten er ideen om at vi endrer oppførsel dersom vi føler at vi blir overvåket, og at vi derfor unngår å foreta oss noe fordi vi er redde for at personopplysningene vi etterlater oss kan få negative konsekvenser.[79] EU-domstolen deler samme bekymring, og uttalte i Digital Rights Ireland at det faktum at data blir innsamlet og gjenbrukt

> « […] is likely to generate […] the feeling that their private life are the subject of constant surveillance»[80]

I beste fall kan en slik nedkjølingseffekt medføre at vi unngår å gjøre helt ordinære gjøremål fordi vi blir usikre på hvordan personopplysningene våre vil bli brukt. I verste fall kan slik nedkjølingseffekt medføre at ytringsfriheten blir satt under press fordi vi blir redde for å uttale oss i frykt for at det vi uttaler oss om kan bli brukt mot oss senere.

Skal hensynet om å redde liv veies opp mot hensynet om nedkjølingseffekten, er det i avveiningen nærliggende å tillegge statens rett til å beskytte seg mot terrorvirksomhet mest vekt. På generelt grunnlag har EMD imidlertid vært tilbakeholden med å uttale seg om hvilke interesser som veier tyngst. Dette skyldes først og fremst at enhver stat er gitt en skjønnsmargin som innebærer at hver enkelt stat ligger nærmest å tolke konvensjonen i tråd med egne forutsetninger. EMD er dermed forpliktet til å legge den enkelte stats forståelse til grunn i sin tolking, og dette vil påvirke EMDs prøvingsintensitet.[81] I saker som gjelder antiterror og

[78] Forente saker 30562/04 30566/04 S. and Marper v United Kingdom avsnitt 118
[79] Laumann, Kari, «*Nedkjølingseffekten indikerer at ytringsfriheten er under press etter Snowden»* (2014)
[80] Digital Rights Ireland avsnitt 37
[81] van der Hilst (2013) s. 257-259

overvåking synes EMD å gi statene en vid skjønnsmargin, nettopp fordi det er staten som er nærmest til å vurdere hvilke tiltak og virkemidler som er mest effektive for dem i deres stat. [82]

EMD har i proporsjonalitetsvurderingen i flere saker vurdert om inngrepet «[is] pursuing a legitimate aim».[83] Spørsmålet er om inngrepet må være effektivt – at det faktisk må fungere. Det kan i den sammenheng argumenteres for at det etter ordlyden ikke stilles noe krav til at inngrepet faktisk må virke. «Pursuing» tilsier at det er tilstrekkelig at staten *søker å oppnå* et mål, og at målet faktisk ikke må være oppnådd.

Hensikten bak å ilegge dette momentet vekt i vurderingen er todelt. For det første skal kravet om at inngrepet skal være effektivt sikre at retten til privatliv ikke ofres for noe som ikke er godt for noe. Tanken er at dersom overvåkingen ikke leder til et resultat, er det ikke proporsjonalt å gjøre inngrep i retten til privatlivet. For det andre er det en frykt for at midlene som tas i bruk i nasjonal sikkerhets navn enten viser seg å være ineffektive eller i praksis blir brukt til andre formål. Dette var tilfellet i Shimovolos v Russia, der russisk etterretning under mappen «potensielle ekstremister» hadde plassert «rettighetsforkjempere».[84]

Målet med overvåking i USA under PPD-28 følger av fortalen, hvor det heter at innsamling av signaletterretning

> «is necessary for the United States to advance its national security and foreign policy interests and to protect its citizens and the citizens of its allies and partners from harm» [85]

Det følger videre av fortalen at dette innebærer å sikre

> «our relationships with other nations, […] counterterrorism, and other issues» [86]

Når det uttalte målet med overvåking er å drive antiterrorarbeid, må det i vurderingen av effektiviteten av overvåkingen ses hen til hvorvidt overvåkingen har gitt resultater. Det er imidlertid vanskelig å vurdere hvorvidt overvåking av europeiske opplysninger har vist seg å være effektivt. Dette ligger først og fremst i overvåkingens natur; blir man hemmelig overvåket er det nettopp hemmelig. Det er derfor vanskelig å si noe sikkert om hvor mange av de som blir

[82] Se for eksempel sak 49548/06 Colon v the Netherlands avsnitt 86-97
[83] Se blant annet sak 5493/72 Handyside v the United Kingdom avsnitt 49
[84] Sak 30194/09 Shimovolos v Russia avsnitt 54
[85] PPD-28 fortale sec. 2
[86] PPD-28 fortale sec. 2

utsatt for overvåking blir tatt av amerikanske myndigheter. Det kan likevel nevnes at den amerikanske regjeringen anslår at 94.368 personer i 2015 ble målrettet overvåket under FISA 702.[87] Tatt i betraktning at 549 personer har blitt dømt for internasjonal terrorisme i tidsrommet 11/9 2001 til 31/12/2016[88], synes omfanget av overvåkingen ikke bare å være enorm, men også for det meste ineffektiv. Det kan på den andre siden fremheves at sannsynligheten for at trusler mot den nasjonale sikkerhet oppdages ved overvåking objektivt sett er til stede. Fengslingen av 594 terrorister underbygger dette. Dette er imidlertid en vanskelig (og i de aller fleste tilfeller konfidensiell) bevisvurdering som ligger til retten.

Et annet moment i proporsjonalitetsvurderingen er hvorvidt det finnes andre mindre inngripende midler. Kan målet oppnås med andre mindre inngripende midler, er inngrepet mindre nødvendig og dermed også ikke proporsjonalt. I saker som gjelder antiterrorarbeid og overvåking er det imidlertid vanskelig å vurdere dette. Dette fremgår også av EMDs rettspraksis, og skyldes statens skjønnsmargin.[89] Likevel må det kunne stilles spørsmål ved om innsamling av personopplysninger kan skje på en mindre inngripende måte enn ved bulkinnsamling, jf. PPD-28 sec 2.

Bulkinnsamling er innsamling av enorme mengder data hvor en betydelig del av disse ikke er relevante for etterretningen. Disse dataene inkluderer tredjeparter som ikke er av noen interesse for etterforskningen, og informasjonen er ofte overhode ikke tilknyttet det målet som overvåkingen var tiltenkt. Dataene har ingen nytteverdi og vil ikke bidra til å identifisere trusler eller annen relevant informasjon. Bulkinnsamling oppstår fordi etterretningstjenestene på tidspunktet for datafiltreringen ikke vet hva som har etterretningsverdi, slik at det er umulig å avgjøre hva som skal samles inn. For å være sikre på at myndighetene får *all* relevant informasjon, samler de derfor inn *all* informasjon. Andelen av data som ikke er av relevans er langt større enn andelen som er av relevans, og det er denne overflødige mengden av irrelevant data som definerer bulkinnsamling.

[87] Schrems II avsnitt 186
[88] The United States Department of Justice (2018) https://www.justice.gov/opa/pr/doj-dhs-report-three-out-four-individuals-convicted-international-terrorism-and-terrorism
[89] Sak 5029/71 Klass and others v Germany avsnitt 49

I forbindelse med den nylige avsagte dommen i Big Brother Watch[90] henviste EMD til en uavhengig organisasjon kalt Independent Reviewer of Terrorism Legislation[91] som i mai 2016 igangsatte en omfattende undersøkelse av britisk terrorlovgivning og konkluderte med at ingen andre overvåkingsmidler vil tilstrekkelig kunne erstatte bulkinnsamling.[92] Rapporten fremhever at dette skyldes to ting; for det første har terrorister blitt mer sofistikerte når det gjelder å unngå bli gjenkjent, og for det andre har globaliseringen og utviklingen av internett medført at kommunikasjonsrutene (veien kommunikasjonsdata reiser) har blitt særdeles uforutsigbare.[93]

Rapporten gjelder kun lovgivning i Storbritannia, og har derfor begrenset betydning når en vurderer bulkinnsamling i USA og hvorvidt det finnes andre mindre inngripende men tilsvarende alternativer. Det er likevel grunn for å tro at situasjonen er den samme i USA, ettersom bakgrunnen for hvorfor bulk er ansett som nødvendig skyldes den teknologiske utviklingen som jo er lik i begge stater. Det konkluderes derfor med at det ikke finnes mindre inngripende midler som ville ført til det samme resultatet som bulkinnsamling.

I dag synes oppfatningen til EU-kommisjonen å være at bulkinnsamling som sådan ikke er et brudd på EMK art. 8. For Kommisjonens del synes det sentrale i Privacy Shield-rammeverket å være at USA eksplisitt har gitt Kommisjonen bekreftelse på at

> «the U.S. Intelligence Community 'does not engage in indiscriminate surveillance of anyone, including ordinary European citizens'» [94]

Og videre uttaler Kommisjonen at:

> «In particular, bulk collection will only be authorised exceptionally where targeted collection is not feasible»[95]

[90] Forente saker Forente saker 58170/13, 62322/14 og 24960/15 Big Brother Watch and others v the United Kingdom
[91] Independent Reviewer of Terrorism Legislation, en uavhengig organisasjon hvis formål er "to inform the public and political debate on anti-terrorism law in the United Kingdom", se https://terrorismlegislationreviewer.independent.gov.uk/about-me/. Se hele rapporten her: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf
[92] Big Brother Watch and others v United Kingdom avsnitt 176 og 384
[93] Big Brother Watch and others v United Kingdom avsnitt 384
[94] Commission implementing decision avsnitt 82
[95] Commission implementing decision avsnitt 89

Kommisjonen konkluderer med at Privacy Shield –og lovgivning og etterretningspraksis i USA–

> «conforms with the standard set out by the Court of Justice in the Schrems judgment»[96]

Privacy Shield forutsetter ikke avvikling av noen pågående utenlandsetterretningsprogrammer i USA, og forutsetter heller ingen endringer i amerikansk lovgivning. Disse uttalelsene forstås dermed slik at Kommisjonen er klar over at bulkinnsamling skjer i USA og at Kommisjonen mener dette ikke er i strid med grunnleggende rettsprinsipper.

Standpunktet til Kommisjonen når det gjelder lovligheten av bulkinnsamling er sammenfallende med konklusjonen i Big Brother Watch. Her fremhever EMD at bulkinnsamlingen i Storbritannia i seg selv ikke er et brudd på EMK artikkel 8.

Til tross for dette fant retten likevel at det forelå et brudd på Konvensjonen fordi de begrensninger, rettssikkerhetstiltak («safeguards») og kontroll som kreves på de ulike stadiene av behandlingen ikke var tilstrekkelig effektive.[97] Fra dommen kan det utledes at bulkinnsamling ikke strider med artikkel 8 dersom lovgrunnlaget er tilstrekkelig klart, det anses nødvendig og forholdsmessig og ledsages av tilstrekkelig kontrollmekanismer. Det er i proporsjonalitetsvurderingen derfor nødvendig å se på hvorvidt de retningslinjer og kontrollmekanismer som USA har garantert EU-kommisjonen i Privacy Shield-avtalen er tilstrekkelige, og denne vurderingen følger av oppgavens neste del.

[96] Commission implementing decision avsnitt 90
[97] Big Brother Watch and others v the United Kingdom avsnitt 387

4 Behandling av personopplysninger i USA

4.1 Innledning

I denne delen av oppgaven skal vi se nærmere på PPD-28 og FISA 702, og se på hvorvidt de rettssikkerhetstiltakene som tilbys gjennom disse lovene - og som er garantert gjennom Privacy Shield – tilstrekkelig holder EUs standard for vern av personopplysninger. Det overordnede spørsmålet er om europeiske personopplysninger lagret i USA tilbys et «tilstrekkelig beskyttelsesnivå» sammenlignet med det som tilbys i EU/EØS.

Av Privacy Shield-beslutningen følger det en rekke brev fra det amerikanske justisdepartementet som gir skriftlige forsikringer om at den amerikanske regjeringen skal sikre at de begrensinger og garantier som skal beskytte europeiske borgeres personvernrettigheter blir overholdt. Når det gjelder PPD-28 og FISA 702 er brevet fra the Office of Director of National Intelligence («ODNI»-brevet) særlig relevant.[98]

Brevene gir en oversikt over de vanligste verktøyene som brukes ved innsamling av data, og de redegjør for gjeldende prosedyrer som følger av det fjerde grunnlovstillegget i USAs grunnlov som inneholder prosessregler og retningslinjer som justisdepartementet har forpliktet seg til å følge.[99]

Det følger av det fjerde grunnlovstillegget at:

> «The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause […]» [100]

Formålet med bestemmelsen er å beskytte ethvert individs personvern og sikkerhet mot vilkårlig og urimelig inngrep. [101] Den tillater inngrep («search and seizures») under to omstendigheter; utgangspunktet er at det i saker som gjelder innenlands kriminaletterforskning

[98] Commission implementing decision, se vedlegg VI
[99] Commission implementing decision avsnitt 126
[100] The Constitution of the United States of America, amendment IV Search and seizures (1791)
[101] US Supreme Court, Berger v State of New York 388 U.S 41 (1967) s. 53

kreves en rettskjennelse.[102] I saker hvor et slikt krav ikke foreligger, er myndighetene heller underlagt en rimelighetstest. Hvorvidt et inngrep er «rimelig» vurderes i to ledd, hvor det først må vurderes i hvilken grad inngrepet utgjør en invasjon av individets privatliv, og deretter i hvilken grad inngrepet er nødvendig for å møte statens interesser. Grunnloven sørger derfor at amerikanske myndigheter ikke har ubegrenset, urimelig eller vilkårlig tilgang til amerikanske personopplysninger. [103] Selv om bestemmelsen kun gjelder for amerikanske borgere i USA, argumenterer EU-kommisjonen for at europeiske borgere og deres personopplysninger indirekte nyter det vernet som følger av grunnloven, under forutsetning av at det i utgangspunktet er amerikanske selskaper som sitter på opplysningene.[104] Europeiske personopplysninger er også indirekte vernet gjennom at PPD-28, som amerikanske myndigheter er bundet til, fastslår at enhver innsamling av såkalt signals intelligence (SIGINT) skal gjennomføres i samsvar med USAs grunnlov og det fjerde grunnlovstillegget. [105]

En generell bestemmelse om personvern, slik som det fjerde grunnlovstillegget, gir imidlertid ikke et tilstrekkelig personvern sammenlignet med EU-retten. Artikkel 29-gruppen har uttalt at dersom en tredjestat skal anses for å ha et «tilstrekkelig beskyttelsesnivå», må tredjestaten ha bestemmelser som omhandler praktiske relevante aspekter til retten til databeskyttelse i sin personvernlovgivning. [106] Det må derfor ses hen til andre, mer spesifikke amerikanske overvåkingslovgivninger for å avgjøre om beskyttelsesnivået er «tilstrekkelig».

[102] The US Supreme Court, Katz v United States 389 U.S. 347 (1967) s. 357
[103] Commission implementing decision vedlegg VII
[104] Commission implementing decision avsnitt 127
[105] Commission implementing decision avsnitt 69 a)
[106] Artikkel 29-gruppen, *Adequacy Referential,* Adopted on 6 February 2018, WP 245 s. 4

4.2 Innsamling etter PPD-28 og FISA 702

4.2.1 PPD-28

The Presidental Policy Directive 28 er et presidentdirektiv som har som hovedformål å sette begrensninger for innsamling og behandling av personlig data. Den gjelder for den delen av etterretningen som kalles the Bureau of Intelligence and Research (INR) som er underlagt the US Department of State. [107] Den gjelder innsamling av signaletterretning uavhengig av hvor dataene befinner seg – i eller utenfor USA – og den gjelder derfor også for data som er samlet inn når de er overført fra EU til USA.[108]

Hovedregelen for innsamling av personopplysninger er etter PPD-28 at:

> «Signals intelligence activities shall be as tailored as feasible»[109]

Signaletterretning er en type etterretning som baserer seg på elektroniske signaler og systemer.[110] I amerikansk etterretning deles SIGINT tradisjonelt inn i to underkategorier; kommunikasjonsetterretning (COMINT) og elektronisk etterretning (ELINT). [111] Kommunikasjonsetterretning er – blant mye annet – overvåking og registrering av forskjellig typer telefoni, e-post og annen elektronisk kommunikasjon. Så lenge opplysningene kan knyttes direkte eller indirekte til en person, representerer signaletterretningen innsamling av personopplysninger, jf. personvernforordningen artikkel 4 nr. 1.

Det er vanskelig å si noe konkret om hva som menes med "as tailored as feasible». Formuleringen er ukjent i europeisk personvernlovgivning, men den lar seg best oversette til det norske uttrykket «så skreddersydd som mulig». Prinsippet kommer til anvendelse i vurderingen av *hvordan* opplysningene blir innsamlet og i vurderingen av *hva* som faktisk samles inn.[112] For å avgjøre om opplysninger skal samles inn, må etterretningsmyndighetene blant annet vurdere om annen informasjon er tilgjengelig, og prioritere innsamling gjennom disse kildene dersom det er hensiktsmessig.[113] Dette betyr at etterretningstjenesten er pålagt å

[107] the National Security Act (1947) sec. 3 (4)(i)
[108] Commission implementing decision vedlegg VI 1.a, se strekpunkt 4
[109] PPD-28 sec. 1(d)
[110] NSA, *Signals Intelligence*, se https://www.nsa.gov/what-we-do/signals-intelligence/
[111] US Department of Defence, *Department of Defence Dictionary of Military and Associated Terms* (2009) s. 500
[112] Commission implementing decision vedlegg VI 1.b
[113] Commission implementing decision vedlegg VI 1.b

snevre inn innsamlingen slik at unødvendige og irrelevante opplysninger ikke blir gjenstand for behandlingen. Dette gjøres gjerne ved at man benytter seg av bestemte søkeord («selectors») som for eksempel et navn, et sted eller en organisasjon. Innsamling av opplysninger ved bruk av slike søkeord kalles «targeted» (målrettet) innsamling. Det kan forøvrig stilles spørsmål ved om en innsamling som for eksempel kun inneholder ordet «Syria» egentlig er målrettet, da dette vil generere store mengder data og omfatte et stort antall mennesker. Uansett er poenget og hovedregelen at innsamlingen skal være målrettet.

Det er nærliggende å dra en parallell mellom kravet til at innsamling av personopplysninger skal være «så skreddersydd som mulig» til kravet om dataminimering som i dag følger av personvernforordningen artikkel 5 nr. 1 bokstav c hvor det heter at personopplysninger skal

> «være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for»

Bestemmelsen lovfester prinsippet om dataminimering, og innebærer at det ikke skal behandles flere opplysninger enn nødvendig og utgjør dermed et forbud mot behandling av overskuddsinformasjon.

PPD-28 gir også adgang til bulkinnsamling. Det heter at:

> «The United States must consequently collect signals intelligence in bulk in certain circumstances in order to identify […] threats» [114]

En problematisk side ved PPD-28 er at den kun setter begrensninger for bulk*innsamling*. Begrensningene lar seg ikke overføre til andre problematiske sider ved masseovervåking som sådan, for eksempel bulk*searching*. Det følger uttrykkelig av PPD-28 at direktivet ikke gjelder

> «signals intelligence data that is temporarily acquired to facilitate targeted collection»[115]

Personopplysninger som er midlertidig anskaffet gjennom bulksøk og som lagres i en kort periode, som jo forekommer for eksempel etter FISA 702 og UPSTREAM, faller dermed utenfor PPD-28s anvendelsesområde. Her møter vi igjen utfordringen med at den amerikanske og europeiske forståelsen av hva som faktisk utgjør en behandling av

[114] PPD-28 sec. 2
[115] PPD-28 sec. 2 fotnote 5

personopplysninger er fundamentalt ulike. Som nevnt under punkt 2.3 ville et slikt søk i en EU/EØS-stat utgjort et inngrep i seg selv fordi det dreier seg om en befatning med personopplysninger, og ville derfor blitt vernet gjennom charteret og personvernforordningen.

4.2.2 FISA 702

The Foreign Intelligence Surveillance Act (FISA) 702 gir amerikanske myndigheter adgang til å overvåke ikke-amerikanske borgere som befinner seg utenfor amerikansk territorium. Den er spesielt relevant for europeiske personopplysninger som har blitt overført fra EU til et Privacy Shield-sertifisert amerikansk selskap i USA, da den hjemler innsamling av utenlandsk etterretningsinformasjon rettet mot ikke-amerikanske personer utenfor amerikansk territorium gjennom å pålegge elektroniske kommunikasjonstjenester å utlevere informasjon. Formålet er å oppdage kommunikasjon mellom utenlandske terrorister før de ankommer USA.[116] Det følger av ODNI-brevet at i den grad personopplysningene som blir innsamlet er signaletterretning, er innsamlingen underlagt retningslinjene i PPD-28. [117]

Det følger av FISA 702 sec.103 at NSA (National Security Agency) under «UPSTREAM»-programmet har hjemmel til å foreta såkalt «about collection» av enkeltpersoner. Det følger av bestemmelsen at med «about collection» menes

> "a communication that contains a reference to, but is not to or from, a target of an acquisition […]" [118]

Det dreier seg altså om innsamling av personopplysninger som ikke har noe med vedkommende å gjøre eller som vedkommende ikke er en del av. Situasjonen oppstår dersom noen for eksempel sender en mail som ikke er til eller fra en person under overvåking, men bare inneholder vedkommendes e-postadresse – fordi e-postadressen er en personopplysning om (*about*) vedkommende. All kommunikasjon som referer seg til den e-postadressen vil dermed bli gjenstand for overvåking. I realiteten medfører det at NSA får tilgang på enorme mengder personopplysninger som det ikke er grunn til å tro at har noe med terror eller annen alvorlig kriminalitet å gjøre. Det er påfallende at denne bestemmelsen har blitt gjeninnført, da den for bare litt over et år siden, i april 2017, ble opphevet fordi The Foreign Intelligence Surveillance

[116] Commission implementing decision vedlegg VI pkt. II
[117] Commission implementing decision vedlegg VI pkt. II
[118] FISA 702 section 103 (b)(1)(A)

Court (FISC) fant at NSA ikke overholdt de begrensningene og prosedyrene som var satt som vilkår for den type behandling av personopplysninger. [119]

Artikkel 29-gruppen deler samme bekymring. I sin årlige rapport fra 2017 har arbeidsgruppen lagt frem en rekke bekymringer i forbindelse med FISA § 702. I rapporten kritiseres særlig det vide begrepet «target», og det stilles spørsmål ved begrepets proporsjonalitet og nødvendighet.[120]

4.3 Er innsamlingen begrenset til det som er «strictly necessary»?

4.3.1 Innledning

Retten til privatliv og beskyttelse av personopplysninger er, som vi har sett, ikke absolutt og kan begrenses, forutsatt at begrensningene er i samsvar med EU-charteret artikkel 52 (1). Det følger av bestemmelsen at

> «subject to the principle of proportionality, limitations [on the exercise of fundamental rights] may be made only if they are necessary […] »

Bestemmelsen lovfester, på lik linje med EMK artikkel 8, at et ethvert inngrep må være proporsjonalt og nødvendig i forhold til det målet som søkes å oppnås. Når det gjelder brudd på de grunnleggende rettighetene om privatliv og beskyttelse av personopplysninger, har EU-domstolen presisert kravene i artikkel 52 (1) og formulert vurderingstemaet som et krav om at inngrepet må være «strictly necessary». Vilkåret følger av blant annet Digital Rights Ireland og Tele2 Sverige, som begge ble avsagt i forbindelse med den nasjonale gjennomføringen av EU-direktivene om datalagring (ePrivacy Directive). [121] I begge sakene var det overordnede spørsmålet om direktivene var i strid med EU-charteret artikkel 7 og 8. I Digital Rights Ireland uttalte domstolen at

[119] NSA, *NSA stops Certain Section 702 "Upstream" Activities* (2017)
[120] Artikkel 29-gruppen, *EU-U.S. Privacy Shield – First annual joint review,* Adopted on 6 February 2018 WP 245 s. 15-16
[121] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

> «derogations and limitations in relation to the protection of personal data must apply in only so far as is strictly necessary» [122]

og i Tele2 Sverige at datalagring kan finne sted dersom den begrenses

> «to what is strictly necessary» [123]

Spørsmålet er dermed om de begrensningene som følger av amerikansk overvåkingslovgivning – og som er garantert gjennom Privacy Shield – er begrenset til det som er «strictly necessary» («strengt nødvendig»).

4.3.2 Klare og presise regler

I vurderingen av hva som er strengt nødvendig, ligger det først og fremst et krav om at lovgivningen må fastsette klare og presise regler for omfanget og anvendelsen av behandlingen.[124] EU-domstolen uttalte i Schrems at lovgivning som setter begrensninger i retten til privatliv

> «must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure» [125]

I dette ligger også et krav om at loven må indikere under hvilke omstendigheter innsamling av personopplysninger kan skje.

I USA har det i den anledning blitt stilt en rekke kritiske spørsmål til hvordan prinsippene i PPD-28 blir gjennomført i praksis. For det første er det grunn til å understreke at PPD-28 er et direktiv, og følgelig må de prinsipper og retningslinjer som følger av direktivet gjennomføres i hver enkelt etterretningsorganisasjon (byrå) og deres interne prosesser. En gjennomføring av relativt vide og uklare prinsipper kan medføre en rekke ulike forståelser og gir rom for ulik tolking – avhengig av hvem og hvilken etterretning som gjennomfører den. Det kan derfor allerede her argumenteres for at reglene som følger av PPD-28 ikke i tilstrekkelig grad resulterer i klare og presise regler.

[122] Digital Rights Ireland avsnitt 52
[123] Forente saker C 203/15 og C 698/15 Tele2 Sverige AB v Post – och telestyrelsen og Secretary of state for the Home Department v Watson avsnitt 108
[124] Tele2 Sverige avsnitt 109
[125] Schrems avsnitt 91

Det kan også stilles spørsmål ved hvorvidt vilkårene for *når* bulkinnsamling kan skje er tilstrekkelig klare og sikrer forutberegnelighet. Adgangen til å samle inn opplysninger i bulk er ikke formulert som et klart unntak fra hovedregelen om at innsamlingen skal være så skreddersydd som mulig. Det følger av PPD-28 at bulk kan skje når målrettet innsamling ikke er mulig

> «due to technical or operational considerations» [126]

Det følger av ordlyden at dette er en vurdering som ligger til etterretningen, og hvert enkelt tilfelle av bulkinnsamling må vurderes konkret. Det innebærer at der teknologien krever det, må bulkinnsamling skje. Det er ikke noe krav om at bulkinnsamlingen må være siste utvei, men operasjonens karakter må tilsi at bulk er nødvendig, jf. «operational considerations». Formuleringen er imidlertid vag, og kan neppe betraktes som en presis begrensning i myndighetenes adgang til å utføre overvåking, da det oppstår en rekke ubesvarte spørsmål i tilknytning til vilkåret; hvem er det som ligger nærmest til å foreta denne vurderingen? Er den som foretar denne vurderingen avskåret fra den myndigheten som utfører overvåkingen? Og hvilke rettslige betraktninger legges til grunn i en slik vurdering? Vilkåret fremstår heller som en vurdering av hva som er mest praktisk og effektivt for etterforskningen, og er således en vurdering av hva som taktisk, strategisk og teknisk vil fungere best. Fra et EU-perspektiv burde vurderingen heller ligge til hvilket inngrep som er det minst inngripende for den som blir utsatt for overvåkingen, ikke hva som egner seg best for etterforskningen.

Som forklart ovenfor, er bulkinnsamling innsamling av personopplysninger uten man bruker selektorer – nettopp fordi man ikke vet man ser etter. Det dreier seg altså om en ubegrenset og ikke målrettet innsamling. I Schrems uttalte domstolen at lovgivning ikke er begrenset til det som er «strictly necessary» når loven gir adgang til å behandle alle personopplysninger

> «without differentiation, limitation or exception being made in the light of the objective pursued […]» [127]

Uttalelsen gir grunnlag for å hevde at bulkinnsamling dermed klart er et brudd på EU-retten. Men til tross for at bulkinnsamling ikke er målrettet, kan det argumenteres for at den likevel er begrenset. I Privacy Shield argumenterer ODNI for nettopp dette. Det heter at bulkinnsamling

[126] PPD-28 sec. 2 fotnote 5
[127] Schrems avsnitt 93

> «[…] is neither 'mass' nor 'indiscriminate'; rather it is focused as precisely as possible» [128]

Bulkinnsamling kan iverksettes for seks formål som skal oppdage og motvirke trusler om: spionasje, terrorisme, masseødeleggelsesvåpen, trusler mot cybersikkerhet, trusler mot væpnede amerikanske eller allierte styrker og andre transnasjonale kriminelle trusler som er relatert til de fem andre formålene. [129] I motsetning til de omtvistede datalagringsdirektivene i Digital Rights Ireland og Tele2 Sverige, som påla lagring av all telekommunikasjon uten at det måtte foreligge noen konkret trussel eller mistanke, er bulkinnsamling i USA begrenset til å gjelde tilfeller hvor det foreligger en alvorlig og (tilsynelatende) konkret trussel. Det kan derfor argumenteres for at PPD-28 ikke gir hjemmel til bulkinnsamling på generelt grunnlag, og dette taler for at lovgivningen er begrenset til det som er «strengt nødvendig».

Formålene som rettferdiggjør bulkinnsamling omtales i Privacy Shield-beslutningen som «specific purposes».[130] Det må likevel kunne stilles spørsmål med hvor konkrete disse formålene egentlig er. Hva menes for eksempel med «cybersikkerhet»? Begrepet er ikke definert hverken i PPD-28 eller Privacy Shield-beslutningen. Homeland Security omtaler på sine nettsider cybersikkerhet som en plikt til å beskytte mot alle typer kriminalitet som skjer over internett, blant annet barnepornografi, bank – og finanssvindel og brudd på immaterielle rettigheter. [131] I den anledning har den franske personvernorganisasjonen La Quadrature du Net saksøkt EU-kommisjonen med krav om at Privacy Shield-avgjørelsen må bli kjent ugyldig blant annet på grunnlag av at de operasjonene amerikansk etterretning kan gjennomføre etter amerikansk lovgivning ikke er begrenset til det som er «strictly necessary» [132]. Saken vil imidlertid mest sannsynlig bli avvist av EU-domstolen ettersom saken er anlagt av en juridisk person.

På den andre siden tilsier kravet til klare og presise regler ikke at lovgiver i detalj må beskrive hvilken oppførsel som kvalifiserer til en beslutning om overvåking. Dette ville vært en umulig oppgave for lovgiver, da saker som gjelder nasjonal sikkerhet, som vi jo har sett under punkt 3.2, kan gjelde en rekke ulike forhold. Truslene mot den nasjonale sikkerhet er gjerne av en karakter som er vanskelig å forutse og definere på forhånd. Statene er derfor gitt et visst rom

[128] Commission implementing decision vedlegg VI pkt. 2
[129] PPD-28 sec. 2
[130] Commission implementing decision vedlegg VI (1)(b)
[131] Homeland Security (2016) https://www.dhs.gov/cybersecurity-overview
[132] T-738/16 La Quadrature du Net and Others v Commission

for skjønn. EMD har i den sammenheng uttalt at i saker som påvirker de grunnleggende rettighetene – som retten til privatliv – må loven angi omfanget av ethvert skjønn som tildeles de enkelte myndighetene. [133] Ettersom dommen gjelder brudd på EMK artikkel 8 som tilsvarer EU-charteret artikkel 7 og 8, må uttalelsen anses å være relevant for denne vurderingen. En svakhet ved PPD-28 er at det ikke er angitt en slik skjønnsangivelse, og dette taler for at regelverket ikke gir tilstrekkelig klare og presise regler.

Et annet argument som taler for at lovkravet ikke er oppfylt, er at det ikke er tilstrekkelig avklart hva som faktisk regnes som signaletterretning. Som nevnt under punkt 4.2.1 er signaletterretning blant annet kommunikasjonsdata, men det er ikke klart hva dette innebærer. Begrepet er ikke definert hverken i PPD-28 eller i ODNI-brevet. The Privacy and Civil Liberties Oversight Board (PCLOB) [134] har i den anledning fremhevet at det er et sterkt behov for veiledning rundt begrepet «signals intelligence», slik at de ulike byråene vet når de skal anvende direktivet.[135] Det er for eksempel uklart om amerikansk etterretning samler inn data fra transatlantiske kabler, og dette ønsker ikke USA å hverken avkrefte eller bekrefte. Det som fremgår av Privacy Shield er at *dersom* dette skjer, så vil det skje innenfor rammene av PPD-28. [136]

Til tross for at PPD-28 inneholder en rekke begrensninger, synes disse begrensningene i for stor grad å avvike fra EU-rettens krav om at begrensningene må være klare og presise. I tilstrekkelighetsvurderingen taler det klart imot at vilkåret for når bulkinnsamling kan skje er så vidt og uklart, og det er ikke gitt retningslinjer for hva som menes med «operational considerations». I tillegg taler den manglende avklaringen rundt hva som faktisk kan samles inn og hva som nyter vern etter PPD-28 sterkt for at overvåkingen ikke er underlagt klare og presise regler. Det konkluderes derfor med at PPD-28 ikke i tilstrekkelig grad angir klare og presise regler for når bulkinnsamling kan skje.

[133] Sak 35252/08 Centrum for Rättvisa v Sweden avsnitt 119
[134] PCLOB er et uavhengig organ bestående av medlemmer utvalgt av den amerikanske presidenten, og har som formål å overvåke regjeringens overholdelse av beskyttelsen av sivile friheter i dens arbeid mot terror https://www.pclob.gov/about/
[135] The Privacy and Civil Liberties Oversight Board, *Report to the President on the Implementation of Presidential Policy Directive 28: Signals Intelligence Activities* (2016) s. 12
[136] Commission implementing decision vedlegg VI 1 (a)

4.3.3 Lagringstid

I kravet til at personopplysningene skal begrenses til det som er strengt nødvendig, ligger også et krav om at opplysningene ikke skal lagres lenger enn nødvendig. Prinsippet om lagringsbegrensing er også lovfestet i personvernforordningen artikkel 5 nr. 1 bokstav e hvor det heter at personopplysninger ikke skal lagres

> «[…] i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for […]»

Bestemmelsen oppstiller et forbud mot å behandle personopplysninger lenger enn det som er nødvendig for formålet.[137] For å sikre at opplysningene ikke lagres lenger enn nødvendig, burde det fastsettes frister for sletting av personopplysningene. [138]

Utgangspunktet er at personopplysninger skal lagres for kortest mulig tid. Hva som er den nødvendige lagringstiden vil imidlertid variere ut i fra hva som er formålet med lagringen. Personvernforordningen gir for eksempel hjemmel til lengre lagringstid der personopplysningene behandles for arkivformål i allmennhetens interesse. [139] Også i enkelte bransjer er det lovfestet krav om oppbevaring, som for eksempel i regnskapsbransjen og bokføringsloven § 13 (2) hvor behovet for gjenfinning ved etterfølgende kontroll krever lagring av dokumentasjon og enkelte opplysninger i fem år.[140] [141] Lagringsperioden er derfor tett knyttet opp mot formålet med lagringen og behovet for lagringen.

Formålet med lagringen av personopplysninger er etter PPD-28

> «to protect its citizens and the citizens of its allies and partners from harm»[142]

og vilkåret for å samle inn opplysningene er at det må foreligge en

> «foreign intelligence or counterintelligence purpose» [143]

Dette betyr at så lenge personopplysningene er relevante for etterretningen og bidrar til å beskytte individer mot «harm» (skade), så er lagringen nødvendig.

---

[137] Skullerud (2018) Kommentar til artikkel 5 nr. 1
[138] Personvernforordningens fortale avsnitt 39
[139] Personvernforordningen artikkel 5 nr. 1 bokstav e
[140] Lov 1. januar 2005 om bokføring (bokføringsloven)
[141] NOU 2002: 20 s. 15
[142] PPD-28 fortale avsnitt 2
[143] PPD-28 sec. 1(b)

Utgangspunktet for lagringstiden etter PPD-28 er at opplysninger må lages

> «for a sufficient period of time»[144]

Lagring i en «sufficient period» betyr at opplysningene må lagres i en tilstrekkelig periode. En lagringstid som utelukkende er basert på skjønn kan ikke sies å være tilstrekkelig begrenset til det som er «strengt nødvendig» etter EU-retten. Det følger imidlertid videre av PPD-28 avsnitt 4 (a)(i) at opplysningene skal lagres så lenge det er nødvendig for etterretningsbyrået å forstå opplysningenes relevans. Dette er vanligvis fem år, med mindre det er særlig fastsatt i lov eller uttrykkelig besluttet av direktøren for National Intelligence at lagring ut over fem år er i den nasjonale sikkerhets interesse. [145] En beslutning om fortsatt lagring må foretas grundig og ta personvernhensyn og synspunktene fra ODNI Civil Liberties Protection Office i betraktning. [146]

Lagringstiden i seg selv kan ikke isolert sett avgjøre om lagringstiden går utover det som er strengt nødvendig. Det følger av Tele2 Sverige at det må være en sammenheng mellom dataene som er lagret og målet som søkes å oppnås. [147] Dette innebærer at opplysningene må slettes når de ikke lenger er nødvendige for det formålet de ble samlet inn for. Så lenge opplysningene tjener til innsamlingsformålet, er lagringstiden i seg selv ikke et selvstendig argument for at lagringen går ut over det som er strengt nødvendig. I Digital Rights Ireland dreide det seg om en generell og vilkårlig lagringsplikt på maksimalt 24 måneder. Domstolen tok ikke stilling til om en lagring på opptil 24 måneder på generelt grunnlag var for lenge, men konkluderte på bakgrunn av en rekke omstendigheter med at datalagringsdirektivet måtte bli kjent ugyldig fordi det gikk ut over det som er proporsjonalt etter Charteret artikkel 7, 8 og 52 (1). Det er derfor nærliggende å slå fast at kravet om proporsjonalitet i lagringssammenheng medfører at jo videre adgang til lagring, jo kortere kan lagringstiden være. Som vi jo har sett ovenfor er adgangen til å samle inn personopplysninger under PPD-28 vid, og dette taler for at lagringstiden burde være klarere formulert og med utgangspunkt i en maksgrense.

Selv om en beslutning om fortsatt lagring i verste fall vil kunne føre til at lagringstiden blir vesentlig lenger enn fem år, vil det likevel foreligge en sammenheng mellom opplysningene lagret og målet som søkes å oppnås – å beskytte statens innbyggere «from harm» - og følgelig

[144] PPD-28 sec. 4 (a)(i)
[145] PPD-28 sec. 4 (a)(i)
[146] Commission implementing decision vedlegg VI (1)(c)
[147] Tele2 Sverige avsnitt 110

må kravet om at lagringen må begrenses til det som er strengt nødvendig, under tvil, være oppfylt.

4.3.4 Domstolskontroll

For å sikre at overvåking skjer i tråd med nasjonale retningslinjer og begrensninger, har EU-domstolen flere ganger fremhevet behovet for domstolskontroll. [148] I Digital Rights Ireland var en av grunnene til ugyldiggjøringen av datalagringsdirektivet at

> «[a]ccess […]is not made dependent on a prior review carried out by a court […] whose decision seeks to limit access to the data and their use to what is strictly necessary» [149]

Behovet for en uavhengig overordnet kontroll av overvåking har også sterk forankring i EMDs rettspraksis. [150]

Overvåking med hjemmel i FISA er underlagt FISC - The Foreign Intelligence Surveillance Court. Rettens hovedoppgave er å avgjøre søknader sendt inn fra etterretningsmyndighetene om overvåking, fysiske søk og andre former for etterforskningsaktiviteter for utenlandske etterretningsformål.[151] Denne overprøvingen sikrer at amerikanske myndigheter ikke overskrider egen kompetanse, og er med å styrke borgernes rettigheter ved å forhindre vilkårlig og ubegrenset overvåking.

Overvåking etter «tradisjonell FISA» [152] er underlagt individuell juridisk autorisasjon fra FISC. Domstolens rolle i autorisering av overvåking etter FISA 702 er imidlertid lite omtalt i loven. Det følger av FISA 702 bokstav a at autorisasjon til overvåking etter 702 ligger til statsadvokaten og direktøren for National Intelligence, og at slik autorisasjon gis «for a period of up to 1 year». Autorisasjonen sendes deretter til FISC for godkjenning, jf. FISA 702 a(j). I 2017 mottok retten 1614 søknader, og godkjente 1149 av dem. 26 søknader ble avvist i sin helhet. De resterende 441 søknadene ble godkjent etter å ha blitt modifisert i ulik grad. [153]

[148] Se blant annet Tele2 Sverige avsnitt 120 og Digital Rights Ireland avsnitt 62
[149] Digital Rights Ireland avsnitt 62
[150] Se blant annet sak 37138/14 Szabó and Vissy v Hungary avsnitt 77
[151] Foreign Intelligence Surveillance Court, se http://www.fisc.uscourts.gov/
[152] Dvs «vanlig» FISA, ikke FISA 702
[153] Administrative Office of the United States Courts, *Annual report for 2017 regarding the activities of the Foreign Intelligence Surveillance Court* (2018)

De årlige autoriseringene må blant annet inneholde spesifikke kategorier av utenlandsk etterretning som ønskes å samles inn, og «targeting» - og minimaliseringsprosedyrer. [154] Hvis kravene til autorisasjonen er oppfylt, må retten godkjenne den. Domstolen får ikke ta del i selve utformingen av autorisasjonen. Disse utformes av NSA med støtte fra CIA og FBI. [155]

Det er flere problematiske sider ved denne måten å føre domstolskontroll på. For det første har det blitt avslørt flere tilfeller av såkalt formålsutglidning - altså at de årlige autorisasjonene som myndighetene baserer sine ransakelsesordrer på, i praksis har fått et større anvendelsesområde enn det som i utgangspunktet ble godkjent av retten. I EU-retten er forbudet mot slik formålsutglidning lovfestet i personvernforordningen artikkel 5 nr. 1 bokstav b. Det følger av bestemmelsen at personopplysninger skal

> «samles inn for spesifikke, uttrykkelige angitte og berettigede formål, og ikke viderebehandles på en måte som er uforenlig med disse formålene […]»

New York Times kunne i 2015 avsløre at NSA brukte en autorisasjon som gjaldt «foreign government» til å søke etter adresser og cybersignaturer assosiert med hacking. [156] Dette viser hvor enkelt det er for myndighetene å gå ut over autorisasjonen de er gitt når retten kun har mulighet til å godkjenne overvåkingen en gang i året. Her kommer i tillegg at «foreign government» i seg selv er en meget vid formålsangivelse og gir myndighetene stort rom for skjønnsanvendelse. EMD uttalte i Zakharov at der myndighetene blir gitt vide autorisasjoner med rom for skjønn, peker dette i retning av at lovgivningen ikke i tilstrekkelig grad sikrer at overvåkingen ikke blir tilfeldig, urimelig og uregelmessig. [157]

En annen problematisk side ved at domstolen kun gir årlige autorisasjoner, er at det er etterretningsmyndighetene selv som avgjør om overvåking skal skje i hvert konkret tilfelle. I Szabó fremholdt EMD imidlertid at tilsyn med overvåking kan være tilstrekkelig selv om tilsynet ikke utføres av et juridisk organ. [158] Men dersom en overordnet kontroll faktisk skal overprøve en beslutning om overvåking, burde organet som overprøver overvåkingen være adskilt fra den som utøver overvåkingen. Også dette synspunktet har støtte i EMD; retten har

[154] Commission implementing decision vedlegg VI pkt. II
[155] Center for Democracy and Technology (CDT), *Section 702: What it is and how it works* (2017). CDT er en NGO som arbeider for å styrke individuelle rettigheter og friheter «by defining, promoting and influencing techology policy», se https://cdt.org/mission/
[156] New York Times, *Hunting for Hackers, NSA Secretly Expands Internet Spying at U.S border* (2015)
[157] Sak 47143/ 06 Zakharov v Russia avsnitt 265 og 267
[158] Sak 37138/14 Szabó and Vissy v Hungary avsnitt 77

uttalt at rettssikkerhetshensyn tilsier at utøvende myndighet burde være «sufficiently independent» fra myndigheten som skal overprøve overvåkingen. [159]

Det er i utgangspunktet positivt for personvernet at USA opererer med en domstol dedikert til overprøving av overvåking utført etter FISA. Det er likevel påfallende at overvåkingen synes mindre vidtrekkende når overvåkingen skjer med hjemmel i FISA 702. Ettersom den årlige kontrollen med autoriseringene som gir hjemmel til overvåking i praksis har vist seg å representere en stor og reell fare for formålsutglidning, er det vanskelig å se at domstolskontrollen sikrer europeiske forbrukeres personvernrettigheter. I tillegg kommer at høringene og rettens vurderinger regnes som klassifisert informasjon, jf. the President Executive Order 13526 avsnitt 1.4. [160] Dette innebærer at FISC er en lukket domstol avskåret fra offentligheten, slik at det er vanskelig å finne ut av hva domstolen faktisk legger til grunn i sine vurderinger når de godkjenner eller avslår overvåkingsautorisasjoner.

[159] Szabó and Vissy v Hungary avsnitt 77
[160] The President Executive Order 13526, Classified National Security Information (2009)

5 Avslutning og oppsummering

5.1 Sprikende tendenser i EU-domstolen og EMD?

Det utslagsgivende for konklusjonen av om Privacy Shield sikrer europeiske forbrukere et tilstrekkelig beskyttelsesnivå av personopplysninger, er amerikanske myndigheters adgang til bulkinnsamling. Når det gjelder lovligheten av bulkinnsamling, virker oppfatningen i EU og i folkeretten å være noe sprikende. Etter EMDs avgjørelse i Big Brother Watch kan det hevdes at personvernstandarden i EMK tåler å bli satt mer under press enn ellers dersom behandlingen skyldes så alvorlige forhold at staten vurderer det dithen at overvåking og innsamling i bulk er nødvendig. Retten uttalte at

> «It is clear that bulk interception is a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime» [161]

I forlengelsen av dette åpner EMD opp for at bulkinnsamling kan skje dersom staten anser det som nødvendig av hensyn til nasjonal sikkerhet. I enda en nylig avsagt dom fra juni 2018 konkluderte EMD med at masseinnsamling av signaletterretning i Sverige ikke var et brudd på EMK artikkel 8, da retten fant at det svenske systemet ga adekvate og tilstrekkelige garantier mot vilkårlighet og misbruk av personopplysningene. [162]

Samtidig uttaler EU-domstolen i Tele2 Sverige at virkemidler iverksatt i nasjonal sikkerhets interesse, uansett hvor viktig det måtte være,

> «[…] can not in itself justify that national legislation providing for the general and indiscriminate retention […]» [163]

Og Artikkel 29-gruppen har gjentatte ganger uttalt at

> «massive and indiscriminate surveillance of individuals can never be considered as proportionate and strictly necessary in a democratic society» [164]

[161] Big Brother Watch avsnitt 386
[162] Sak 35252/08 Centrum for Rättvisa v Sweden avsnitt 181
[163] Tele2 Sverige avsnitt 103
[164] Artikkel 29-gruppen, *First annual Joint Review*, Adopted 28. November 2017 WP 255 s. 14-15

Uttalelsene og avgjørelsene i domstolene viser at EU og folkeretten har ulik tilnærming til problemet. Den ulike vurdering av lovligheten av bulkinnsamling skyldes trolig at EU synes å vektlegge statenes skjønnsmargin i langt mindre grad enn EMD. Den beste forklaringen på dette er nok at det klare formålet med unionsretten er å oppnå rettsenhet og likhet blant medlemsstatene. Dette målet ville vært vanskelig å oppnå dersom statene stod fritt til å regulere og utøve overvåkingsmidler i enhver sak som gjelder nasjonal sikkerhet.

I EMD virker ikke kravet til nødvendighet og proporsjonalitet å være like strengt som i EU, men her stilles det til gjengjeld strenge krav til kontrolltiltak på alle stadiene av inngrepet. Det er likevel vanskelig å skille på disse vurderingene. Som vi har sett under punkt 3.3 er kontrolltiltak ofte en del av proporsjonalitetsvurderingen. Det ser derfor ut til at det ikke lenger er et spørsmål om lovligheten av bulkinnsamling, men heller et spørsmål om gjennomføringen av den. Det skal derfor bli spennende å se om EU-domstolen følger i EMDs fotspor når de til neste år skal komme til en avgjørelse Schrems II-saken.

5.2 Kan bulkinnsamling forenes med kravene til behandling av personopplysninger oppstilt i EU-retten?

I vurderingen av om USA sikrer et «tilstrekkelig beskyttelsesnivå», er det viktig å huske på at beskyttelsesnivået ikke skal være tilsvarende det som følger av EU-retten. Europeisk og amerikansk personvernlovgivning er ikke identisk, og en direkte sammenligning av de to rettsordenene vil fort kunne lede til et forenklet bilde av den rettslige situasjonen. Det avgjørende er at USAs rettsorden må ivareta de sentrale aspektene ved det europeiske personvernet.

Selv om EU-domstolen og EMD har ulik tilnærming til bulkproblematikken, er EU-kommisjonen i sine tilstrekkelighetsbeslutninger først og fremst bundet av EU-retten og ikke folkeretten. Selv om EU-domstolen anerkjenner at dagens trusselbilde tilsier at etterretningstjenestene kan ta i bruk avansert teknologi, og vedkjenner at overvåking er et nyttig virkemiddel, er det vanskelig å se at personvernforordningen, kjernen i EU-charteret artikkel 7 og 8 og EU-domstolens rettspraksis lar seg forene med innsamling av personopplysninger i bulk.

Terskelen for å benytte seg av bulkinnsamling i USA er ikke høy. Det kan som tidligere nevnt skje dersom målrettet overvåking ikke er mulig «due to technical or operational considerations», og behandlingen kan skje under seks svært vide og omfattende omstendigheter. Dette er klart i strid med formålsbegrensningen i personvernforordningen artikkel 5 nr. 1 bokstav b, som jo krever at behandling av opplysninger skal skje etter spesifikke, uttrykkelige angitte formål. Det stilles derfor spørsmål ved om hvordan Privacy Shield kan sikre en tilsvarende europeisk personvernstandard dersom rammeverket ikke engang inkorporerer de grunnleggende personvernprinsippene som følger av personvernforordningen. Det må derfor konkluderes med at the EU-U.S Privacy Shield ikke i tilstrekkelig grad sikrer at europeiske personopplysninger er beskyttet fra overvåking utført av amerikanske myndigheter.

5.3 Veien videre

Det er kanskje urealistisk å ønske seg en overordnet juridisk løsning for transatlantiske overføringer, særlig på områder som gjelder behandling av personopplysninger med formål å beskytte rikets sikkerhet. Det er nok for optimistisk å håpe at enkelte stater er villige til å gå på akkord med egne verdier og nasjonal lovgivning for å imøtekomme en annen stats beskyttelsesnivå – enten dette nivået er sterkere eller svakere enn den andres.

Selv om Privacy Shield i denne oppgaven vurderes til å per i dag ikke gir europeiske forbrukere et tilstrekkelig vernenivå som tilsvarer europeisk personvern, er avtalen et godt startpunkt for videre forhandlinger mellom EU og USA. Personvernforordningen artikkel 45 nr. 3 slår fast at Kommisjonen løpende skal holde øye med utviklingen i den aktuelle godkjente tredjestaten. Gjennomgangen skal skje minst hvert fjerde år, men det følger av Privacy Shield at avtalen årlig skal gjennomgås av organer i EU og USA i en såkalt «annual joint review». [165] Utviklingen i tredjestaten som EU-kommisjonen må følge med på kan gjelde en rekke omstendigheter – både juridiske og politiske. For Privacy Shield vil antakeligvis både presidentvalget i 2016, USAs uttreden av FNs menneskerettsråd[166] og gjenautoriseringen av FISA 702[167] være omstendigheter av betydning for den årlige gjennomgangen.

Den årlige gjennomgangen fant i år sted i Washington i oktober, og det er ventet at gjennomgangen blir offentliggjort i midten av desember. Kommisjonen har juridisk

[165] Commission implementing decision avsnitt 146
[166] NRK, *USA ut av FNs menneskerettsråd* (2018)
[167] CNN *«Senate passes FISA section 702 reauthorization"* (2018)

kompetanse til å oppheve, endre eller suspendere Privacy Shield dersom man kommer til at USA ikke lenger sikrer et tilstrekkelig beskyttelsesnivå. Prosedyren for dette følger av personvernforordningen artikkel 93 nr. 2, og innebærer at Kommisjonen må vedta en ny gjennomføringsrettsakt om oppheving eller endring av den foregående. [168]

[168] Skullerud (2018) Kommentar til artikkel 45 nr. 5

6 Litteraturliste

Lover og forskrifter

1992	Lov 1992-11-27-109 Lov om gjennomføring i norsk rett i hoveddelen om avtale om Den europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven)
1999	Lov 21-05-1999 Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven)
2000	Lov 2000 – 04-14-31 Lov om behandling av personopplysninger (personopplysningsloven) [Opphevet]
2005	Lov 2004-11-19-72 Lov om bokføring (bokføringsloven)
2010	Lov 2010-05-28-16 Lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)
2018	Lov 2018-06-15-38 Lov om behandling av personopplysninger (personopplysningsloven)

Lovforarbeider

NOU 2002: 20	*Ny bokføringslov – Nye regler om bokføring, spesifikasjon, dokumentasjon og oppbevaring av regnskapsopplysninger*
NOU 2015: 13	*Digital sårbarhet – sikkert samfunn*
Ot.prp. nr. 49 (1996-1997)	Om lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)
Lysne II-Utvalget (2016)	*Digitalt grenseforsvar (DGF)*

Internasjonale traktater og konvensjoner

EMK	Den europeiske menneskerettskonvensjon, Roma, 4.11.1950
EØS-avtalen	Avtalen om Det økonomiske samarbeidsområde, Brussel, 17.03.1993
SP	FNs konvensjon om sivile og politiske rettigheter, New York, 16.12.1966
EU-charteret	EUs charter om grunnleggende rettigheter, Strasbourg, 18.12.2000
TEU	Traktaten om Den europeiske union, Lisboa, 01.12.2009

EU/EØS-rettsakter

EP/Rfo. 2016/679	Europaparlaments – og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (Generell personvernforordning) [GDPR]

Fo. 2016/679 fortale	Europaparlaments – og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (Generell personvernforordning) [GDPR]
EP/Rdir. 2016/860	Europaparlaments – og rådsdirektiv (EU) 2016/680 om vern av fysiske personer i forbindelse med vedkommende myndigheters behandling av personopplysninger med henblikk på å forebygge, etterforske, avsløre eller straffeforfølge straffbare forhold eller iverksette strafferettslige sanksjoner, om fri utveksling av slike opplysninger og om oppheving av Rådets rammebeslutning 2008/977/JIS
EP/Rdir. 1995/46	Europaparlaments- og rådsdirektiv 95/46/EF av 24.oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (Opphevet) [Personverndirektivet]
C/2016/4176	Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 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 (notified under document **C(2016) 4176**) (Text with EEA relevance) 12.07.2016
EP/Rdir. 2002/58/EC	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
EØS-komiteens beslutning nr. 144/2017	EØS-komiteens beslutning av 7. juli 2017 om endring av EØS-avtalens vedlegg XI (Elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunnstjenester)

Avgjørelser fra Den Europeiske Unions domstol (EU-domstolen)

[Hentet fra https://curia.europa.eu/jcms/jcms/j_6/en/]

C-6/64	*Costa v ENEL* 15.06.1964
C-387/05	*European Commission v Italian Republic*, 15.12.2009
Forente saker C-92/09 og C-93/09	*Volker und Markus Schecke and Eifert v Land Hessen and Bundesanstalt für Landwirtschaft und Ernährung*, 09.11.2010
C-300/11	*ZZ v Secretary of State Home Department*, 04.06.2013
Forente saker C-293/12 og C-594/12	*Digital Rights Ireland Ltd. v Ireland and Kärntner Landesregierung and others* 08.04. 2014
C-362/14	*Maximillian Schrems v Data Protection Commissioner, Digital Rights Ireland Ltd.* 06.10.2015
Forente saker C-203/15 og C-698/15	*Tele2 Sverige AB v Post – och telestyrelsen og Secretary of State for the Home Department v Watson* 21.12.2016
T-738/16	*La Quadrature du Net and Others V Commission* (Søksmål anlagt 15. oktober 2016)
C-311/18	*Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*

Avgjørelser fra Den Europeiske Menneskerettsdomstol (EMD)

[Hentet fra https://hudoc.echr.coe.int/eng# {"documentcollectionid2»: ["GRANDCHAMBER","CHAMBER"]}]

Sak 5493/72	*Handyside v the United Kingdom*, Strasbourg, 07.12.1976
Sak 5029/71	*Klass and others v Germany*, Strasbourg, 06.09.1978
Forente saker 947/72, 6205/73, 7052/75, 7061/75, 7107/75 og 7113/75	*Silver and others v the United Kingdom*, Strasbourg, 25.03.1983
Sak 18954/91	*Zana v Turkey*, Strasbourg, 25.11.1997
Sak 19392//92	*United Communist Party of Turkey v Turkey,* Strasbourg, 30.01.1998
Forente saker 30562/04 30566/04	*S. and Marper v United Kingdom*, 04.12.2008
Sak 30194/09	*Shimovolos v Russia*, Strasbourg, 21.06.2011, FINAL 28.11.2011
Sak 49548/06	*Ferdinand Jozef Colon v the Netherlands*, Strasbourg, 15.05.2012
Forente saker 40660/08 og 60641/08	*Von Hannover v Germany (No. 2)*, Strasbourg, 07.02.2012
Sak 47143/ 06	*Roman Zakharov v Russia*, Strasbourg, 04.12.2015
Sak 37138/14	*Szabó and Vissy v Hungary*, Strasbourg 12.01.2016 FINAL 06.06.2016
Sak 35252/08	*Centrum for Rättvisa v Sweden*, Strasbourg, 19.08.2018

Forente saker 58170/13, 62322/14 og 24960/15 *Big Brother Watch and others v the United Kingdom*, Strasbourg 13.09.2018

Artikkel 29-gruppen/European Data Protection Board/Supervisor

Artikkel 29-gruppen, *Opinion 1/2010 on the concepts of "controller" and "processor",* Adopted on 16 February 2010, WP 169

Artikkel 29-gruppen, *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision,* Adopted on 13 April 2016, WP 238

EDPS, *Opinion 4/2016 on the EU-U.S Privacy Shield draft adequacy decision,* 03.05.2016

Artikkel 29-gruppen, *Working Document on surveillance of electronic communication for intelligence and national security purposes,* Adopted on 5 December 2014, WP 288

Artikkel 29-gruppen, *EU-US Privacy Shield – First annual Joint Review,* Adopted on 28 November 2017, WP 255

Artikkel 29-gruppen, *Adequacy Referential,* Adopted on 6 February 2018, WP 245 rev. 01

Juridisk litteratur

Bygrave, Lee A. *Data Privacy Law – An International Perspective,* 2. utg., Oxford: Oxford University Press, 2014

Fredriksen, Halvard Haukeland og Mathisen, Gjermund *EØS-rett*, 3. utg., Bergen: Fagbokforlaget, 2018

Lando, Ole *Kort indføring i komparativ ret*, 3. utg., Danmark: Jurist og økonomforbundets forlag, 2009

Ruud, Morten og Ulfstein, Geir *Innføring i folkerett*, 4. utg., Oslo: Universitetsforlaget, 2011

Sejersted, Fredrik, Arnesen Finn, Rognstad, Ole-Andreas og Kolstad, Olav *EØS-rett*, 3.utg., Oslo: Universitetsforlaget, 2011

Skullerud, Åste Marie Bergseng, Rønnevik, Cecilie, Skorstad, Jørgen og Pellerud, Marius Engh *Personvernforordningen (GDPR)* Kommentarutgave, Oslo: Universitetsforlaget, 2018

van der Hilst, Rozemarinj *Putting privacy to the test: How counter-terrorism technology is challenging article 8 of the European Convention on Human Rights,* 1. utg., Oslo: Akademika publishing, 2013

Wessel-Aas, Jon og Ødegaard, Martin *Personvern – publisering og behandling av personopplysninger*, 1. utg., Oslo: Gyldendal, 2018

Tidsskrifter og artikler

Center for Democracy and Technology, *Section 702: What it is and How it works*, 15.02.2017 https://cdt.org/insight/section-702-what-it-is-how-it-works/ [Hentet 14.11.18]

Laumann, Kari *«Nedkjølingseffekten indikerer at ytringsfriheten er under press etter Snowden»*, 2016 https://www.personvernbloggen.no/2016/05/03/nedkjolingseffekten-indikerer-at-ytringsfriheten-er-under-press-etter-snowden/ [Hentet 19.10.18]

NSA, Statement, *NSA stops Certain Section 702 "Upstream" Activities*, 28.04.17 https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml [Hentet 09.10.18]

Savage, Charlie (2015) "Hunting for Hackers, NSA Secretly Expands Internet Spying at U.S border" *New York Times* 04.06.2015 https://www.nytimes.com/2015/06/05/us/hunting-for-hackers-nsa-secretly-expands-internet-spying-at-us-border.html [Hentet 08.11.18]

Thon, Bjørn Erik, *Personvern i USA – part one*, 2013 https://www.personvernbloggen.no/2013/02/11/personvern-i-usa-part-one/ [Hentet 06.09.18]

Elster, Kristian (2018) «USA ut av FNs menneskerettsråd» *NRK* 19.06.2018 https://www.nrk.no/urix/usa-ut-av-fns-menneskerettsrad-1.14091613 [Hentet 29.11.18]

Barret, Ted og Killough Ashely (2018) «Senate passes FISA section 702 reauthorization" *CNN* 18.01.2018 https://edition.cnn.com/2018/01/18/politics/fisa-reauthorization-senate-vote/index.html [Hentet 29.11.2018]

Rapporter og offisielle uttalelser

Administrative Office of the United States Courts, *Annual report for 2017 regarding the activities of the Foreign Intelligence Surveillance Court,* Washington, D.C (2018) http://www.uscourts.gov/sites/default/files/ao_foreign_int_surveillance_court_annual_report_2017.pdf [Hentet 14.11.18]

EDPS, *The transfer of personal data to third countries and international organizations,* Posisjonsnotat, Brussel, 14.07.14

EDPS, *Privacy Shield: more robust and sustainable solution needed,* Pressemelding EDPS/2016/11, Brussel, 30.05.2016

European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: fundamental rights, safeguards and remedies in the EU,* Volum II: field perspectives and legal update, Luxembourg (2017)

National Academies, *Committee on responding to section 5(D) of the Presidential Policy Directive 28: The feasibility of software to provide alternatives to bulk signals intelligence collection* (2015)

Privacy and Civil Liberties Oversight Board (PCLOB), *Report to the President on the Implementation of Presidential Policy Directive 28: Signals Intelligence Activities* (2016) https://www.pclob.gov/library/PPD-28%20Report%20(for%20FOIA%20Release).pdf [Hentet 05.11.18]

The Independent Reviewer of Terrorism Legislation, *Report of the Bulk Powers Review* (2016) https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf [Hentet 21. 10.18]

The U.S Department of Defence, Joint publication 1-02, *Department of Defence Dictionary of Military and Associated Terms,* (12.06.2007) https://web.archive.org/web/20091108082044/http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf [Hentet 22.11.18]

The U.S Department of Justice, *Three Out of Four Individuals Convicted of International Terrorism and Terrorism-Related Offenses were Foreign-Born* (16.01.2018) https://www.justice.gov/opa/pr/doj-dhs-report-three-out-four-individuals-convicted-international-terrorism-and-terrorism [Hentet 20.10.18]

Nettsider

Center for Democracy and Technology https://cdt.org/mission/ [Hentet 14.11.18]

Datatilsynet, *Hva er Privacy Shield?* 2018
https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overfore/hva-er-privacy-shield/ [Hentet 28.09.18]

FISC, http://www.fisc.uscourts.gov/ [Hentet 18.10.18]

Homeland Security, https://www.dhs.gov/cybersecurity-overview [Hentet 09.11.18]

National Academies http://national-academies.org/ [Hentet 19.10.18]

NSA, *Signals Intelligence,* 03.05.16
https://www.nsa.gov/what-we-do/signals-intelligence/ [Hentet 11.10.18]

The Independent Reviewer of Terrorism Legislation
https://terrorismlegislationreviewer.independent.gov.uk/about-me/ [Hentet 21.10.2018]

The Privacy and Civil Liberties Oversight Board (PCLOB)
https://www.pclob.gov/about/ [Hentet 06.11.18]

Utenlandske rettskilder

1791	The fourth amendment to the United States https://www.law.cornell.edu/constitution/fourth_amendment
1978	Foreign Intelligence Surveillance Act: Section 702, 50 U.S.C. § 1881 a https://legcounsel.house.gov/Comps/Foreign%20Intelligence%20Surveillance%20Act%20Of%201978.pdf
1947	National Security Act (26.06.1947) https://www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947

2009	The President Executive Order 13526, Classified National Security Information (29.12.2009) https://www.archives.gov/isoo/policy-documents/cnsi-eo.html
2014	The Presidential Policy Directive 28, Signals Intelligence Activities (17.01.2014) https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities#_ftn5
Ireland High Court	*the Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* 2016 No. 4809 P (03.10.2017)
The United States Supreme Court	*Cole v Young* 351 U.S 563 (10.06.1956)
The United States Supreme Court	*Berger v State of New York* 388 U.S 41(12.06.1967)
The United States Supreme Court	*Katz v United States* 389 U.S. 347 (17.12. 1967)
The United States Supreme Court	*Jane Roe v Henry Wade* 410 U.S. 113 (22.01.1973)