Lov & Data

Nr. 145
Mars 2021
Nr. 1/2021

Innhold









Lov&Data

Lov&Data er et skandinavisk tidsskrift for rettsinformatikk og utgis av

Lovdata
Postboks 6688 St. Olavs plass
NO-0129 Oslo, Norge
Tlf.: +47 23 11 83 00
E-post: lovogdata@lovdata.no
Nettside: www.lovdata.no

Ansvarlig redaktør er Jarle Roar Sæbø
Medredaktør er Trine Shil Kristiansen, Lovdata.
Redaktører for Danmark er dr.juris Henrik Udsen ved Center for informations- og innovationsret, Københavns universitet og Tue Goldschmieding, partner i firmaet Gorrissen Federspiel, København.
Redaktør for Sverige er Daniel Westman, uavhengig rådgiver og forsker.
Fast spaltist er Halvor Manshaus, partner i advokatfirmaet Schjødt.

Trykk: ISSN 0800-7853
Elektronisk: ISSN 1503-8289
Utkommer med 4 nummer pr. år.

Abonnementspriser for 2020
Norge: nkr 370,- pr. år
Utland: nkr 450,- pr. år
Studenter, Norge: nkr 175,- pr år
Studenter, utland: nkr 235,- pr. år
Alle fritt tilsendt.

Lov&Data sendes gratis til ordinære abonnenter av Lovdata Pro og er medlemsblad for foreningene Norsk forening for jus og edb, Svenska föreningen för IT och Juridik (ADBJ), Dansk forening for Persondataret og Danske IT-advokater.

Foreningene kan ev. sende låste pdf-er til sine medlemmer.

Abonnenter på papirutgaven av Lov&Data kan ved henvendelse til Lovdata/sin forening få passord som gir tilgang til elektroniske utgaver av tidsskriftet. Disse er tilgjengelige på *http://www.lovdata.no/pro/tidsskrift/*

Leder

Hvor stor er GDPR hammeren egentlig?

De databeskyttelsesretlige regler har fået en enorm opmærksomhed gennem de senere år. Dette har ikke mindst været drevet af forventningen om/frygten for de meget store bødebeløb, som databeskyttelsesforordningen (GDPR) potentielt lægger op til med bøderammerne på op til 4 % af den globale årlige omsætning. Vi har også set, at de nationale tilsynsmyndigheder har udmålt ganske høje bødebeløb, når de har brugt forordningens mulighed for at uddele administrative bøder for overtrædelse af forordningen. Det er dog en vigtig pointe, at disse bøder kan indbringes for domstolene, og at det derfor i sidste ende er domstolene, der kommer til at fastlægge bødeniveauerne for overtrædelse af forordningen. Der er endnu kun afgjort et begrænset antal bødesager ved domstolene, og det er derfor for tidligt at sige, om domstolene generelt vil tilslutte sig tilsynsmyndighedernes hidtidige bødeniveauer og beregningsmodeller.

At dette ikke nødvendigvis vil være tilfældet, illustrerer den første danske dom på området, der blev afsagt af Retten i Aarhus den 12. februar 2021. Datatilsynet havde indstillet møbelkæden ILVA til en bøde på 1,5 mio. kr. for overtrædelse af forordningen ved at have gemt 385.000 personers oplysninger i et gammelt ERP-system uden en plan for sletning. Retten idømte imidlertid kun møbelkæden en bøde på 100.000 kr., bl.a. med henvisning til, at der alene var handlet uagtsomt. Dommen er blevet anket, men den er en illustration af, at domstolene ikke nødvendigvis anlægges samme vurdering som tilsynsmyndighederne, når der skal fastsættes bøder for overtrædelse af forordningen.

Dommen understreger også, at det er en vanskelige balancegang at fastsætte bødeniveauerne i disse sager. På den ene side bør mindre overtrædelse af et i øvrigt ekstrem komplekst regelsæt ikke udløse millionbøder. Der findes desværre mange eksempler på, at »GDPR bødespøgelset« har skygget for sund fornuft, og virksomheder har undladt at iværksætte fornuftige tiltag eller forfølge forretningsmæssige muligheder med en forkert henvisning til, at GDPR ikke gjorde

det muligt. På den anden side skal det også undgås, at bøderne bliver så små, at de ikke har pønaleffekt, og virksomheder derfor kan spekulere i at betale en lille bøde fremfor at bruge et stort beløb på at indrette deres systemer og processer i overensstemmelse med de databeskyttelsesretlige krav. Den begrænsede effekt af databeskyttelsesreglerne under det tidligere direktiv viser, at dette er en reel risiko.

Det er denne balancegang som domstole (og tilsynsmyndigheder) skal ramme. Trods den meget snak om de høje bøder og omtale af afgørelser fra tilsynsmyndighederne, viser ILVA-dommen, at det er for tidligt at fastslå, hvor stor »GDPR hammeren« reelt er. Dette vil først kunne fastslås i takt med, at vi får mere retspraksis.

Og så kan man i øvrigt pege på, at domstolene også får en vigtig rolle i fastlæggelsen af, hvornår registrerede kan kræve godtgørelse, herunder gennem gruppesøgsmål. Denne type krav kan potentielt udgøre en mindst lige så stor »GDPR hammer« som bøderne. Men det er en helt anden historie.

Henrik Udsen

På rett vei mot selvkjørende biler?

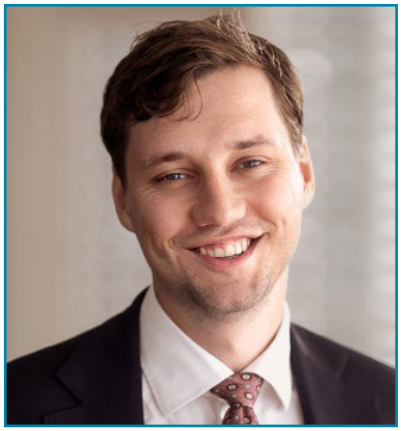
Av Iver Jordheim Brække og Stian Hultin Oddbjørnsen

Innledning

En av store potensielle gullgruvene i mobilitets- og teknologiverden er selvkjørende biler, og det bil- eller teknologiselskapet som klarer å lage den første *helt* selvkjørende bilen går nok en lys tid i møte. De ledende aktørene innenfor selvkjøringsteknologi er nemlig ikke bare bilfabrikanter. Waymo, eid av Google, er et eksempel på en verdensledende aktør innen selvkjøringsteknologi der selskapet i utgangspunktet ikke har en direkte kobling med en tradisjonell bilprodusent.

Av bilselskaper som utprøver selvkjøringsteknologi er Tesla blant de mer fremtredende – i alle fall i media med Elon Musk i spissen. Realiteten er uansett at de aller fleste bilselskaper i dag på en eller annen måte driver med selvkjøringsteknologi i den tro på at selvkjørende biler er (en del av) den nye fremtiden på mobilitetsfeltet. Innenfor kollektivtrafikken er selvkjørende kjøretøy identifisert som en (av flere) mulige løsninger på «last mile»-problematikken. Dette er den siste kilometeren mellom et kollektivknutepunkt og ditt hjem. I stedet for at en rekke mennesker skal belaste veiene og (parkering) areal med å kjøre og parkere sin bil ved togstasjonen, kan man tenke seg selvkjørende minibusser som kjører deg hjem «on demand» sammen med naboene som kommer med det samme toget.

Men hva er egentlig en selvkjørende bil, og hvor langt har man kommet i å regulere selvkjørende biler?



Iver Jordheim Brække

Stian Hultin Oddbjørnsen

Om selvkjørende biler

Det finnes ikke én enkelt autoritativ definisjon av hva en selvkjørende bil er, og forskjellige land har utviklet ulike definisjoner. Kjært barn har også mange navn, og andre vanlige betegnelser på en selvkjørende bil er «førerløs bil» eller «autonom bil». Storbritannia har for eksempel definert at kjøretøyet «kjører selv» dersom kjøretøyet opererer i en modus der det ikke blir kontrollert, og ikke trenger å bli overvåket av en person.[1] Bilselskapene som utvikler selvkjøringsteknologi har derimot en tendens til å erklære at den splitter nye biltypen deres er helt selvkjørende, selv om bilen egentlig bare har en form for avansert *cruise-control*.

Variasjonen av ulike definisjoner har gjort at «The Society of Automotive Engineers» (SAE) har laget en skala som beskriver *nivåer* av kjøreautomatisering på en skala fra 0-5. SAEs skala er en glideskala, der et kjøretøy kan skåre både i bunnen og toppen av et spesifikt nivå. Skalaen skal bidra til å definere i hvor stor grad en bil *faktisk* er selvkjørende, og brukes også blant annet av det amerikanske transportdepartementet.

> Variasjonen av ulike definisjoner har gjort at «The Society of Automotive Engineers» (SAE) har laget en skala som beskriver nivåer av kjøreautomatisering på en skala fra 0-5.

Skalaen er overordnet todelt i den forstand at biler med installert selvkjøringsteknologi som skårer på nivå 0-2 ikke er mer selvkjørende enn at bilen også er avhengig av at

1 Se British Automated and Electric Vehicles Act 2018 artikkel 8 (1) bokstav a.

et menneske konstant overvåker systemet og kjøremiljøet. På nivå 3-5 vil det være et automatisert system som monitorer kjøresystemet og bilens omgivelser. En eventuell fører vil bare være en «backup»-løsning i tilfelle noe går galt.

Går man nærmere inn i de enkelte nivåer, blir graden av menneskelig involvering og maskinens «intelligens» tydeligere. Dersom en bil scorer 0 på skalaen, er bilen en vanlig manuell bil der en fører utfører alle oppgavene i forbindelse med bilkjøringen. Biler som scorer 1 på skalaen vil typisk være biler som har cruise control-funksjon eller andre funksjoner som assisterer sjåføren. Selvkjørende biler på nivå 2 og 3 er biler som kan styre og akselerere av seg selv, men som også er avhengig av en fører som eventuelt kan overprøve selvkjøringssystemene dersom noe går galt. Hovedforskjellen mellom skalaens nivå 4 og 5, er at på nivå 4 kan den selvkjørende bilen bare kjøre under bestemte forhold, og fungerer *bare* når disse forholdene er materialisert. Det er ikke før på skalaens nivå 5 at en bil *faktisk* er fullstendig selvkjørende og kjører av seg selv i alle mulige omgivelser. En selvkjørende bil på nivå 5 burde altså kunne skjønne hva som er riktig prosedyre dersom det utføres veiarbeid på en veistrekning, mens en selvkjørende bil på nivå 4 nok vil fremstå som «forvirret».

Måten en selvkjørende bil «styrer» på foregår gjennom at bilen har programvare som behandler og analyserer all informasjonen som de ulike radarene og sensorene samler inn. Selvkjørende biler er nemlig, i motsetning til vanlige manuelle biler, helt avhengige av blant annet sensorer, algoritmer og maskinlæringssystemer. Selvkjørende biler lager og vedlikeholder et kart over sine omgivelser basert på en rekke sensorer i kjøretøyet. Bilen bruker radarsensorer som overvåker posisjonen til kjøretøyet, og videokameraer oppdager trafikklys, leser veiskilt og sporer andre fremmedobjekter som biler og fotgjengere. Selvkjørende biler har også en rekke andre tekniske funksjoner.

Programvaren vil til slutt sende instruksjoner til bilens styringssystemer, og bilen kjører deretter basert på programvarens instruksjoner uten å involvere en menneskelig sjåfør. Det her den kunstige intelligensen kommer inn for full styrke. Jo mer en selvkjøringsprogramvare brukes, desto mer vil programvaren lære og komme nærmere målet om å være helt selvkjørende på nivå 5.

For å trene opp den kunstige intelligensen er det vanlig å teste ut selvkjøringsteknologien i simulatorer der selvkjøringsprodusentene lager sine egne virtuelle miljøer for å trene opp programvaren. Dette gjør at selvkjøringsprodusentene kan utvikle programvaren uten at bilen utgjør en sikkerhetsrisiko i den fysiske virkeligheten. Virtuelle miljøer kan likevel ikke erstatte utprøving på virkelige veier. I virtuelle miljøer får programvaren forholdsvis god trening på å bruke bilens ulike kameraer riktig, men det er for eksempel vanskeligere å skape et reelt treningsmiljø for radarteknologien til selvkjøringssystemet.

Per dags dato er ingen selskaper som enda har klart å lage en helt selvkjørende bil på nivå 5. De fleste produsentene av selvkjøringsteknologi har bare klart å skape biler som opererer på nivå 2 og 3, selv om flere bilprodusenter -i alle fall selvmener de utprøver biler på vei som opererer på SAEs nivå 4. Det vil si at alle såkalte selvkjørende biler som eksisterer i dag ikke kan kjøre uten at en ansvarlig operatør overvåker systemet, og bilen kjører alltid innenfor et bestemt forhåndsavgrenset område.

Det har imidlertid ikke manglet på spådommer fra ulike selskaper om at de kommer til å klare å lage selvkjørende biler innen få år. Daimler uttalte for eksempel i 2017 at de skulle kunne produsere helt selvkjørende biler i starten av det «neste tiåret». Daimler og andre selskapers uttalelser har vist seg inntil videre ikke å være realistiske, og man er nok i realiteten også i dag et godt stykke unna å få selvkjørende biler på det kommersielle personbilmarkedet.

Ulike utfordringer med å skape helt selvkjørende biler

Det er flere årsaker til at det er vanskelig å lage *helt* selvkjørende biler som har en automatiseringsgrad på nivå 5 etter SAEs skala. Teknologien er avansert, og ikke minst kostnadskrevende. Et hovedproblem som produsentene per dags dato sliter med å overkomme, er at de ikke har klart å gjøre at selvkjøringsteknologien får så god kunstig intelligens som er nødvendig for å få bilen til å operere på nivå 4 etter SAEs skala.

For det andre er det svært vanskelig å tilpasse teknologien ulike geografiske omgivelser. Selv om en bil kjører utelukkende på vei, er *variasjonen* av veier og omgivelser en stor utfordring. Kunstig intelligens må ofte trenes opp veldig spesifikt, og programvaren er enda god ikke nok til å tolke litt uvante situasjoner selv om programvaren har erfart noe lignende før. I byområder kan for eksempel myke trafikanter, trafikklys og komplekse veikryss skape store problemer. I mer landlige områder kan man tenke seg at dårlige veier og manglende merking kan forstyrre bilens ulike sensorer. Også været er en utfordring, der kraftig regn og snø ofte vil forstyrre selvkjøringssystemet. Værforholdene i Norge gjør altså at vi kanskje ikke er det landet som ligger først i selvkjøringskøen, selv om våre unike værforhold også har skapt et eget marked for utvikling av selvkjøringsteknologi. Også ulik fauna har vist seg å by på hodebry. Svenske Volvo måtte blant annet for noen år tilbake innrømme at deres selvkjøringssystem var dårlig tilpasset australske forhold fordi systemet ikke klarte å måle bilens avstand til hoppende kenguruer, selv om systemet

fungerte dersom en elg og hjort gikk over veien.[2]

En tredje hovedutfordring er at den *rettslige* reguleringen av selvkjørende biler ikke har kommet langt. Lovverket er rett og slett ikke på plass, og de reguleringene som gjelder alminnelige manuelle biler passer i mange tilfeller ikke på situasjoner som selvkjørende biler kan komme opp i. Et godt eksempel er eksisterende ansvarsregler, som ofte krever en form for uaktsom handling eller unnlatelse fra fører som betingelse for at det skal foreligge et erstatnings- eller straffeansvar. En populær problemstilling i debatten omkring selvkjørende biler, er ulike etiske aspekter dersom en selvkjørende bil kommer i situasjoner der bilen må «velge» mellom to onder. Skal bilen for eksempel kjøre i en fjellvegg og drepe sin eier, eller isteden kjøre på et gammelt ektepar som går tur? Selv om tankeeksperimentet nok er mer relevant som (morbid) tema i selskapelige lag enn en reell risiko, er ansvarsplassering for ulykker et tema som må adresseres i lovgivning omkring selvkjørende biler.

EUs bærekraft- og mobilitetsstrategi

Også EU har innsett at teknologi som fører til mobilitetsendringer er fremadstormende, og at dette sannsynligvis vil endre hvordan mennesker beveger seg. Bevegelsesfrihet innad i EU er et helt grunnleggende aspekt ved EU-regelverket, og et eventuelt inntog av selvkjørende biler kan ha innvirkning på menneskers muligheter til å bevege seg over landegrensene. Hvis for eksempel landene innad i EU har ulike regler om reguleringen av selvkjørende biler for alminnelig persontransport, kan dette fungere som en mobilitetshindring og svekke grunntanken om fri bevegelighet.

EU har enda ikke vurdert om selvkjørende biler skal reguleres av EU-retten, og eventuelt hvor detaljert et slikt regelverk skal være. I EU-kommisjonens nye rapport om bærekraft- og mobilitsstrategi,[3] der strategiens overordnede mål er å sette europeisk transport på riktig spor mot den nye mobilitetsfremtiden, er derimot selvkjørende biler og selvkjøringsteknologi omtalt. Kommisjonen uttaler i strategien at de mener at automatisert mobilitet vil bli distribuert over en stor skala i EU innen 2030.

> I Norge har man fått på plass en lov om utprøving av selvkjørende kjøretøy med tilhørende forskrift, som skal sikre at produsenter av selvkjøringsteknologi kan teste ut teknologien på norske veier.

EU-kommisjonen uttaler også at EU må adressere mangelen på harmonisert lovgivning og koordinering av relevante trafikkregler og ansvarsregler for automatiserte kjøretøy. Det er altså ikke usannsynlig at en eventuell ny veitrafikklov i Norge vil være basert på et EU-direktiv, eller at det kommer en egen forordning som harmoniserer all veitrafikklovgivning i Europa. Det kan imidlertid være en fordel for EU å starte opp disse prosessene tidlig, hvis de ønsker å implementere et felles regelverk *før* EU-landene lager sine egne detaljerte regler. For eksempel er Tyskland i ferd med å vedta en ny lov om «autonom kjøring».[4]

I tillegg til lovgivning som regulerer selvkjørende biler ute i trafikken, har EU-kommisjonen uttalelser om viktigheten av å *tilrettelegge* for testing og prøving av innovative mobilitetsløsninger. På nåværende tidspunkt er nok tilrettelegging for at markedsaktører kan teste og prøve ut selvkjørende biler vel så viktig som å starte på arbeidet med å harmonisere relevant erstatnings- og bilansvarslovgivning.

Utprøving av selvkjøringsteknologi for alminnelig persontransport krever enten biler som er laget spesielt for selvkjøringsteknologi, eller at man gjør inngrep i standardiserte biler. Da trenger man et regelverk som legger til rette for at det kan gjøres unntak for de strenge reglene vedrørende hva slags kjøretøy som er tillatt på europeiske veier. I Norge er dette gjort gjennom lov om utprøving av selvkjørende kjøretøy.[5]

Det norske regelverket om utprøving av selvkjørende kjøretøy

I Norge har man fått på plass en lov om utprøving av selvkjørende kjøretøy med tilhørende forskrift, som skal sikre at produsenter av selvkjøringsteknologi kan teste ut teknologien på norske veier.

Loven og forskriften legger opp til at Vegdirektoratet kan gi tillatelse til utprøving av selvkjørende kjøretøy.[6] Regelverket er rigget for at eventuelle søkere kan prøve ut ethvert selvkjørende kjøretøy, også potensielle kjøretøy som skårer 4 eller 5 på SAEs skala. Man kan søke om å prøve ut selvkjørende kjøretøy for alminnelig ferdsel både i urbane områder og utenfor bykjernen. Det er i tillegg lagt opp til at kjøretøy ikke alltid trenger å ha en mennes-

2 https://www.theguardian.com/technology/2017/jul/01/volvo-admits-its-self-driving-cars-are-confused-by-kangaroos

3 Navnet på rapporten er «Sustainable and Smart Mobility Strategy – putting European transport on track for the future».

4 Loven er planlagt vedtatt sommeren 2021.

5 LOV-2017-12-15-112

6 Forskrift om utprøving av selvkjørende kjøretøy § 3.

kelig fører som kan overprøve selvkjøringsteknologien.

Formålsbestemmelsen i loven oppsummerer godt hva som er hensikten bak loven, samt hvordan norske myndigheter ønsker å gå frem ved utprøving av selvkjørende kjøretøy. I formålsbestemmelsen står det at loven skal legge til rett for utprøving av selvkjørende kjøretøy innenfor rammer som særlig ivaretar trafikksikkerhets- og personvernhensyn. Det står også at utprøvingen skal skje gradvis særlig ut fra teknologiens modenhet og med formål om å avdekke hvilke effekter selvkjørende kjøretøy kan ha for trafikksikkerhet, effektivitet i trafikkavviklingen, mobilitet og miljø.[7]

At utprøvingen skal foregå gradvis bærer også resten av regelverket preg av. Man har etter loven ikke *rett* på å utprøve selvkjøringsteknologi på norske veier, uansett prosjekt. Loven er bygget opp slik at Vegdirektoratet *kan* gi tillatelse på nærmere fastsatte vilkår.[8] Selv om forskriften har en rekke detaljerte vilkår og dokumentasjonskrav for hva en søknad skal inneholde, har Vegdirektoratet mulighet til å kreve ytterligere dokumentasjonskrav og eventuelt kreve at dokumentasjonskravene skal være vurdert av en uavhengig kompetent institusjon.[9]

Om ulike produsenter av selvkjøringsteknologi vil få mulighet til å prøve teknologien på norske veier avhenger altså sterkt av hva offentlige myndigheter legger til rette for, og hvordan de anvender sitt eget forvaltningsskjønn. På den ene siden er dette forståelig, sett i lys av at norske myndigheter er i startfasen av å tillate selvkjørende kjøretøy på norske veier. På den andre siden kan det argumenteres for at regelverket gir produsenter av selvkjøringsteknologi lite forutberegnelighet. Søknader krever svært mye forarbeid, og det burde etter vårt syn være lettere for markedet å forutse hvilke prosjekter Vegdirektoratet ønsker å godkjenne.

At det kan være vanskelig for produsenter av selvkjøringsteknologi å vurdere om de vil få godkjent sine prosjekter ser man kanskje særlig i de tilfellene der en teknologiaktør, og ikke en bilprodusent, ønsker å utprøve selvkjøringsteknologi i Norge. Regelverket er lagt opp på en måte som gjør at kravene til motorvognen som skal benyttes i utgangspunktet må oppfylle de alminnelige forskriftskrav som kreves for kjøretøy på norske veier. Vegdirektoratet har etter regelverket imidlertid mulighet til å gjøre unntak fra de alminnelige reglene dersom det foreligger tilstrekkelig garantier for at sikkerheten i forbindelse med kjøringen likevel blir ivaretatt.[10] Dette vil som oftest være lettere for aktører som er en bilprodusent og *samtidig* utvikler selvkjøringsteknologi.

Bilprodusenter kan selv modifisere sine egne biler og lage versjoner av bilene som er tilpasset selvkjøringsteknologi, og dermed lettere vise og dokumentere at bilens sikkerhetsfunksjoner og egenskaper ikke er redusert selv om bilen er tilpasset til å være selvkjørende.

Den vanlige måten for rene teknologiselskaper som utvikler selvkjøringsteknologi, og særlig de litt mindre selskapene, er derimot å kjøpe standardiserte biler og deretter montere selvkjøringsteknologi i bilen. Monteringen av selvkjøringsteknologien er inngripende, og går naturlig nok på bekostning av bilens opprinnelige manuelle kjøreegenskaper. Hvis ikke bilprodusenten er involvert i selvkjøringsprosjektet vil bilprodusenten normalt heller ikke kunne gi garantier til Vegdirektoratet eller selvkjøringsprodusenten om at ulike sikkerhetsfunksjoner og kjøreegenskaper er like godt ivaretatt når det er montert selvkjøringsteknologi i bilen.

Ellers bærer reglene om utprøving av selvkjørende kjøretøy preg av å være et risikobasert regelverket, der regelverket i utgangspunktet legger opp til å eliminere enhver mulig risiko dersom det lar seg gjøre. Det er blant annet en egen bestemmelse som ber søker redegjøre for risikoen forbundet med utprøvingen, i tillegg til de omfattende dokumentasjonskrav som følger av øvrige bestemmelser i lov og forskriften.[11] En søker må også redegjøre for forhold som kan oppstå utover såkalt normal drift, enten det er veiarbeid, vær eller andre forhold.

Særlig om aspekter knyttet til personvern og selvkjøringsteknologi

På nåværende stadium i *utviklingen* av selvkjørende biler kan det diskuteres om bruk av selvkjøringsteknologi er et personvernrettslig problem. I utgangspunktet vil ikke bilens systemer trenge å kommunisere med omverdenen i stor grad, og utprøving av selvkjørende biler burde heller ikke nødvendiggjøre noe særlig innsamling av sensitive personopplysninger. I lov om utprøving av selvkjørende kjøretøy er det et eget kapittel om behandling av personopplysninger.[12] Det er imidlertid vanskelig å se at loven gir noen føringer på hvordan personopplysninger skal behandles som ikke allerede følger av GDPR, annet enn at den gir et nasjonalt rettslig grunnlag for å behandle personopplysninger ved utprøving av selvkjørende kjøretøy.

Når selvkjørende biler etter hvert blir mer vanlig i alminnelig drift, vil det imidlertid oppstå komplekse personvernspørsmål. Hvis selvkjørende biler skal bli en vanlig del av

7 Lov om utprøving av selvkjørende kjøretøy § 1.

8 Lov om utprøving av selvkjørende kjøretøy § 4.

9 Forskrift om utprøving av selvkjørende kjøretøy § 8.

10 Forskrift om utprøving av selvkjørende kjøretøy §§ 6 og 7.

11 Forskrift om utprøving av selvkjørende kjøretøy § 10.

12 Lov om utprøving av selvkjørende kjøretøy kapittel 4.

menneskers mobilitetshverdag, vil det være nødvendig at systemene til bilene samfungerer med hverandre. En enkelt selvkjørende bil vil sannsynligvis måtte samfungere med flere hundre andre selvkjørende biler samtidig, og kanskje også infrastruktur som trafikklys og broer. Man kan i tillegg se for seg at en måte å effektivisere trafikkbildet på er å la egne systemer ta kontroll over bilene i for eksempel komplekse veikryss eller byområder med svært mye kødannelse. Dette gjør nok at det vil være vanskelig å bruke en selvkjørende bil og samtidig nekte selvkjøringsteknologien i bilen å kommunisere med andre biler i trafikken.

Et svært dynamisk nettverk av ulike biler som må kommunisere med hverandre vil stille strenge krav til systemene og lovverket for å hindre at informasjonssikkerheten knyttet til personopplysninger svekkes uforholdsmessig. I tillegg til er det åpenbare utfordringer knyttet til cybersikkerhet. Biler har de siste årene vært et virkemiddel for å utføre terror, og en eventuell hacking av en selvkjørende bil vil ikke bare krenke menneskers personvern, men være potensielt livsfarlig, både for de inni bilen og de utenfor.

Det kan videre diskuteres om personvernregelverket med GDPR i spissen rent teknisk sett er tilpasset en hverdag full av selvkjørende biler. Dette kan illustreres med et eksempel om hvordan ansvarsrollene etter GDPR er bygd opp.

Etter GDPR vil det alltid være minst én behandlingsansvarlig for behandlingen av personopplysninger, og personopplysningene som behandles vil være knyttet til en registrert person.[13] I tillegg kan den behandlingsansvarlig engasjere en databehandler som kan behandle personopplysninger på vegne av den behandlingsansvarlige.[14] Den behandlingsansvarlige og en eventuell databehandler har en rekke plikter etter GDPR som skal sørge for at rettighetene til den registrerte ikke krenkes.

De rettslige konseptene behandlingsansvarlig og databehandler er ikke nytt med GDPR, også det gamle personverndirektivet hadde samme ansvarsroller, men å *identifisere* rollene blir stadig mer komplisert som følge av en økende informasjonsflyt og økt digitalisering i samfunnet. Dette kommer nærmest på spissen for selvkjørende biler, så fremt man ikke finner opp et system som gjør det mulig å organisere kjøringen slik at ingen personopplysninger blir behandlet.

Først og fremst kan det nok være en utfordring å fastsette hvem som er behandlingsansvarlig for ulike behandlinger som utføres, enten det er eier av bil, bruker av bil eller produsenten av selvkjøringsteknologi. Man kan også tenke seg at selvkjøringsprodusenten er databehandler. I tillegg må man fastsette ansvarsrollen til de som styrer eventuell infrastruktur.

Siden bilene vil kommunisere, og sannsynligvis dele personopplysninger med hverandre, vil det også være et spørsmål om det skal oppstå et enkelt behandlingsansvar eller felles behandlingsansvar når bilene samfungerer i trafikken. GDPR er per dags dato ikke dimensjonert for felles behandlingsansvar for noe så dynamisk som selvkjørende biler i trafikk, fordi et felles behandlingsansvar i utgangspunktet krever at de behandlingsansvarlige fastsetter en ordning om hvordan de skal overholde pliktene etter GDPR.[15]

Et paradoks er at en selvkjørende bil risikerer å måtte motta eventuelle nødvendige personopplysninger, men *samtidig* gi fra seg opplysninger til andre biler, altså i potensielt en og samme behandling være både behandlingsansvarlig og registrert. En slik løsning vil være lite holdbar etter GDPR.

Regulering av ansvarsroller i forbindelse med behandling av personopplysninger er altså et konsept som kanskje krever særskilt lovregulering for selvkjørende biler. Det er dermed ikke bare ansvarsregler og etiske problemstillinger som krever nye typer regulering, også innenfor informasjonssikkerhet er det sannsynlig at man må tenke mye nytt.

Avslutning

Veien til selvkjørende biler på de høyeste nivåer av autonomi i alminnelig trafikk fremstår inntil videre som lang og svingete. Både tekniske og regulatoriske utfordringer skal forseres. I tillegg vil det for svært mange bilister antakeligvis sitte langt inne før man tør eller vil slippe rattet helt. Samtidig er dette et felt hvor utviklingen går fort. Vi har allerede vært med på prosjekter hvor selvkjørende kjøretøy er blitt pensjonert og sendt til museum fordi teknologien har løpt videre. Vi vil neppe nå pensjonsalderen før vi som en del av transporten hjem fra jobben sitter i en førerløs bil.

Brække og Oddbjørnsen er del av Kluges fagmiljø innen teknologi og mobilitet. De har bistått juridisk på flere prosjekter knyttet til selvkjørende kjøretøy de senere årene.

13 Se GDPR artikkel 4 (1) og 4 (7).

14 Se GDPR artikkel 4 (8).

15 Se GDPR artikkel 26.

Schrems II: Faktisk risiko bør spille en rolle ved overføring av personopplysninger til tredjestater

Av Ove A. Vanebo og Marianne Gjerstad

Ove A. Vanebo

Marianne Gjerstad

1 Innledning

Den såkalte *Schrems II*-dommen[1] fra EU-domstolen tydeliggjør hvor strenge krav som oppstilles etter EUs personvernforordning[2] (heretter bare «forordningen») for å overføre personopplysninger til tredjestater (utenfor EU/EØS).

Hovedproblemstillingen er om de fysiske personene som personopplysningene gjelder er sikret «a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter».[3] Dommen ga imidlertid ikke klare retningslinjer for hva som skal til for å oppfylle kravene for å overføre personopplysninger til tredjestater, og har skapt mye debatt om temaet. I etterkant av *Schrems* II-dommen ga European Data Protection Board (heretter bare «EDPB» eller «Personvernrådet») ut anbefalinger (heretter «anbefalingene») om ytterligere tiltak som må iverksettes dersom beskyttelsesnivået i tredjelandet ikke er tilsvarende som i EU/EØS.[4] Slike ytterligere tiltak skal oppveie det manglende beskyttelsesnivå i tredjelandet og sikre et i det vesentlige tilsvarende beskyttelsesnivå i praksis.

Anbefalingene legger opp til en sekstrinnsvurdering som må gjennomføres for overføring av personopplysninger til tredjeland. Vurderingen skal imidlertid være objektiv og det er ikke tillatt å legge vekt på sannsynligheten for at myndighetene i tredjeland vil skaffe seg tilgang til dataene.[5]

Uttalelsen fra Personvernrådet skiller seg fra tilnærmingen som forordningen ellers legger opp til, hvor det foretas en vurdering av risikoen for brudd på registrerte personers rettigheter og friheter med grunnlag i den konkrete behandlingen. Vi stiller oss skeptiske til den formalistiske tilnærmingen Personvernrådet har valgt, og vil redegjøre for hvorfor vi mener faktisk risiko bør vektlegges i vurderingen.

2 Privacy Shield og Schrems II-dommen

Amerikanske selskaper kunne tidligere benytte rammeverket *Privacy Shield* til å sertifisere seg selv og dermed garantere for at de overholdt personvernkravene i EU. I *Schrems II* vurderte EU-domstolen hvorvidt Privacy Shield var gyldig etter bestemmelsene i personvernforordningen.

Bakgrunnen for saken var at den østerrikske personvernforkjemperen Max Schrems klaget på Facebook Irlands behandling av personopplysninger, herunder selskapets overføring av personopplysninger til morselselskapet Facebook Inc., som er etablert i USA. Schrems krevde at Facebook Irlands overføring av personopplysninger til Facebook Inc. måtte opphøre, fordi

1 Sak C-311/18 av 16. juli 2020, *Data Protection Commissioner mot Facebook Ireland Ltd og Maximillian Schrems* (heretter «Schrems II»).

2 Europaparlaments- og Rådsforordning (EU) 2016/679 av 27. april 2016.

3 Se *Schrems II* bl.a. avsnitt 105.

4 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

5 https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/retningslinjer-og-uttalelser-fra-personvernradet/utfyllende-veiledning-om-schrems-ii/

USA hadde et utilstrekkelig vern av hans personvernrettigheter.

EU-domstolen kom til at Privacy Shield er ugyldig og viste til at den brede adgangen amerikanske myndigheter har til personopplysninger som behandles i USA ikke oppfylte kravene til proporsjonalitet og nødvendighet som kreves etter EU-retten. EU-domstolen viste også til at amerikansk lovgivning ikke gav tilstrekkelig vern for EU-/EØS-borgere.

Dommen konkluderer med at selv om det foreligger et overføringsgrunnlag i personvernforordningen kapittel V, kan dataimportør i tredjelandet være underlagt nasjonale eller lokale lover som er i strid med og går foran forpliktelsene i overføringsgrunnlaget. Dataeksportøren må først undersøke om beskyttelsesnivået som oppnås i praksis, faktisk er i det vesentlige tilsvarende som i EU/EØS. Herunder er det særlig viktig å undersøke om det finnes overvåkingslover eller andre lover som gir tredjelandets myndigheter uforholdsmessig stor adgang til opplysningene.

Domstolens vurderinger i Schrems II får i prinsippet anvendelse på enhver overføring av opplysninger til tredjeland, uavhengig av hvilket overføringsgrunnlag som velges.[6]

3 Personvernrådets veiledningsdokument – seks trinn

Anbefalingene handler som nevnt om hvilke vurderinger man må foreta før man kan overføre personopplysninger til land utenfor EU/EØS og er delt i seks trinn.

Trinn 1 er å kartlegge egne overføringer til land utenfor EØS.[7] Personvernrådet anbefaler å bygge på virksomhetens behandlingsprotokoll, som skal være på plass i tråd med artikkel 30 i personvernforordningen.[8]

Trinn 2 er å identifisere hvilket overføringsgrunnlag som benyttes, jf. kapittel V i forordningen.[9] Virksomheten kan overføre opplysninger dersom EU-kommisjonen har fastslått tilstrekkelig beskyttelsesnivå for tredjestaten.[10] Et viktig overføringsgrunnlag er overføring som omfattes av «nødvendige garantier» fra behandlingsansvarlig eller databehandler.[11] Dette kan sikres ved for eksempel standard personvernbestemmelser vedtatt av EU-kommisjonen (Standard Contractual Clauses, heretter SCC).[12]

Trinn 3 er å vurdere om overføringsmekanismen er effektiv i lys av omstendighetene rundt overføringen. Det må altså vurderes om overføringsmekanismen er effektiv i praksis.[13] At overføringsmekanismen er effektiv innebærer at de overførte opplysningene sikres et beskyttelsesnivå i tredjelandet som i det vesentlige tilsvarer nivået som sikres i EU/EØS. Det må vurderes om det er noe i tredjelandets lovgivning eller praksis som begrenser en effektiv beskyttelse av opplysningene.[14]

Eksempler på relevante momenter som må vurderes er listet opp i et eget vedlegg til Personvernrådets veiledning.[15] Personvernrådet anbefaler å vektlegge lovgivning som er tilgjengelig. For det tilfelle at relevant lovgivning ikke er offentlig tilgjengelig, skal virksomheten vurdere andre «relevante» og «objektive faktorer». Virksomheten skal ikke vektlegge «subjektive» faktorer, som for eksempel sannsynligheten for at offentlige myndigheter i tredjelandet får tilgang til opplysningene i strid med standarden i EU.[16] Hvorvidt «subjektive faktorer» som sannsynlighet kan vektlegges, er kjernen i vår uenighet med Personvernrådets anbefalinger.

Personvernrådet understreker at denne vurdering må gjøres med omhu og dokumenteres grundig, ettersom virksomheten blir holdt ansvarlig for den avgjørelse som den treffer på dette grunnlag. Derimot kan vurderingen vise til rapporterte hendelser, lovgivning, praksis for å påvise at tredjelands myndighet vil søke eller være i stand til å oppnå tilgang til overførte opplysninger.[17]

Trinn 4 er å iverksette ytterligere tiltak for å sikre tilstrekkelig beskyttelse.[18] Dersom vurderingen i trinn 3 avdekker at overføringsmekanismen ikke er effektiv, må virksomheten (eventuelt i samarbeid med databehandler) vurdere ytterligere tiltak. Slike tiltak kan være av kontraktsmessig, teknisk eller organisatorisk art.[19]

Trinn 5 er å gjennomføre eventuelle prosessuelle tiltak.[20] For øvrig viser Personvernrådet til EU-domstolens uttalelse i Schrems II om at det er behandlingsansvarlig og databehandlers ansvar å vurdere om sikkerhetsnivået i tråd med EU-rett kan overholdes i praksis.[21]

Trinn 6 er å gjenta evalueringen med passende mellomrom.[22] Dersom det skjer endringer i tredjelandet som medfører at tiltakene ikke lenger er effektive, må virksomheten ha på plass mekanismer som åpner for at virksomheten kan innstille eller avslutte overføringen.[23]

6 *Schrems II*, avsnitt 92 og 105. Se Personvernårdet uttalelse om dette i avsnitt 5 i *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, datert 10. november 2020.
7 Anbefalingene, side 8, avsnitt 8.
8 Anbefalingene, side 8, avsnitt 9.
9 Anbefalingene, side 9, avsnitt 14.
10 Personvernforordningen artikkel 45.
11 Personvernforordningen artikkel 46.
12 Anbefalingene, side 11, avsnitt 21.
13 Anbefalingene, side 12, avsnitt 28.
14 Anbefalingene, side 12, avsnitt 30.
15 Anbefalingene, side 38, vedlegg 3.
16 Anbefalingene, side 14, avsnitt 42.
17 Anbefalingene, side 14, avsnitt 43.
18 Anbefalingene, side 15, avsnitt 45.
19 Anbefalingene, side 15, avsnitt 47.
20 Anbefalingene, side 17, avsnitt 55.
21 Anbefalingene, side 18, avsnitt 60.
22 Anbefalingene, side 18, avsnitt 62.
23 Anbefalingene, side 19, avsnitt 63.

4 Betraktninger om Anbefalingene

Etter vårt skjønn er en tilnærming der man ser vekk fra en risikobasert analyse med grunnlag blant annet i sannsynlighet, vanskelig å forene med prinsipper og tilnærminger som ellers understøtter personvernforordningen, som redegjort i punkt 7 under. Det er dermed vanskelig å se at vurderingen som skal gjøres i forbindelse med overføring av opplysninger til tredjeland skal være unntatt fra en vurdering av sannsynlighet for at dette tredjelands myndigheter vil søke, eller har mulighet til å få tilgang til opplysningene.

Personvernrådets uttalelse om ikke å trekke inn «subjektive» vurderinger om tredjelandets myndigheter modereres noe ved at Personvernrådet uttaler at virksomheter kan legge vekt på opplysninger innhentet fra andre kilder, som for eksempel rapporterte hendelser, praksis og rettslige myndigheter.[24] I bilag 3 til anbefalingen har Personvernrådet listet opp mulige informasjonskilder til vurdering av et tredjeland. Det fremgår her at rapporter fra akademiske institusjoner og samfunnsorganisasjoner, herunder for eksempel ikke-statlige organisasjoner og bransjeorganisasjoner, kan vektlegges. Dersom en rapport fra slik organisasjon viser at et tredjeland sikrer et tilstrekkelig godt personvern i tråd med EU-standarder, så vil altså dette kunne vektlegges når overføringsmekanismens effektivt skal vurderes i trinn 3.

Det kan dermed argumenteres for at Personvernrådet ikke stenger helt for at en virksomhet kan vurdere sannsynligheten for at et tredjelands myndigheter vil få tilgang på personopplysninger, men at en slik vurdering må basere seg på «objektive» kilder. For en virksomhet som står i en situasjon hvor hverken offentlig regelverk i tredjeland eller slike rapporter er tilgjengelig, vil det imidlertid være relevant å basere seg på en sannsynlighetsvurdering. Det er dermed påfallende at Personvernrådet avviser at en «subjektiv» vurdering kan legges til grunn i slike tilfeller.

Uttalelsen om «subjektive» vurderinger gir også rom for tvil og forvirring når anbefalingene i trinn 4 legger opp til at dataeksportør skal gjøre en «case-by-case»-vurdering av hvilke ytterligere tiltak som sikrer tilstrekkelig nivå av sikkerhet.[25] I dette trinn trekkes det ikke en klar grense mot «subjektive» vurderinger.

> Personvernrådets uttalelse om ikke å trekke inn «subjektive» vurderinger om tredjelandets myndigheter modereres noe ved at Personvernrådet uttaler at virksomheter kan legge vekt på opplysninger innhentet fra andre kilder, som for eksempel rapporterte hendelser, praksis og rettslige myndigheter.

Personvernrådet påpeker som nevnt at ytterligere tiltak i trinn 4 kan være av kontraktsmessig, teknisk eller organisatorisk art.[26] Samtidig fremholder Personvernrådet at kontraktsmessige og organisatoriske tiltak, hvorav sistnevnte gjerne inneholder risikovurderinger, som regel ikke alene vil være tilstrekkelige tiltak.[27]

5 Hva sier Schrems II om vurdering av risiko?

EU-domstolen uttalte om artikkel 46 nr. 1 og nr. 2 at overføringer som er underlagt SCC må:

> «*take into consideration both the contractual clauses agreed […] and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country*».[28]

Uttalelsen trekker i retning av at EU-domstolen legger opp til en helhetlig vurdering av rettssystemet i tredjelandet. Dette underbygges av domstolens uttalelse senere i dommen, hvor det fremgår at ettersom SCC ikke kan gi garantier for personvernet utover av ren kontraktsrettslig karakter, så kan det være nødvendig «*depending on the prevailing position in a particular third country, the adoption of supplementary measures […] in order to ensure compliance with that level of protection*».[29]

Igjen synes EU-domstolen å legge opp til en helhetlig vurdering av den gjeldende situasjonen i tredjelandet. Endelig vises det til domstolens uttalelse om at ettersom SCC ikke kan forplikte tredjeland myndigheter, så vil gyldigheten av SCC være avhengig av at det inkorporeres virkningsfulle tiltak «*that make it possible, in practice, to ensure compliance with the level of protection required by EU law*.» [Vår understrekning][30]

De ovennevnte uttalelsene legger opp til at dataeksportør må foreta en konkret vurdering av hvilke tiltak som er nødvendige for å sikre et tilstrekkelig nivå av beskyttelse for opplysningene som overføres til tredjeland. Vurderingen må ta inn over seg «*the relevant aspects of the legal system of that third country*», avhengig av «*the prevailing position in a particular third country*» som gjør det mulig «in

24 Anbefalingene, side 15, avsnitt 42.

25 Anbefalingene, side 15, avsnitt 46.
26 Anbefalingene, side 15, avsnitt 47.
27 Anbefalingene, side 17, avsnitt 48.

28 *Schrems II*, avsnitt 105.
29 *Schrems II*, avsnitt 133.
30 *Schrems II*, avsnitt 137.

practice» å sikre tilstrekkelig beskyttelse. Uttalelsene trekker etter vår vurdering klart i retning av at EU-domstolen har lagt opp en helhetlig vurdering hvor alle relevante forhold i tredjelandet må hensyntas, jf. også punkt 7 under.

EU-domstolens uttalelser kan etter vårt syn ikke sies å trekke en grense mot «subjektive» vurderinger i tredjelandet. Tvert imot pålegges dataeksportør en utstrakt plikt til å vurdere alle relevante forhold i et tredjeland før opplysninger kan overføre dit. Dataeksportør skal primært legge vekt på offentlig tilgjengelig lovgivning i tredjelandet. Er slik lovgiving imidlertid ikke offentlig tilgjengelig, kan det være både en rett og en plikt etter *Schrems II* å vurdere tredjelandet i sin helhet og foreta en konkret vurdering av eventuelle sikkerhetstiltak på denne bakgrunn.

6 Uttalelser fra EU-kommisjonen og Personvernrådet

I etterkant av *Schrems II*, har EU-kommisjonen utformet forslag til nye SCC i EU for overføring av personopplysninger til tredjeland.[31]

I forslaget er det inntatt en bestemmelse hvor partene i SCC erklærer at de ikke har grunn til å tro at lovgivningen i tredjelandet vil forhindre dataimportøren fra å oppfylle kravene i SCC. Det fremgår her at partene i den anledning har tatt i betraktning «*any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred*».[32] [Vår understrekning]

Bestemmelsen uttrykker klart at det skal gjøres en vurdering på bakgrunn av praktisk erfaring med tredjelandet. EU-kommisjonen kan dermed sies å legge opp til en «subjektiv» vurdering av tredjelandets myndigheter.

Personvernrådet og det europeiske datatilsynet har inngitt en *Joint Opinion* på EU-kommisjonens forslag til nye SCC.[33] Det fremgår her at vurdering av lovgivning og praksis i tredjelandet i relasjon til en konkret overføring av opplysninger «*should be based on objective factors regardless of the likelihood of access to the personal data*.»[34]

Det blir her referert til uttalelsene i anbefalingene om at det ikke skal vektlegges «subjektive» faktorer.[35] Videre fremgår det at «*the EDPB and the EDPS also recall that in the Schrems II ruling, the CJEU did not refer to any subjective factor such as the likelihood of access, for instance*.»[36]

Dersom lovgivningen i tredjelandet i seg selv gir myndighetene tilgang på opplysningene skal det, etter Personvernrådets mening, vurderes som en mulighet uten at det legges vekt på praktisk erfaring, slik EU-kommisjonen la opp til.[37] På den bakgrunn foreslår Personvernrådet og det europeiske datatilsyn at setningen om praktisk erfaring fjernes fra EU-kommisjonens nye SCC.

Etter vårt skjønn, uttrykker uttalelsen fra Personvernrådet og Det europeiske datatilsynet en for snever tolkning av dommen – og tar ikke til seg helhetsvurderingen fra *Schrems II*. EU-domstolen uttalte at det måtte legges vekt på relevante deler av tredjelandets rettssystem, den gjeldende situasjonen i tredjelandet og hva som i praksis sikrer tilstrekkelig sikkerhetsnivå for opplysningene. Det ble ikke foretatt en avgrensing mot «subjektive» vurderinger i den anledning.

7 Anbefalingene og forholdet til andre kilder

Tilnærmingen om at det skal sees vekk fra reell risiko synes å være et brudd med hvordan risiko vurderes ut fra andre forpliktelser.

For det første er fokuset på risiko et av de mest sentrale elementene som skiller forordningen fra det gamle personverndirektivet: Mens det gamle direktivet i stor grad benyttet forhåndskontroll og tilsynsgodkjenning, er det den behandlingsansvarliges risikovurderinger som nå benyttes som den sentrale mekanismen for å etterleve forordningens krav.[38] Christopher Kuner bemerker at nye forpliktelser til å vurdere personvernkonsekvenser og identifisere risiko, er del av et skifte fra «paper-based bureaucratic requirements» og over til «compliance in practice».[39]

I forordningen artikkel 24 og 32 slås det fast at egnet sikkerhet ved behandling av personopplysninger skal fastsettes ut fra en helhetlig vurdering, hvor blant annet risikoen av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter skal vurderes. Også plikten til å vurdere personvernkonsekvenser i artikkel 35 er her sentral.[40] Artikkel 29-gruppens retningslinjer for vurdering av personvernkonsekvenser utdyper bestemmelsene og understreker

31 Kan lastes ned her: *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PI_COM:Ares(2020)6654686&rid=1*

32 Ibid, klausul 2, bokstav b, (I).

33 *EDPB – EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries.*

34 Ibid, avsnitt 86.

35 Anbefalingene, side 14, avsnitt 42.

36 Ibid, avsnitt 87.

37 Ibid, avsnitt 87.

38 Maria Eduarda Gonçalves, *The risk-based approach under the new EU data protection regulation: a critical perspective, Journal of Risk Research*, 2020, s. 139-152. Som Eduarda Gonçalves nevner i artikkelens note 7: «Note that the term "risk" appears 76 times in the text of the Regulation, whereas it appeared 8 times in the text of the Directive.» Se også fortalepunkt 89.

39 Christopher Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*. I: Bloomberg BNA Privacy and Security Law Report, (2012) s. 1.

40 Forordningens fortalepunkter 89-91.

«den risikobaserte tilnærmingen som er innarbeidet av GDPR».[41]

Samtidig er det naturligvis også andre elementer ved GDPR som utgjør bærende hensyn, blant annet personvernprinsippene og de registrertes rettigheter. Tilsynelatende vektlegger Personvernrådet en svært snever, rettighetsbasert tilnærming til forordningens regulering – som vi oppfatter som vanskelig å forene med andre tungtveiende kilder.[42]

Centre for Information Policy Leadership deler vår vurdering, og mener det bør gjennomføres en vurdering av de faktiske forhold, med grunnlag i sannsynligheten for ulemper (som at myndighetene får tak i informasjonen), når opplysninger skal sendes ut av EU/EØS. Senteret viser til at et kjerneelement må være en «*data transfer risk assessment*» som ledd i «*identifying potential risks associated with an organisation's data transfers and identifying mitigating measures commensurate with those risks*». Dette bør skje «*in light of the risk-based approach enshrined in the GDPR*», noe om anses å være mer i samsvar med andre uttalelser fra Artikkel 29-gruppa og Personvernrådet.[43] Dette må håndteres ved at man ser på «*whether such transfers could result in a high likelihood and severity of risk of harm, for example due to governmental access to that data*».[44]

For det annet er Personvernrådets tilnærming også klart i strid med hvordan også amerikanske myndigheter oppfatter EU-domstolens avgjørelse. I et White Paper[45] utformet av det amerikanske handelsdepartementet, justisdepartementet og etterretningsdirektøren påpekes det at for mange virksomheter er sjansen for myndighetsinnsyn «*unlikely to arise because the data they handle is of no interest to the U.S. intelligence community.*» De amerikanske myndighetsorganene viser også til at «*the overwhelming majority of companies have never received orders to disclose data under FISA 702 […].*»[46] Det samme dokumentet understreker også at en teoretisk mulighet til å få hånd om informasjonen neppe kan ha betydning.[47]

For det tredje er oppfatningen i anbefalingene vanskelig å forene med formuleringer i EU-kommisjonens utkast til SCC for overføring til tredjestater,[48] som skal avbøte utilstrekkelig lovgivning. Det fremgår her at partene ved vurdering av egnet sikkerhetsnivå skal ta hensyn til «the risks involved in the processing, the nature of the personal data and the nature, scope, context and purposes of processing».[49]

For det fjerde synes det også som om anbefalingene i seg selv mangler konsistens, jf. også vårt punkt 4 over: Selv om det i trinn 3 er fastslått at objektive faktorer skal vektlegges, er det i trinn 4 om ytterligere tiltak tilsynelatende tillatt å vektlegge mer subjektive faktorer, idet det legges opp til konkret helhetsvurdering i hver enkelt sak om ytterligere tiltak anses som effektive.[50] En reell helhetsvurdering av om tiltakene er effektive, bør ta hensyn til sannsynligheten for at tredjelands myndigheter får tilgang på opplysningene.

> Teoretikeren W. Kuan Hon påpeker at en dataeksportør vanskelig kan verifisere om et tredjelands lovgivning gir et sikkerhetsnivå for opplysningene som tilsvarer nivået i EØS.

For det femte er det i juridisk teori trukket frem at kravene i EU til overføring av opplysninger til tredjeland bør se på den reelle risikoen for at myndighetene får tilgang til opplysningene. Zwillinger, Weisz og Parsons påpeker blant annet at myndighetene «*only uses Section 702 where there is a repeated need for multitarget collection without the inefficiency of going to the FISA court for individual surveillance orders via a procedure that has greater judicial oversight.*» Forfatterne viser også til da Snowdens informasjonslekkasjer skjedde, var

41 Artikkel 29-gruppa, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679"*, side 5.

42 Debatten om forholdet mellom en risikobasert og en rettighetsbasert personvernbeskyttelse er gammel og komplisert diskusjoner, som er redegjort for blant annet i Raphaël Gellerts nye bok, *The Risk-Based Approach to Data Protection* (2020).

43 Senteret mener det er overføring til tredjeland ikke automatisk skal innebære høy risiko i henhold til forordningen, og antar det er «[c]onsistent with the EDPB guidelines on DPIAs and high risk processing (WP 248) …».

44 The Centre for Information Policy Leadership, *White Paper, A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision*, (2020) s. 8.

45 The White Paper ("Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II")

46 Se side 8 i *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, som er utgitt av Department of Commerce, Department of Justice og Office of the Director of National Intelligence.

47 Ibid, side 3.

48 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf

49 Klausul 1.5(a) ("Module One"), klausul 1.6 ("Module Two" og "Module Three") og klausul 1.2 ("Module Four"). Materialet kan lastes ned her: *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PI_COM:Ares(2020)6654686&rid=1*

50 Anbefalingene, side 15, avsnitt 46.

det rapportert om at færre enn ti selskaper hadde mottatt «702-ordrer» om informasjonsutlevering. De viste derfor til at problemstillingen i praksis kun var aktuell for an «*insignificant percentage of the more than 5,300 companies that may be moving from Privacy Shield to SCCs*». Konklusjonen var derfor at nær sagt alle virksomheter «*could promise that they have received no process under 702, and they can keep making that promise unless and until they receive a directive.*»[51]

Teoretikeren W. Kuan Hon påpeker at en dataeksportør vanskelig kan verifisere om et tredjelands lovgivning gir et sikkerhetsnivå for opplysningene som tilsvarer nivået i EØS. Dataeksportøren må heller basere seg på ytterligere tiltak av teknisk eller organisatorisk karakter, som i praksis vil medføre at myndighetene ikke kan hente ut informasjonen. Dette vil «*make it a lot more difficult for intelligence agencies – admittedly EU as well as third country – to obtain intelligible, usable data*».[52]

8 Anbefalingene er et steg tilbake for fornuftig dataflyt

Anbefalingene fra Personvernrådet utgjør etter vårt syn et avvik fra personvernforordningens system hvor behandlingsansvarlige i stor grad selv vurderer risiko ved behandling av personopplysninger og hvilke tiltak som danner tilstrekkelig beskyttelse av opplysningene.

> En økt bruk av disse unntaksbestemmelsene bør unngås, fordi det vil gi vesentlig mindre sikkerhet for personopplysninger når informasjonen er overført.

Det kan være vanskelig å skaffe oversikt over et tredjelands lovgivning og praksis i tråd med anbefalingenes trinn 3. Når slik oversikt ikke er offentlig tilgjengelig, blir det ytterligere et hinder for dataeksportøren når det ikke kan foretas en helhetlig risikovurdering som ledd i overføring til tredjeland. Anbefalingene legger opp til at tekniske tiltak i de fleste tilfeller utgjør de eneste tilstrekkelige tiltak. Dataeksportører kan i realiteten bli pålagt sterk kryptering av all overført data.

Anbefalingene kan være uoverkommelig for mindre selskaper med begrensede ressurser. Store aktører innen data og telekom vil ha de nødvendige ressurser til å få tilgang til og vurdere tredjelands lovgivning og praksis. Konsekvensen er at anbefalingene vil kunne føre til mindre forretningsvirksomhet og handel til land som USA – som selskaper og myndigheter i EU driver utstrakt forretning og samarbeid med, og som det er uheldig om blir «stengt ute» fra digital kommunikasjon med EU. Bruk av digitale tjenester og kommunikasjon har økt drastisk under smitteverntiltakene i hele den vestlige verden under covid-19 pandemien. Det er ingen grunn til å tro at det vil bli mindre etterspørsel etter denne type tjenester og kommunikasjon når økonomien i flere land må gjenreises etter covid-19-nedstenging.

Når anbefalingene oppleves som uoverkommelig av flere, er det en risiko for at flere aktører baserer seg på overføring av opplysninger til tredjeland på bakgrunn av unntak for særlige situasjoner i personvernforordningen artikkel 49, blant annet samtykke. En økt bruk av disse unntaksbestemmelsene bør unngås, fordi det vil gi vesentlig mindre sikkerhet for personopplysninger når informasjonen er overført.

Vi er derfor enige med Theodore Christakis, som påpeker at: «*The rejection of the risk-based approach by the EDPB is odd.*»[53]

Ove A. Vanebo er senioradvokat i Kluge Advokatfirma.
Marianne Gjerstad er senioradvokat i Kluge Advokatfirma.

51 Marc Zwillinger, Mason Weisz og Kandi Parsons, Supplementing SCCs to solve surveillance shortfalls. *https://iapp.org/news/a/supplementing-sccs-to-solve-surveillance-shortfalls/*

52 Dr. W Kuan Hon, "Schrems II: data localization, encryption & the bigger picture", *https://blog.kuan0.com/2020/07/schrems-ii-data-localization-encryption.html.*

53 Theodore Christakis, *"Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 2)*, datert 16. november 2020: *https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/*

SSA-SKY er forventet å foreligge i mars 2021 – hvorfor trenger vi den?

Av Vemund Sande og Fredrik Lilleaas Ellingsen

Vemund Sande

Fredrik Lilleaas Ellingsen

Direktoratet for forvaltning og økonomistyrings (Difi) nye standardavtale for kjøp av skytjenester (SSA-SKY) ble sendt ut på høring 10. juli 2020. Difi hadde håpet å få avtalen klar før jul samme år, men tilbakemeldingene var såpass omfattende at ferdigstillelsen måtte utsettes til mars 2021. Utformingen av nye SSA-SKY er med andre ord et tema som engasjerer. Mange er nok av den oppfatning at behovet for en velfungerende avtale for kjøp av forskjellige skytjenester er stort, og at dagens standardavtaler ikke dekker dette på en tilstrekkelig måte. Samtidig er det mange hensyn som skal balanseres i den nye avtalen. Nedenfor skal vi se nærmere på noe av grunnen til at det er et behov for en ny avtale for kjøp av skytjenester. Det presiseres at endelig versjon av SSA-SKY ikke forelå da denne artikkelen ble skrevet.

Markedet har de senere årene endret seg i retning av at leverandørene tilbyr tjenester i større grad enn det som var tilfelle tidligere da kundene eksempelvis kjøpte maskinvare, programvare, implementeringstjenester og deretter vedlikeholds- og eventuelt driftstjenester, og hvor kunden selv langt på vei ble sittende igjen med ansvar og risiko for at det de kjøpte fungerte som en helhet. Stadig flere leverandører kombinerer flere av disse elementene og tilbyr mer helhetlige tjenester, og da gjerne i form av skytjenester. Disse skytjenestene er i økende grad standardiserte, og leverandøren går langt i å kreve at kunder aksepterer samme kontraktsvilkår.

> Dagens standardavtale om løpende tjenestekjøp (SSA-L), som SSA-SKY skal være et alternativ til, er beregnet på anskaffelser av standard skytjenester med liten grad av individuelle tilpasninger.

Dagens standardavtale om løpende tjenestekjøp (SSA-L), som SSA-SKY skal være et alternativ til, er beregnet på anskaffelser av standard skytjenester med liten grad av individuelle tilpasninger. Avtalen tar videre sikte på å være en slags hybrid bestående av leverandørens standardvilkår og mer tradisjonelle «SSA-vilkår» ved at leverandørens standardvilkår inngår som vedlegg til bilag 9. Som regel vil det være en del kolliderende vilkår i SSA-L og leverandørens standardvilkår. Dette er naturlig, da begge skal være komplette avtaleverk. Blant annet inneholder sistnevnte ofte ansvarsfraskrivelser som går langt utover det som følger av SSA-Ls standardtekst. Utgangspunktet ved slik motstrid er at den generelle avtaleteksten, samt bilag 1, 2, 7 og 8, skal ha forrang. I realiteten vil forrangsproblematikken sjeldent komme på spissen, da man i praksis velger å tolke seg rundt en eventuell motstrid. Dette er i seg selv en krevende øvelse, som strengt tatt ikke burde ha vært

nødvendig (i alle fall ikke i såpass utstrakt grad).

> SSA-SKY skal i større grad enn SSA-L være tilpasset dagens markedssituasjon og imøtekomme behovet for økt fleksibilitet, og forholdet til leverandørens standard kontraktsvilkår skal forhåpentligvis løses på en bedre måte.

Situasjonen med kolliderende/avvikende vilkår innebærer at den leverandøren (systemintegratoren) som signerer SSA-L med kunden ender opp som et mellomledd som påtar seg ansvar og risiko det ikke vil være dekning for i leverandørens standardvilkår (kunde – systemintegrator – leverandør). Dette er forsøkt delvis avhjulpet i SSA-L punkt 2.2 som ber systemintegratoren beskrive hvilke forpliktelser leverandørens standardvilkår pålegger kunden og hvilke ansvarsbegrensninger tredjepart forbeholder seg. Dette kan være en svært krevende øvelse med et lite forutsigbart resultat. Oppsettet skaper spesielt store utfordringer for kunder som er underlagt regler for offentlige anskaffelser.

Oppsettet beskrevet ovenfor medfører at systemintegratoren blir sittende med en betydelig risiko som følge av delta mellom SSA-L og leverandørens standardvilkår. Denne risikoen vil systemintegratoren naturlig nok ta seg betalt for, noe som resulterer i en merkostnad for kunden som langt på vei kunne vært unngått (eller i alle fall redusert) ved bruk av en avtale som hensyntok dagens markedssituasjon.

SSA-SKY skal i større grad enn SSA-L være tilpasset dagens markedssituasjon og imøtekomme behovet for økt fleksibilitet, og forholdet til leverandørens standard kontraktsvilkår skal forhåpentligvis løses på en bedre måte. Avtalen skal også kunne benyttes for sammensatte leveransemodeller av forskjellige kompleksitet, slik at man slipper å inngå forskjellige SSAer for forskjellige deler av leveransen. Bruk av flere SSAer er ofte nødvendig ved kjøp av skytjenester med en ikke-ubetydelig grad av individuelle tilpasninger slik situasjonen er i dag. Hvorvidt SSA-SKY løser problemstillingene nevnt ovenfor på en hensiktsmessig måte gjenstår å se når endelig avtale foreligger.

Vemund Sande er advokat og Fredrik Lilleaas Ellingsen er senioradvokat i avdelingen for HITEK i Advokatfirmaet Selmer, Oslo.

Fra konsesjon til Schrems II – eksport av personopplysninger i det 21. århundre

Av Kristian Foss

Overføring av personopplysninger til utlandet har gått fra å være en «usexy» disiplin på et «usexy» rettsområde til et spørsmål som havner på styrerommene i store konsern. Data har blitt blodet som flyter i årene til nesten alle typer virksomheter, og for noen, det nye gullet. Reglene om overføring bestemmer hvilke tjenester som kan brukes, og legger dermed føringer for utviklingshastighet, kostnader og forretningsmodeller. Det vil si forhold som kan bestemme om en virksomhet vinner eller taper.

Vi har gått fra krav om konsesjon, via trygghetsfiksjonen Safe Harbor til Schrems II-dommen av 16. juli 2020. Hvilke krefter er det som driver regelutviklingen, hvilken betydning får utviklingen for dataeksportørene og hva kan vi forvente oss fremover?

I det følgende vil vi se litt på historikken, før vi går mer detaljert inn i dagens situasjon. Basert på funnene gjør vi to analyser i et forsøk på å se hva som kan vente oss i årene, og kanskje tiårene, som kommer.

På vei inn i den fjerde personvernbølgen

Utviklingen av personvernet har gått i bølger. Hoveddriverne har vært ære, ideologi og teknologi – og naturligvis et ønske om privatliv.

Den **første bølgen** var preget av fragmentarisk og ulovfestet regelutvikling. Den begynte med beskyttelse av ære. Frostatingsloven (rundt år 1200) forbød å dikte om andre, selv om diktet var positivt. Æren skulle beskyttes. Kong Christians IVs lov 1604 tillot diktningen, bare den ikke var negativ. Fremdeles ære, men også en reaksjon på trykkekunsten – en teknologi.

Kristian Foss

Da den tyske landsfaderen Otto von Bismarck døde, ble han snikfotografert i sottesengen. Da ble det bråk. Retten besluttet i 1898 at fotoplatene skulle ødelegges (Bismarck-dommen). Igjen en reaksjon på ny teknologi – fotografering – og trolig ære, eller i det minste et ønske om vern av privatlivet. Og et tidlig eksempel på manglende etterlevelse. Fotografiet overlevde, som du ser.

Dommen ga også støtet til vern av retten til eget bilde. I Norge ble retten til eget bilde beskyttet i fotografiloven av 1909.

Privatlivets fred fikk vern i straffeloven av 1902. Telefonsjikanedommen ble avsagt i 1952. Teknologien var telefonen. Denne blandingen av snevre regler og rettspraksis preget den første, fragmentariske bølgen. Følgende sentrale dommer bør i den forbindelse nevnes:

- Aars-dommen 1896 om vern av familienavn
- To mistenkelige personer 1952 om nektelse av å vise film om et lensmannsmord
- Sykejournaldommen 1977 om tilgang til egen sykejournal
- Gatekjøkken-kjennelsen 1991 om vern mot overvåking på jobb
- Fotobokskjennelsen 1990 om bruk av bilde til nytt formål

Den **andre bølgen** kunne vært døpt menneskerettighetsbølgen. Bølgen var en konsekvens av det økte fokuset på menneskerettigheter i kjølvannet av grusomhetene under den annen verdenskrig. FNs verdenserklæring om menneskerettigheter ble på denne bakgrunn vedtatt i 1948. En av rettighetene var retten til privatliv (artikkel 12). Rettigheten ble også inntatt i Den europeiske menneskerettighetskonvensjonen av 1950 (artikkel 8).

Det er på menneskerettighetenes vern av privatliv det moderne personvernet hviler. Det fremgår ikke minst av Schrems II-dommen, hvor retten i stor grad henviser til EU-charteret om grunnleggende rettigheter artikkel 7 (respekt for privat- og familieliv) og artikkel 8 (beskyttelse av personlige data).

Den **tredje bølgen** kunne vi kalt implementeringsbølgen. I denne bølgen fikk vi lover som skulle gjennomføre og konkretisere menneske-

rettighetenes overordnede vern om privatlivet og kodifisere eksisterende rettspraksis. Dermed skjedde det en implementering av grunnleggende personvernprinsipper. I Norge begynte det med personregisterloven av 1978, en av verdens første generelle personvernlover. EU kom med sitt personverndirektiv i 1995 (95/46/EF), som ledet til vår personopplysningslov av 2000. Menneskerettighetene er gjort til norsk lov gjennom menneskerettsloven og Grunnloven. Grunnloven § 102 verner privatlivet spesielt.

PCen ble lansert av IBM i 1981. Tyngre datamaskiner hadde allerede vært i bruk i statsforvaltningen siden slutten av 1960-tallet. Det var åpenbart at elektronisk behandling av data ville ta over fra papirbaserte arkiv. Men datalinjene var elendige og serverene sto gjerne i skapet. Overføring til utlandet var derfor en liten bekymring.

Likevel var personregisterloven (eller Europarådskonvensjonen om persondatabeskyttelse av 28. januar 1981 som reguleringen bygget på) visjonær nok til å regulere spørsmålet (personregisterloven kap. 9). I henhold til tilhørende forskrift gikk vi fra konsesjonskrav til meldeplikt.

På 1990-tallet dukket såkalte application service provision (ASP) opp – datidens *software as a service* (SaaS). Ikke fleksibelt nok til å kalles sky, men med data lagret et annet sted enn der brukerne satt. Et stort skritt. Internett hadde fantes siden slutten av 1960-tallet, men det var ikke før rundt 1993 at world wide web ble popularisert med den grafiske nettleseren *Mosaic*.

EU-kommisjonen hadde sett hvor det bar, og kom med sitt personverndirektiv i 1995. Da hadde noen europeiske land fremdeles ikke nasjonale personvernlover, i motsetning til Norge.

Den **fjerde bølgen** tok dagens sky- og datadrevne verden innover seg. På 2000-tallet ble datalinjer bedre og billigere. Verdens største skyleverandør Amazon Web Services (AWS) revolusjonerte fra 2004 med sine skytjenester. Facebook kom til samme år. SaaS så dagens lys. Overføring av data over landegrensene gikk fra å være unntaket til å bli normen.

Otto von Bismarck hviler ut

11. september 2001 styrtet to fly inn i hver sin skyskaper i New York. Amerikansk etterretningsvesen var tatt med buksene nede. Reaksjonen var ikke bare USAs angrep på Afghanistan i oktober samme år, men også en oppbygging av digital overvåking verden ikke hadde sett maken til. Amerikanske National Security Agency (NSA) sto i spissen, utrustet med nye penger og en tro på at mer overvåking ville gi mer sikkerhet. Foreign Intelligence Surveillance Act (FISA) og presidentdekret 12 333 ga to sentrale hjemler, som tidligere beskrevet i min artikkel *Vil Bidens overvåkingsstat bli bedre?* (Lov & data, nr. 4/2020 (kortversjon)). Hjemlene gir amerikanske myndigheter blant annet adgang til å gjennomføre masseovervåking utover USAs landegrenser.

Vi stod dermed overfor en overveldende og økende kommersiell bruk av data og skytjenester, kombinert med kraftig økning av statlig etterretning fra USA og andre land. På denne bakgrunnen ble arbeidet med en ny personvernforordning initiert i Europa i 2010. Arbeidet munnet ut i EU-kommisjonens forslag til personvernforordning i 2012. Grunnprinsippene i det tidligere 1995-direktivet ble videreført, men håndhevingsreglene ble kraftig skjerpet.

Det hadde fra omkring 2005 versert rykter og visse avsløringer om omfanget av NSAs overvåking. Men det var ikke før Edward Snowdens avsløringer i 2013 at verden fikk ugjendrivelige bevis og det enorme omfanget ble klart. Avsløringene bidro til at personvernforordningen ble utstyrt med sanksjoner få trodde ville se dagens lys. Brudd på forordningene kunne resultere i sanksjoner på opptil 4 % av årlig konsernomsetning for en virksomhet. Kanskje takket være Snowdens avsløringer, klarte ikke lobbyistene for de store leverandørene å redusere sanksjonsnivået.

Tre klasser av dataimportører

På samme måten som 1995-direktivet (og personopplysningsloven) deler personvernforordningen mot-

tagerne av persondataene (dataimportørene) inn i tre klasser, nemlig:

1. EØS-land
2. Hvitlistede land som «sikrer et tilstrekkelig beskyttelsesnivå»
3. Andre (utrygge) land

EØS-landene (klasse 1) består av i alt 30 EFTA og EU-land, som alle har vedtatt personvernforordningen (pvf) som lov. De hvitlistede landene i klasse 2 omfatter 12 land inkludert Argentina, Israel, New Zealand, Japan, Sveits og Canada (kommersielle organisasjoner). Landene er godkjent som trygge land å overføre personopplysninger til i henhold til adekvansmekanismen omtalt i pvf artikkel 45 (adekvansbeslutninger). Eksport av data til land i klasse 1 og 2 under pfv. artikkel 45 (1) skaper relativt få problemer. Det er likevel på sin plass å minne om at alle de alminnelige kravene til behandling av personopplysninger gjelder, selv om EU-kommisjonen har vurdert landene til å tilby tilstrekkelig beskyttelse for europeiske personopplysninger.

Det store spørsmålet, som vi skal konsentrere oss om her, er hvordan overføring av personopplysninger skal skje til de mindre trygge landene i klasse 3. I den forbindelse står særlig USA og virkningene av Schrems II-dommen fra 16. juli 2020 sentralt.

Fra «Unsafe» Harbor via Privacy Shield til Schrems II

Personverndirektivet av 1995 benyttet som antydet et lignende klassesystem som personvernforordningen. Overføringsgrunnlaget, som skulle sikre tilfredsstillende behandling av personopplysninger i USA, het da Safe Harbor, men var ikke direkte hjemlet i den gamle personopplysningsloven (2000) eller i 1995-direktivet. Det ganske løse rammeverket ble i Schrems I-dommen fra 6. oktober 2015 kjent ugyldig fordi det ikke sikret europeiske borgeres personopplysninger på en tilfredsstillende måte.

Med bortfallet av det mye brukte overføringsgrunnlaget Safe Harbor, startet et lett panisk arbeid med erstatningen. 12. juli 2016 ble EU US Privacy Shield vedtatt som forsvarlig overføringsgrunnlag av EU-kommisjonen. Neste sovepute var på plass. Sammen med en håndfull adekvansbeslutninger ble skjoldet i mai 2018 ansett å gjelde for også personvernforordningen i henhold til pvf. artikkel 46 (2) a. Særlig oppfølgingsregimet ble skjerpet i forhold til Safe Harbor, men fremdeles baserte Privacy Shield seg på selvsertifisering.

Det som imidlertid ble spikeren i kisten for Privacy Shield som hjemmel for overføring, var USAs inngripende etterretningsregler og -praksis kombinert med manglende rettsmidler for den overvåkede til å angripe behandlingen overvåkingen innebar. EU-domstolen trakk i Schrems II-dommen som nevnt særlig frem FISA artikkel 702 og presidentdekret 12 333. Masseovervåking uten individuell innretting skjer under for eksempel PRISM og UPSTREAM-programmene (premiss 178 til 180). Rettsmidler mot ulovlig overvåking finnes heller ikke (premiss 181 og 182). Ombudsmannsordningen i skjoldet kan ikke avhjelpe disse svakhetene (premiss 190). Svakhetene med ordningen og tilstanden i USA medførte at Privacy Shield ikke etterlevde EU-charteret og forordningen (premiss 198 til 201). (For dem som vil ha en levende beskrivelse av hvordan overvåkingen fant sted anbefales Oliver Stones fascinerende film Snowden (2016) og Glenn Greenwalds bok No Place to Hide (2013)).

Retten til å motsette seg vilkårlig overvåking ligger i USAs fjerde grunnlovstillegg. Dessverre for oss europeere gjelder vernet bare amerikanske innbyggere. Til sammenligning verner EU-charteret artikkel 7 og artikkel 8 alle («everyone»), det vil si også ikke-europeere. EU-domstolen kom derfor til at rettstilstanden i USA ikke ga europeere et tilsvarende vern som de nøt i Europa.

Schrems II-dommen brakte dermed rettstilstanden nærmere det de fleste allerede hadde skjønt; persondata behandlet i USA ble bare ikledd et slør av forsvarlighet med Privacy Shield. Allerede ved unnfangelsen av Privacy Shield ble dens svakheter kritisert, og det var bare et tidsspørsmål før Maximilian Schrems eller andre ville utfordre dette fernisset av et vern.

Standardbestemmelsene slapp unna, men...

Det andre mye brukte overføringsgrunnlaget for eksport av persondata til USA er de såkalte standardbestemmelsene (*Eng.* standard contractual clauses – SCC). Bestemmelsene gir de registrerte en rekke rettigheter overfor dataimportøren.

Det var derfor en lettelse for mange da EU-kommisjonens godkjenninger av standardbestemmelsene fra 2001 (2001/487/EF) og 2010 (2010/87/EF) som grunnlag for eksport av persondata ble opprettholdt i Schrems II-dommen. Opprettholdelsen skjedde på tross av at overføring i henhold til bestemmelsene lider av mange av de samme svakhetene som Privacy Shield (premiss 149). Retten fremhever imidlertid at behandlingsansvarlig også ved bruk av standardbestemmelsene er pliktig til å gjøre en konkret («case by case») vurdering (premiss 134, jf. premiss 95 og forordningens fortalepunkt 108). Sikringstiltakene fra retningslinjene vi skal gå igjennom under, må derfor iverksettes også ved bruk av standardbestemmelsene.

Hva med CLOUD Act?

Som følge av vanskelighetene amerikanske FBI hadde med å tvinge Microsoft til å gi fra seg epostdata lagret i Irland i en narkotikasak, ble CLOUD Act (Clarifying Lawful Overseas Use of Data Act) vedtatt (Hotmail-saken). Loven økte rekke-

vidden av Stored Communications Act (SCA) fra 1986, slik at amerikanske selskaper måtte etterleve tilgangskjennelser avsagt i medhold av SCA. CLOUD Act gjorde at Microsofts Hotmail-sak, som da sto for Høyesterett, ble trukket og dataene ble utlevert.

Med SCAs økte rekkevidde skulle man kanskje tro EU-domstolen ville begrunne Schrems II-dommen også med vedtakelsen av CLOUD Act. Det gjorde den ikke. Grunnen er at CLOUD Act gir amerikanske justismyndigheter hjemmel til å gjøre beslag i data lagret på servere kontrollert av amerikanske selskaper bare etter særlig kjennelse fra en domstol. Det dreier seg da heller ikke om masseinnsamling av persondata. I slike tilfeller kan personen som begjæringen om tilgang retter seg mot, bestride denne. Dermed har datasubjektet det rettsmiddelet EU-domstolen savnet ved det fjerde grunnlovstillegget, FISA artikkel 702 og presidentdekret 12 333.

Hvordan eksportere til «utrygge» land (som USA)?

EU-domstolens budskap var at Privacy Shield og de andre avtalebaserte grunnlagene i pvf. artikkel 46 (2) ikke forpliktet importlandets myndigheter og dermed ikke sikrer europeiske borgeres grunnleggende personvernrettigheter. Botemiddelet var å iverksette «supplerende tiltak» og «tilleggssikringer» (premiss 133 og 134). Domstolen opplyste imidlertid ikke hva disse kunne bestå i.

Schrems II-dommen betyr dermed at ganske vanskelige vurderinger må gjøres. For å forenkle denne vurderingen utstedte Det europeiske personvernrådet (EDPB) 10. november 2020 retningslinjer for dataeksport (anbefaling 01/2020).

Personvernrådet innleder sine anbefalinger om eksport av persondata med at Schrems II-dommen minner oss om at vernenivået i EØS må «reise med dataene hvor enn de drar». Rettstilstanden og praksis i importlandet må derfor vurderes, alt i lys av det generelle forsvarlighetskravet (pvf. artikkel 5 (2)).

Under ser du retningslinjenes **seks steg** med kommentarer.

Se ytterligere detaljer i veiledningens pkt. 2 og bilag 2 med eksempler på konkrete tiltak for ulike situasjoner.

Vurderingene som gjøres i de ulike stegene må dokumenteres for å kunne påvise etterlevelse (pvf. artikkel 5 (2) og 24 (1)).

Figuren under viser strukturen i den vurderingen som må gjøres gjennom de seks stegene.

Hvilke overføringsgrunnlag har vi nå?

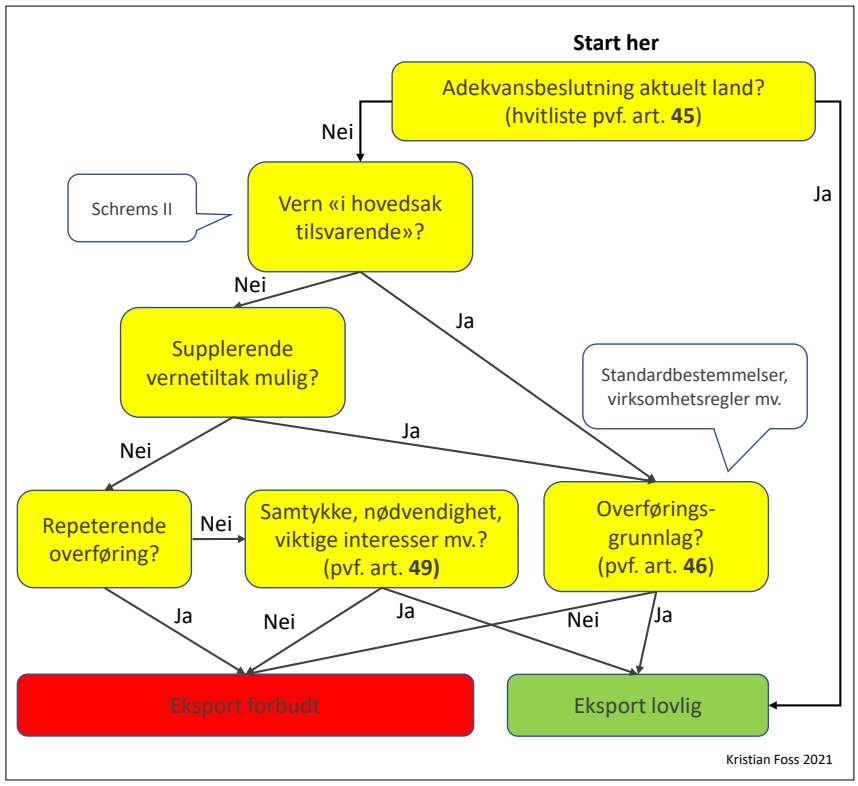
Med Privacy Shield kjent ugyldig, står vi under personvernforordningen igjen med disse overføringsgrunnlagene:

a) et eventuelt nytt **rettslig instrument** mellom offentlige myndigheter, men med bedre sikringer enn det EU-domstolen mente Privacy Shield kunne tilby (pvf. 45),
b) **EUs standardbestemmelser** (pfv. 46 (2) c)
c) **bindende konsernregler** (pfv. 46 (2) b)
d) **adferdsnormer** (pfv. 46 (2) e)
e) **serfifiseringsmekanismer** (pfv. 46 (2) f)
f) **spesialavtale** godkjent av datatilsynet (46 (3) a)
g) **spesialordning** mellom offentlige organer (46 (3) b)
h) **særlige situasjoner** (pvf. artikkel 49)

Schrems II-dommen er relevant for alle de *kontraktuelt* baserte grunnlagene i nevnt i bokstav b) til g) fordi partene ikke kan binde offentlige myndigheter i importlandene. Dermed lider i prinsippet alle avtalebaserte grunnlag av samme svakheter som Privacy Shield.

Utkastet til nye standardbestemmelser

Siden standardbestemmelsene utgjør det mest praktiske overføringsgrunnlaget etter Privacy Shield falt bort som overføringsgrunnlag til USA, fremla EU-kommisjonen 12. november 2020 et forslag til nye



Forenklet beslutningsdiagram basert på Schrems II-dommen, retningslinjer og pvf

Steg	Vurdering og tiltak
1. Kartlegg	Skaff oversikt over hvilke data som blir overført hvor og til hvem. Vurder om alle data overføres. Hvor lenge vil dataene bli behandlet? Dataminimer (så lite data som mulig, behandlet så kort som mulig). Overføres data videre? Husk at fjerntilgang anses som overføring. Kartleggingen er også en del av den generelle protokolleringen som uansett skal skje etter pvf. artikkel 30 (1) e. Kartlegging må skje før overføring skjer.
2. Bekreft grunnlaget for overføringen	Det finnes tre hovedgrunnlag: **1. Adekvansbeslutning** (hvitliste). Er importlandet for data omfattet av adekvansbeslutning etter pvf. artikkel 45 vil overføringen automatisk anses forsvarlig og slik oppfylle pvf. artikkel 44. **2. Kontraktuelt**. Står importlandet ikke på hvitlisten, må overføringsgrunnlagene i pvf. artikkel 46 vurderes – standard kontraktsbestemmelser, – konsernregler, – adferdsnormer mv – sertifiseringer – ad hoc kontraktsbestemmelser for rutinepregede overføringer. Slik etableres et *kontraktuelt* vern. **3. Nødventil**. Unntaksvise overføringer kan hjemles i pvf. 49. Se under for mer om disse.
3. Vurder rettslig tilstand i importlandet	Fordi målet er fortsatt vern av personopplysningene, må rettstilstanden (lov og praksis) i det importerende tredjelandet vurderes i lys av valgt overføringsgrunnlag i steg 2. Vurderingstemaer: – **grad av overvåking,** – **krav om myndighetstilgang til data,** – **regler som kan redusere effekten av sikringstiltak, generell rettssikkerhet (som påvirker rettsmidler), og** – **om personvernlovgivning i landet finnes**. Vurderingen skal gjøres i samarbeid med dataimportøren. I praksis kan dette gjøres ved å stille dataimportøren spørsmål. Om det ikke finnes gode offentlige tilgjengelige kilder, bør lokal bistand søkes i importlandet. Om tid eller økonomi ikke tillater lokal bistand, må dataeksportøren gjøre en best mulig vurdering basert på tilgjengelig informasjon. Vurderingen bør være mest mulig objektiv. Eksempelvis kan ikke sannsynligheten for at offentlige myndigheter får ulovlig tilgang til personopplysningene vektlegges.
4. Identifiser og implementer tilleggstiltak for sikring	Kommer du i steg 3 frem til at rettighetene til datasubjektene ikke blir godt nok ivaretatt i importlandet, som i USA, må du vurdere tilleggstiltak for å sikre dataene. Slike tiltak kan være kontraktuelle, organisatoriske eller tekniske. Fordi kontraktuelle og organisatoriske tiltak raskt kan komme til kort overfor en inngripende stat, blir i praksis de tekniske tiltakene viktige. I veiledningens vedlegg 2 listes opp en rekke scenarier. Utfra disse foreslås tiltak. Særlig sterk kryptering hvor dataeksportøren eller tredjepart har kontroll over den private nøkkelen er aktuelt. Pseduonymisering, særlig beskyttede mottagere (f.eks. medisinsk forsking) og oppdelt behandling nevnes også. Scenarier hvor nødvendig sikring ikke kan skje, listes også. Ulike tiltak kan også kombineres. Kan ikke et forsvarlig vernenivå oppnås, kan ikke overføringen skje etter pvf. artikkel 46.
5. Få det formelle på plass	Dersom importlandet ikke står på hvitlisten til EU-kommisjonen (pvf. artikkel 45) må det formelle på plass i henhold til pvf. artikkel 46 (eller 49). Det mest praktisk grunnlaget under artikkel 46 (2) er standardbestemmelsene (c og d). Se listen under for alle grunnlag.
6. Revider jevnlig	Ettersom personvernreglene og rettstilstanden i importlandet er i kontinuerlig utvikling, kreves det jevnlige evalueringer av om sikkerhetsnivået på din overføring oppfyller det nødvendige beskyttelsesnivået. Denne overvåkingen av situasjonen i importlandet må gjøres i samarbeid med dataimportøren, og er en av forholdene som må dekkes av avtalen med importøren.

standardbestemmelser for eksport av persondata i henhold til pvf. artikkel 46 (2) c. De nye bestemmelsene følger opp kravene som følger av Schrems II-dommen og veilederen som vi så på over. Når bestemmelsene vedtas, trolig i mars i år, vil de utdaterte bestemmelsene fra 2001 og 2010 falle bort.

Hovedendringene som er foreslått:

a) økt fokus på tekniske beskyttelsestiltak
b) skjerpede plikter til å varsle om lokal lov som kan medføre myndighetsinnsyn
c) databehandleravtale etter pvf. artikkel 28 inkluderes i standardbestemmelsene
d) alle fire partskonstellasjoner (se under) dekkes

a) og b) – Den forståelige frykten for fremmede makters tvungne innsyn i europeiske personopplysninger, har gitt seg utslag også i utkastet til nye standardbestemmelser. Det viser seg særlig gjennom fokuset på tekniske beskyttelsestiltak og at partene må varsle hverandre om lokal rettstilstand og ved forespørsler om innsyn.

Også den situasjon at parten ikke har lov til å varsle, reguleres ved at parten likevel skal informere så mye som mulig, inkludert på aggerertert nivå. Myndighetsinnsyn har blitt en hovedbekymring etter Snowdens avsløringer, Schrems II og den generelle utviklingen fra demokrati og rettsstat mot autoritære styresett og overvåking i mange land.

Ved vurderingen av vernenivået etter lokal rett skal en konkret vurdering av overføringen gjøres. Hva er varigheten, hvilke type data og mottagere omfattes og hva er formålet? Litt overraskende skal også praktisk erfaring med myndighetsforespørsler vurderes. I eksportretningslinjene beskrevet i tabellen over, fremgår det at vurderingen skal være objektiv, og nemlig *ikke* vektlegge slik praksis.

Tanken bak en objektiv vurdering kan ha vært at myndighetspraksis fort kan endre seg. Det er naturligvis riktig, men samtidig virker det kunstig å skulle se bort fra faktisk praksis i et land. Etter min mening betyr dette at man må vurdere begge forhold, men ikke la seg forlede av (tilsynelatende) mild praksis dersom etterretningshjemlene er vide.

c) – Ved at også bestemmelser for databehandleravtaler etter pvf. artikkel 28 inkluderes i standardbestemmelsene endres dagens praksis med to dokumenter, slik at man bare får ett. Ifølge utkastet til nye standardbestemmelser artikkel 1 (c) oppfyller disse sin funksjon bare om at de forblir umodifiserte, med unntak av tekst i vedleggene og styrking av personvernet. Det kan være praktisk med bare ett dokument, med det frarøver partene muligheten til å påvirke innholdet av databehandlerdelen av avtalen. Det kan være særlig uheldig for ansvarsreguleringen, og synes dårlig begrunnet utfra personvernhensyn. Nær alle andre bestemmelser skal bidra til god sikring av behandlingen, håndhevbare rettigheter for datasjubjektene og rettsmidler. Ansvarsfordelingen mellom leverandør og kunde vil imidlertid i stor grad være et kommersielt forhold. Det må derfor være riktig å ta kommisjonens implementeringsbeslutning på ordet når den uttaler at rollen til standardbestemmelsene er å «begrenset til sørge for tilstrekkelige sikringstiltak for internasjonale overføringer.», og regulere ansvar selvstendig (side 1, siste avsnitt).

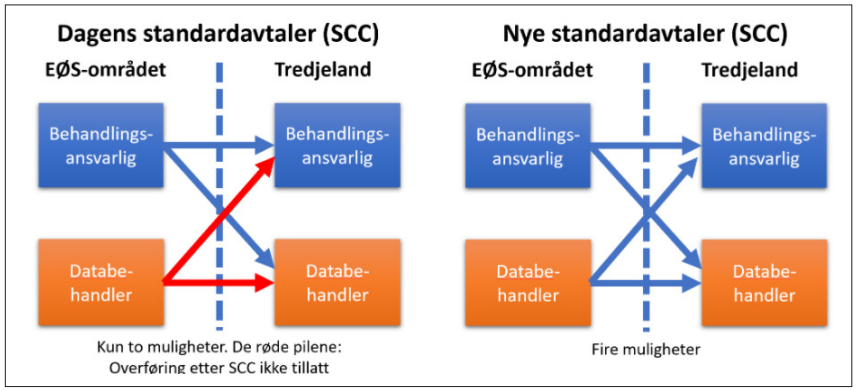
Det må gjelde også andre forhold, som betalingsplikter. Stilt overfor en stor amerikansk leverandør som ikke gir ved dørene, ville nok en motsatt konklusjon være velkommen for en del kunder, men vi må huske på at flertallet av databehandlere er vanlige bedrifter som har behov for å ha kontroll på sin juridiske eksponering.

d) – Med den modulært oppbygde malen til nye standardbestemmelser vil begrensningene i partskonstellasjoner opphøre. Forskjellen illustreres enklest med Jan Sandtrøs diagram.

Dermed blir problemet med overføring fra databehandlere til behandlingsansvarlige eller databehandler løst.

Ytterligere fire forhold det også kan være greit å være observant på:

– Landet – jurisdiksjonen – som velges for kontrakten må tillate tredjepartskrav. Siden et av hovedformålene med en overføringsavtale er at datasubjekter skal kunne håndheve sine rettigheter, kan ikke datasubjektenes rettsmidler være avskåret etter lokal rett.
– Malen er som nevnt modulær, for å støtte de fire partskonstellasjonene. Det vil dermed kreve litt fotarbeid å klargjøre malen til en konkret overføringsavtale.
– Pliktene til dataimportøren tydeliggjøres, som for eksempel krav til føre protokoll over behandlingen.
– Overgangsordningen vil bli på ett år fra Kommisjonen vedtar de nye standardbestemmelsene.



Innen dette året må dermed alle gamle avtaler erstattes.

Bindende virksomhetsregler

Det andre grunnlaget som fremdeles står åpent er bindende virksomhetsregler (pvf. artikkel 46 (2) b jf. artikkel 47). Med Schrems II-dommen vil disse kunne bli mer aktuelle for en del større virksomheter.

Virksomhetsreglene er en slags avart av standardklausuler, men brukes internt i en virksomhet med avdelinger i ulike land. Poenget er å lage ett sett behandlingsregler for hele konsernet, fremfor en vev av ulike avtaler på kryss og tvers. Fordelen er forenklet administrasjon. Ulempen er at reglene må godkjennes av Datatilsynet, en prosess som kan ta mange måneder, og kanskje år. Man slipper heller ikke unna seksstegs-vurderingen som beskrevet over.

Adferdsnormer og sertifiseringsmekanismer

Heller ikke adferdsnormer eller sertifiseringsmekanismer (pvf. 46 (2) e og f) ble kjent ugyldig i Schrems II-dommen. Dette er mindre utbredte overføringsgrunnlag, men vil støte på de samme prinsipielle utfordringene som øvrige grunnlag. Se nærmere artikkel 40 og 42 i forordningen.

Nødventilen

Det finnes som nevnt også spesielle unntak for overføringer som i utgangspunktet ikke skjer regelmessig i pvf. artikkel 49. Unntaket krever at det foreligger uttrykkelig samtykke fra datasubjektet, nødvendighet for å oppfylle eller inngå avtale, viktige allmenne interesser, vern av vitale interesser, forsvare rettskrav mv. Slike unntak skal tolkes strengt, uten av vi går noe nærmere inn på disse nå (retningslinjer 2/2018).

Verden sett i lys av Schrems II

USA har vi allerede behandlet over, men uten å nevne utviklingen i **California**. I solskinnsstaten ble California Consumer Privacy Act (CCPA) vedtatt i 2018 og trådte i kraft 1. januar 2020. CCPA gir et bedre vern enn hva andre delstaters regler tilbyr, men er likevel et godt stykke unna vernet den europeiske personvernforordningen gir. Det er derfor interessant at en folkeavstemning i California 3. november 2020 gikk i favør av en ny og mer heldekkende personvernlov kalt California Privacy Rights Act (CPRA). Loven vil tre i kraft 1. januar 2023.

Nye CPRA skal bygge på rammeverket i CCPA, men i større grad speile den europeiske personvernforordningen. Herunder skal USAs første rendyrkede datatilsyn, California Privacy Protection Agency (CCPA), etableres.

Når CPRA er på plass, kan vi kanskje få en situasjon hvor det vil være forsvarlig å overføre data til California, men ikke andre delstater.

India er interessant fordi mye programvareutvikling, forvaltning og support skjer der. For øyeblikket foregår et arbeid med å gjennomføre Indias første dedikerte personvernlov, kalt Indian Personal Data Protection Bill (PDPB). Tidligere har lagring og overføring av persondata blitt regulert av den generelle Information Technology Rules (ITR), som imidlertid fremstår noe utdatert stilt overfor de nye problemstillingene på området. PDPB er enda ikke vedtatt av parlamentet, men det er ventet at den vil bli det i løpet av 2021.

Loven er foreslått å gjelde for indiske myndigheter, firmaer som opererer i India og utenlandske firmaer som behandler indiske borgeres persondata.

PDPB har siden det første lovutkastet hatt store likhetstrekk med GPDR, særlig strukturelt. Ser man nærmere på det siste lovutkastet, foreligger det imidlertid visse sentrale forskjeller, som må vurderes ved eksport av personopplysninger. Landet er likevel et demokrati med en rettsstat som muliggjør bruk av rettsmidler for de registrerte.

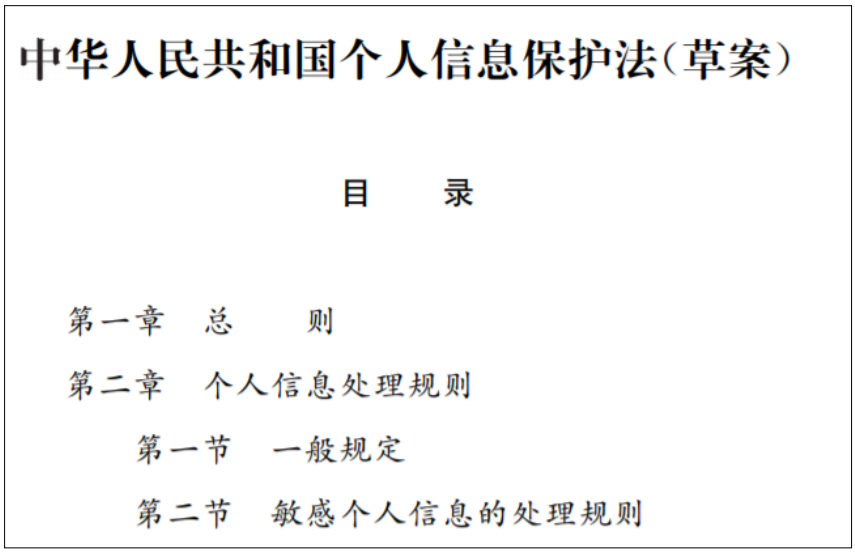
Kina må også nevnes, selv om det ikke spiller en så sentral rolle for europeisk databehandling som India. Fordi landet er så viktig økonomisk, vil persondata uunngåelig flyte til Kina og tilgang gis fra Kina i forbindelse med handel, produksjon og de mange oppkoblede forbrukerprodukten landet produserer.

Når «Kina» og «personvern» nevnes, vil mange sikkert tenke på landets (groteske) sosiale poengsystem. Det skjer imidlertid nå et arbeid med å innføre den første personvernloven i Kina, kalt Personal Information Protection Law (PIPL). Utkastet, som ble offentliggjort i oktober 2020, bygger på hovedprinsippene fra GDPR, blant annet med krav om lovlighet, nødvendighet, formålsbestemthet, innsyns- og korreksjonsrett.

Når forsvarligheten av dataeksport til Kina skal vurderes i lys av Schrems II-dommen og de etterfølgende retningslinjene, er det verdt å merke seg at PIPL også pålegger statlige organer i Kina plikter. Når det er sagt, er det ifølge observatører som Jamie P. Horsely tvilsomt om disse pliktene vil håndheves i praksis fordi unntakene for statlige myndigheter er vide, ikke minst innenfor nasjonal sikkerhet. Vi må naturlig nok også ha i mente at Kina er en autoritær stat med et enormt overvåkingssystem, og på ingen måte en rettsstat.

Storbritannia har landet i en slags mellomposisjon etter sin uttreden av EU. Formelt sett har dronningdømmet ikke rukket å komme på kommisjonens hvitliste, samtidig som realiteten er at reglene i Storbritannia tilsvarer personvernforordningen. Fra EUs side er det lagt opp til en totrinnsrakett:

- Første trinn gjelder inntil 30. juni 2021 og innebærer at overføringer til Storbritannia ikke vil anses som overføring til et tredjeland.
- Andre trinn forutsetter at en beslutning om tilstrekkelig vernenivå (adekvansbeslutning) avsies. Om det ikke skjer innen 30. juni



中华人民共和国个人信息保护法（草案）

目　　录

第一章　总　　则

第二章　个人信息处理规则

第一节　一般规定

第二节　敏感个人信息的处理规则

Ny kinesisk personopplysningslov (visstnok)

2021, vil Storbritannia anses som et tredjeland. Sjansen for at det skal skje er imidlertid liten, siden kommisjonen 19. februar 2021 varslet at den var i gang med å utforme en adekvansbeslutning for Storbritannia. Den vil i første omgang gjelde i fire år.

For Norges del ble det av traktatttekniske grunner laget en forskrift som sier det samme. Den rekordkorte forskriften er hjemlet i personopplysningsloven § 13.

Hva gjør leverandørene?

I den virkelige verden vil det ofte være avgjørende hvordan leverandørene tilpasser seg endringer i rettstilstanden. Ikke minst fordi markedsandelene til de store amerikanske leverandørene øker på bekostning av de europeiske, må vi se nærmere på enkelte av disse leverandørene.

Den største er **Amazon Web Services** (AWS). Selskapet leverer *platform as a service* og i liten grad programvare klart til å kjøres. Det vil si at kundene til AWS bygger sine løsninger på toppen av det underliggende tjenestelaget (som nå visstnok teller over flere hundre tjenester). Kundene vil dermed i stor grad kontrollere hvordan løsningen vil se ut, inkludert hvordan persondataene blir behandlet. AWS tilbyr standard personvernbestemmelser. Men som Schrems II gjorde klart, holder ikke avtalen alene. Dermed må kundene som lager løsningene som skal kjøre på AWS' servere, sørge for tilstrekkelig beskyttelse. AWS oppfordrer til bruk av kryptering, utover den betydelig sikkerheten selskapet selv besørger. Med bevisst fokus på innebygget personvern (pvf. artikkel 25), skal dermed lovlige løsninger kunne bygges, selv om de kjører på AWS' amerikanske servere. Ønsker man å skrelle vekk den usikkerheten USAs manglende rettsmidler for ikke-amerikanere representerer, vil imidlertid et bedre valg være å kjøre løsningen på et av AWS' datasentre innen EØS.

Microsoft har gått fra å være et symbol på det onde, monopolistiske konsernet, til å bli ansett som en personvernforsvarer. Selskapets bastante motstand mot det amerikanske justisvesenet i forbindelse med den nevnte Hotmail-saken fra 2013, er nok best kjent. Microsoft har også forsøkt å sikre data mot beslag ved å overføre råderett til datasentre til Deutsche Telekom i 2015.

Det siste initiativet fra Microsoft kom 19. november 2020, fem dager etter at retningslinjene fra Personvernrådet kom. Selskapets holdning er særlig viktig ikke bare fordi veldig mange mennesker bruker Office 365, men også fordi Microsoft, i motsetning til AWS, leverer *Software as a Service*. Det vil si programvare klar til bruk. Dermed vil få ha mulighet til å legge en trygg løsning oppå programvaren Microsoft tilbyr slik AWS muliggjør.

Initiativet var todelt. For det første et løfte om å bestride alle offentlige myndigheters krav om innsyn der det var mulig. For det andre, å gi erstatning til registrerte som får sine opplysninger utlevert til offentlige myndigheter i strid med personvernforordningen.

I lys av Hotmail-saken og øvrige tiltak, som kryptering og åpenhet, har Microsoft troverdighet. Selskapet påstår faktisk at det er en «entusiastisk tilhenger av GDPR».

På samme måte som for Apple, henger nok entusiasmen sammen med at forretningsmodellen til Microsoft ikke krever kommersiell utnyttelse av kundenes personopplysninger, fordi kundene betaler med penger, ikke persondata.

Googles og **Facebooks** situasjoner er diametralt motsatt. Selskapene tjener det meste av sine penger nettopp på bruk av andres personopplysninger. Dermed oppstår det naturlig en spenning med personvernhensyn, uten av jeg går nærmere inn på dette i denne forbindelsen. Jeg vil likevel anbefale dokumentarene The Great Hack og The Social Dilemma (Netflix).

Europa AS. På dette bakteppet kan man spørre seg hvorfor ingen gode europeiske alternativer har kommet på banen. Det får bli tema for en annen artikkel.

Hvor går vi videre?

Vi kan analysere veien videre på flere måter. Her er to måter å se det på:

Analyse 1 – tre krefter. Tre krefter vil etter min mening styre i hvilken retning utviklingen vil gå:

1. håndheving
2. behov

3. evne

Hvor effektiv vil *håndhevingen* av regelverket bli? Foreløpig er det liten grunn til å tro at sanksjonsnivået til det norske Datatilsynet vil bli en sterk kraft for etterlevelse. Gebyrene har så langt vært lave. I andre europeiske land har de vært betydelig større, men likevel langt unna det nivået for eksempel konkurransemyndighetene ligger på. Håndhevingseffekten er derfor etter min mening foreløpig begrenset, men vil tilta.

Behovene virksomheter har for å bruke de beste skytjenestene og samhandle med andre land er sterke. De virksomhetene som raskt tar i bruk nye muligheter vil oppnå en konkurransefordel. For eksempel sparer man enormt med tid og kostnader på å bruke det rike tjenestetilbudet til AWS, fremfor selv å bygge en teknisk grunnmur for tjenesten man ønsker å bygge.

Den manglende *evnen* virksomheter har til å etterleve regelverket vil også bremse etterlevelse, selv for motiverte virksomheter. I praksis er de fleste virksomheter prisgitt leverandørenes tilbud. Dermed blir leverandørens tilpasning til regelverket den avgjørende faktoren for om etterlevelse blir mulig. Som utviklingen med Microsoft viser, kan det være grunn til optimisme. Med hard håndheving og regelutvikling i USA, vil trolig andre store leverandører følge etter.

I sum gir analyse 1 grunn til optimisme.

Analyse 2 – fire megatrender. Vi kan også se utviklingen i lys av fire underliggende megatrender knyttet til overføring av personopplysninger til andre land.

1. *Mer overvåking.* Både etterretningsvesen og annonsører øker sin digitale overvåking. Annonsørene elsker pixel-IDer og remarketing. Etterretningsorganisasjoner tar i bruk alle tenkelige og utenkelige metoder. Kina og USA går i front. Bringes ikke disse overvåkningen under en eller annen form for kontroll, ser jeg ikke for meg et reelt personvern. Selv om det ikke er en enkel jobb, mener jeg det likevel bør være mulig, med en blanding av tekniske og juridiske tiltak.
2. *Mer oppkobling.* Flere tjenester og mer personlige data blir behandlet utenfor vår reelle kontrollsfære fordi vi blir stadig mer oppkoblet. Treningsapper, koronaapper, kjernejournal og andre helsedata er eksempler. Sosiale medier blottlegger hele sosiale nettverk og interesser. De fleste har minst en app påslått som sporer din geolokasjon. Support ytes fra India og andre steder med svak regulering.
3. *Mer cyberkriminalitet.* Om annonsører og spioner hadde holdt seg på matta, vil de kriminelle likevel fortsette å øke sin pågang. Gevinstene for de kriminelle er enorme, og sårbarhetene er store. Noen av de største personvernbruddene vi har sett kommer av kriminell hacking.
4. *Strengere personvernregler.* Det er ikke bare Europa og California som ønsker å begrense og kontrollere behandlingen av personopplysninger. Mange land har i lang tid latt seg inspirere av både EUs 1995-personverndirektiv og personvernforordningen. EUs imponerende regelfabrikk har hatt stor eksportsuksess, noe som også har økt bevisstheten verden over.

Om den regeltrenden i punkt 4 vil klare å demme opp for de tre andre trendene er et stort spørsmål. Skal man se på den historiske utviklingen, som vi begynte med, ser det ikke så lyst ut. Gradvis, over flere hundre år, har vi måtte leve med stadig større inngrep i privatlivet. De reglene som har blitt laget har bremset eller modifisert utviklingen litt, men utviklingen har gått sin gang. Vi blir tilvendt og vi aksepterer. Slik tror jeg dessverre det vil gå også denne gangen, selv med analyse 1 i mente. Håpet er at reguleringen som kommer modererer nok til at lykken ikke tørker inn med privatlivet.

Hva gjør jeg?

Tilbake i det praktiske hjørnet: Skal man drive forretning, og til en viss grad offentlig forvaltning, slipper man ikke unna eksport av persondata. Hva skal du gjøre?

Som ellers når man står overfor en kraft man ikke kan kontrollere – gjør det beste ut av det:

1. gi ikke opp
2. følg de seks stegene i tabellen over (skaff kontroll på hva som eksporteres, begrens mest mulig, gjør sikkert – krypter, slett når ikke trenger lenger mv.)
3. dokumenter at du har vurdert og handlet
4. følg opp over tid – legg inn i årshjulet for styrearbeid og internkontroll

Som samfunn bør vi bygge opp egne alternativer i Norge og EØS.

Lykke til – verden vil ikke bli den samme igjen – det blir den aldri.

Advokat Kristian Foss er partner i Bull & Co Advokatfirma, med over 20 års erfaring fra personvern, IT- og teknologijuss. Foss er medlem av Fagutvalget for IKT-rett i Juristenes utdanningssenter og har har vært president i IT IP Law Group Europe. kf@bull.no

Kredittvurderinger

– Når kan det gjøres og hva sier Datatilsynet?

Av Emilie Sverdrup og Line Haukalid

Kredittvurderinger av privatpersoner kan være nødvendig i flere sammenhenger, for eksempel når en virksomhet selger varer på kreditt eller utstede kredittkort. Det kan også være nyttig for en virksomhet å kredittvurdere privatpersoner selv om virksomheten ikke skal yte kreditt til personen selv, for eksempel hvis personen innehar en sentral funksjon i et selskap.

Det siste året har vi sett et økende antall overtredelsesgebyrer fra Datatilsynet til private virksomheter som har innhentet kredittvurderinger av privatpersoner. Av de totalt seks gebyrene ilagt private virksomheter gjelder fire kredittvurderinger.

En kredittvurdering er en analyse av en persons kredittverdighet. Resultatet er basert på en sammenstilling av personopplysninger fra flere kilder. En kredittvurdering vil også vise detaljer om personens privatøkonomi, herunder eventuelle betalingsanmerkninger, frivillige pantstillelser og gjeldsgrad.

I denne artikkelen vil vi redegjøre for hvilke krav GDPR stiller til innhenting av kredittvurderinger av privatpersoner og enkeltpersonforetak, og hvilke tilfeller man kan innhente kredittvurderinger. Avslutningsvis vil vi kort se på Datatilsynets overtredelsesgebyrer.

Emilie Sverdrup

Line Haukalid

Krav om behandlingsgrunnlag

Innhenting av kredittopplysninger om enkeltpersoner utgjør en behandling av personopplysninger. Det samme gjelder for enkeltpersonforetak, ettersom opplysningene sier noe om innehaverens økonomi. Virksomheten må derfor ha et behandlingsgrunnlag. Aktuelt i denne sammenhengen er GDPR artikkel 6 (1) bokstav f) berettiget interesse, som i korte trekk tillater behandling av personopplysninger hvis man etter en interesseavveining kommer til at virksomhetens interesse i behandlingen overstiger hensynet til den enkeltes personvern, såfremt behandlingen er nødvendig for å oppfylle den aktuelle interessen.

Den tidligere personopplysningsforskriften, som nå er opphevet, oppstilte som vilkår for innhenting av kredittvurderinger at virksomheten måtte ha et saklig behov for kredittopplysningene. Datatilsynet har imidlertid uttalt at saklig behov etter ikrafttredelsen av GDPR ikke lenger er et tilleggsvilkår. En vurdering av om det foreligger et saklig behov vil likevel ligne vurderingen av om det foreligger en berettiget interesse. Tidligere praksis fra Personvernnemnda knyttet til dette vilkåret vil derfor fremdeles være relevant i berettiget interesse-vurderingen.

Krav om internkontrollrutiner og informasjon

Virksomheter må dokumentere at kredittvurderinger innhentes i samsvar med GDPR. Dette kan gjøres gjennom dokumenterte rutiner til ansatte som skal innhente kredittvurderinger. Rutinene bør vise til hvilke vilkår i GDPR som må være oppfylt for at virksomheten skal kunne gjøre en kredittvurdering av kunden. Herunder har Datatilsynet videre uttalt at rutinene bør fremheve de relevante rettslige grunnlagene i artikkel 6, samt sørge for organisatoriske tiltak som sikrer at kravene i GDPR er oppfylt før man innhenter kredittvurderingen. Slike organisatoriske tiltak kan for eksempel være opplæring av ansatte med ansvar for kredittvurdering.

I noen av vedtakene til Datatilsynet har virksomheten anført at kredittvurderingen ble innhentet ved en feiltakelse. Datatilsynet har likevel ilagt overtredelsesgebyr, blant annet under henvisning til at virksomheten mangler gode internkontrollrutiner for å forhindre urettmessig innhenting av kredittvurdering.

Når kan man innhente kredittvurderinger?

Vedtak fra Datatilsynet og Personvernnemnda viser at det må foreligge en tilknytning mellom virksomheten og personen som blir kredittvurdert. Slik tilknytning kan være et kunde- eller leverandørforhold. De klare tilfellene hvor virksomheten vil kunne ha en berettiget interesse i å kredittvurdere en person er når virksomheten skal yte denne personen kreditt.

Personvernnemnda har uttalt at formålet med en kredittvurdering er normalt å kartlegge hvorvidt en potensiell kunde er kredittverdig, og dermed om virksomheten ønsker å inngå avtale med vedkommende. Saklighetskravet vil dermed være oppfylt når virksomheten skal bruke kredittopplysningene i forbindelse med sin vurdering av kredittrisiko, for eksempel ved et tilsagn om lån eller avtale om løpende ytelser som faktureres etterskuddsvis, slik som mobilabonnement. I slike tilfeller er det normalt påregnelig for den som blir kredittvurdert at virksomheten ønsker å vite noe om vedkommendes betalingsevne.

I andre tilfeller, hvor behovet ikke er like opplagt, er det viktig at virksomheten vurderer sin interesse i kredittvurderingen grundig. Kredittopplysninger er ikke sensitive personopplysninger, men er likevel ansett av mange som private opplysninger, fordi de sier noe om personens privatøkonomi. Overtredelsesgebyrene fra Datatilsynet viser at personvernhensynet veier tungt i vurderingen av om virksomheten har en berettiget interesse.

Eksempler på tilfeller hvor kredittvurdering skjer uten noen form for tilknytning er når kredittvurderingen er begrunnet i kikkermentalitet og nysgjerrighet. Personvernnemnda har uttalt at dette er det motsatte av saklig behov. Der kredittvurderingen bærer preg av nysgjerrighet og påfølgende vilkårlighet vil berettiget interesse klart nok ikke foreligge.

Overtredelsesgebyrenes størrelse

Ved vurderingen av om det skal ilegges overtredelsesgebyr og ved utmålingen skal det tas hensyn til en rekke momenter, blant annet karakteren, alvorlighetsgraden, varigheten av overtredelsen og om virksomheten har implementert egnede tekniske og organisatoriske tiltak, for eksempel gode internkontrollrutiner.

Datatilsynet uttaler i sine vedtak at overtredelsesgebyret skal være virkningsfullt, stå i et rimelig forhold til overtredelsen og virke avskrekkende. Gjennomgående i kredittvurderingsvedtakene er at Datatilsynet vektlegger at personopplysningene som innhentes er svært beskyttelsesverdige, og som individene har en forventning om at ikke innhentes med mindre det er saklig begrunnet.

Overtredelsesgebyrene har vært i størrelsesordenen 75.000 til 1 millioner kroner. Sistnevnte er foreløpig kun varslet, og ikke vedtatt.

Emilie Sverdrup er advokatfullmektig i Advokatfirmaet Wiersholm.
Line Helen Haukalid er fast advokat i Advokatfirmaet Wiersholm.

Halvor Manshaus

Leder IP/Media-gruppen i Advokatfirmaet Schjødt AS, Oslo og fast spaltist i Lov&Data.

Digitale angrep og utpresning – løsepengevirus

1. Trusselbildet

Nasjonal Sikkerhetsmyndighet (NSM) publiserer sin årlige sikkerhetsrapport i midten av mars 2021. I forbindelse med en felles pressekonferanse med Politiets Sikkerhetstjeneste (PST) og Etterretningstjenesten ble det lagt frem en forhåndsvis oppsummering av sikkerhetsrapporten. Denne oppsummeringen tegner et dystert bilde når det gjelder datasikkerhet både globalt og i Norge[1]. I forbindelse med pressekonferansen uttalte direktør i NSM, Kjetil Nilsen:

«Det skjerpede digitale risikobildet handler om den teknologiske utviklingen. En utvikling som vi alle har nytte av og som gir oss velferd, trygghet og verdiskaping. Men utviklingen skaper også sårbarheter»

Et viktig trekk ved denne utviklingen den senere tid ligger i tiltakene mot koronapandemien. Takket være utviklingen bare de siste 5-10 årene har det nå vært mulig å implementere en digital hverdag med hjemmekontor, dokumentdeling og videokonferanser som har tatt en del av brodden fra tiltak som nedstengning og karantene. Dette innebærer samtidig at vi har fått en økt digital sårbarhet, ikke bare ved at antall digitale grensesnitt øker så voldsomt, men også fordi overgangen har skjedd så hurtig. I oppsummeringen fra NSM er dette formulert slik:

«Flere virksomheter har forsert egne digitaliseringsplaner som følge av covid-19-pandemien. Dagens beslutninger skaper fremtidige utfordringer dersom sikkerhetsløsninger ikke er godt nok ivaretatt.»

Samtidig har vi sett en økning i større dataangrep kombinert med såkalt ransomware eller løsepengevirus. NSM sendte 17. januar ut varsel til alle kommuner og informasjon til offentlige virksomheter om slike utpresningsangrep i kjølvannet av et større angrep mot Østre Toten kommune[2]. Løsepengevirus er en form for utpresning hvor dine egne data holdes som gissel inntil betaling skjer - eller dataene frigjøres på annet vis. Det skilles normalt mellom løsepengevirus som krypterer eller låser selve datafilene der de ligger lagret, slik at disse i praksis gjøres utilgjengelige. Andre varianter låser tilgang til selve datamaskinen, slik at den i praksis gjøres ubrukelig inntil sperren er fjernet.

Hvis man kan omtale løsepengevirus som en bransje, så kan vi konstatere at denne har modnet til en internasjonal virksomhet som i dag omsetter for milliarder av kroner. Et særtrekk ved virksomheten er at den har et stort globalt nedslagsfelt kombinert med standardiserte systemer hos ofrene som bruker samme operativsystem, samme infrastruktur, samme komponenter og brukere som aggregerer data i skyen. Alt dette innebærer at en svakhet et sted også vil kunne gjenfinnes en hel rekke andre steder. Automatisering av angrep og bruk av standardiserte hacke-programmer åpner for at mindre kvalifiserte kriminelle kan benytte slike skadeprogrammer. Samtidig er det åpenbart at store presseoppslag om spektakulære utpresningssummer kan virke rekrutterende i det kriminelle miljøet.

Som advokat kan man på enkelte områder se utviklingen i samfunnet speile seg i sakstypene som kommer inn. Tidligere var det langt mellom de spektakulære sakene om utpresning av denne typen, mens dette nå dukker opp stadig oftere. Spørsmål som går igjen er først og fremst hvordan dette kunne skje, hva man gjør, hvem man skal henvende seg til og hvordan man skal forholde seg til selve utpresningen. Litt senere i prosessen er det kanskje også noen som tar opp hvordan man kan hindre at dette skjer igjen.

2. Hvordan kunne dette skje?

Virus og dataangrep får innpass på en rekke ulike måter. En vanlig fremgangsmåte er å lure en eller flere enkeltbrukere til å kjøre filer som inneholder angrepet. Dette kan foregå f. eks. gjennom vedlegg til e-post eller lenker til tilsynelatende legitime eksterne nettsider som laster inn de nødvendige programlin-

1 *https://nsm.no/getfile.php/136165-1612871437/Demo/Dokumenter/Rapporter/Risiko%202021%20hand-out.pdf*

2 *https://nsm.no/aktuelt/kommuner-og-offentlige-virksomheter-ma-beskytte-seg-mot-losepengevirus*

jer. I andre tilfeller oppdages det generiske svakheter som har stor utbredelse og som gir parallelle angrepsvektorer inn mot en rekke virksomheter over hele verden. Eksempler på dette er løsninger som skal åpne for vennligsinnet trafikk utenfra, som Remote Desktop Protocol (RDP) og Virtual Network Computing (VNC) som begge er standarder for fjernstyring eller fjernpålogging mot datasystemer. En annen kategori er målrettede angrep der man tråler offerets systemer på jakt etter åpninger eller svakheter. Slike angrep kan være mer subtile og krevende både å oppdage og forhindre. Det finnes også eksempler på angrep i form av datafiler lagret på minnepinner som fysisk bringes inn i virksomheten, for eksempel gjennom fysisk overføring eller at minnepinnen sendes som markedsmateriell.

Når angrepet først er i gang, er det tilfeller der gjerningspersonen i forkant har kopiert ut fildata som fremvises for offeret. Dette gjøres både for å vise den kontroll man har over angrepet, samt at det åpner for ytterligere styrke i utpresningen. Offeret trues ikke bare med sperret tilgang til egne data, men også med publisering av offerets egen informasjon publisert på Internett. En vanlig fremgangsmåte er å kryptere de aktuelle filområdene det er snakk om med en sterk krypteringsalgoritme, slik at dekryptering kun kan skje med gjerningspersonens nøkkel.

Det er på dette tidspunktet at offeret gjerne får beskjed om at angrepet avbrytes og systemene tilbakeføres først når et definert beløp er overført, gjerne i en kryptovaluta som bitcoin eller lignende som er vanskelig å spore. Det settes vanligvis en frist på noen dager, der det samtidig heter at dataene etter dette vil være permanent sperret, eller at prisen dobles med en ny kort frist.

3. Hva gjør man og hvor henvender man seg?

Massedistribuerte angrep som utnytter standard-svakheter vil kunne ramme vilkårlig. Mange privatpersoner har allerede opplevd at deres personlige datamaskiner blir kryptert eller sperret. Da mister man kanskje tilgang til bildesamlingen eller annen personlig informasjon som i seg selv kan være ille nok. Samtidig kan nok også trusselen med at nedlastet informasjon spres videre på nettet utgjøre en ytterligere belastning.

Her vil vi fokusere på kommersielle virksomheter som rammes. Situasjonen vil ofte være ekstremt alvorlig enten det er filer man ikke får tilgang til eller det er snakk om utestenging fra datasystemet. Angrepet mot Hydro våren 2019 er beregnet å ha medført tap på over en halv milliard kroner[3], i tillegg til at man måtte utsette rapportering av kvartalstall grunnet begrenset tilgang og kontroll over systemene[4]. Et annet løsepengevirus rettet mot Maersk i 2017 skal ha kostet rederfirmaet om lag 2 milliarder kroner[5]. For andre vil opplevelsen være at virksomheten stopper helt opp, eller at trusselen om publisering av informasjon vil ødelegge omdømme og troverdighet på en måte som ikke lar seg overkomme. Uansett vil behovet for ekstern bistand melde seg øyeblikkelig. Det er de færreste virksomheter som sitter på denne type spesialkompetanse internt, og det må nå tas krevende og vanskelige beslutninger. Eiere og ansatte må orienteres og trusselbildet må avklares så raskt som mulig. Som nevnt jobber man normalt innenfor en trang tidsfrist fastsatt av gjerningspersonen.

Det første man gjør er normalt å forsøke å få en **oversikt** over hva som er rammet – for deretter å **isolere** dette som en fysisk eller logisk enhet. Dette kan bety å skru av enkelte komponenter, koble ut strømmen og/eller nettverkstilkoblinger. Tanken er å hindre at angrepet sprer seg, og samtidig gjøre det vanskelig for den som forsøker å koordinere fra utsiden. Her kan det være flere vanskelige avveininger, for eksempel å velge mellom å sikre spor for en etterfølgende etterforskning og det å gjøre umiddelbare tiltak i en desperat situasjon.

I det man vet at man er under angrep vil det være fornuftig både å **varsle** og innhente **ekstern kompetanse**. Både i små og store bedrifter vil det normalt være nødvendig å trekke inn en eller flere IT-leverandører. I mer alvorlige tilfeller må man vurdere om det skal innhentes spesialkompetanse innen datasikkerhet som er vant til å håndtere slike situasjoner. **Politiet bør informeres** og trekkes inn så tidlig som mulig. Der det er snakk om et alvorlig eller omfattende angrep vil det være naturlig at riktig enhet hos NSM også trekkes inn – eller i det minste får en orientering.

På dette tidspunktet vil det være hektisk, og det er lett å glemme **informasjonsflyten**. Man trykker på alle de røde knappene og det skjer nå veldig mye på en gang. Som regel har man hverken oversikt eller kontroll. Man møter IT-ressurser som bruker en rekke tre-bokstavers akronymer og man lærer mer om IT-sikkerhet enn man opprinnelig kunne ønske eller forestille seg. Likevel sitter man på mer informasjon enn alle andre rundt virksomheten. Det bør umiddelbart lages en oversikt over hvem som trenger informasjon og hva som skal formidles. En prematur melding ut i markedet kan medføre like mye skade som selve markedet, samtidig som det å vente for lenge kan skade renommé

3 *https://www.hydro.com/en/media/on-the-agenda/cyber-attack/*

4 *https://www.tu.no/artikler/dataangrepet-mot-hydro-koster-selskapet-nesten-en-halv-milliard/463986*

5 *https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/?sh=7d26e6014f9a*

og omdømme vel så mye. I første omgang bør ansatte få beskjed om hva som skjer og hvordan de skal forholde seg i den nærmeste perioden. Hvordan skal kommunikasjonen internt foregå dersom epostssystemet er nede. Hvordan skal man jobbe når man ikke får åpnet dokumenter eller hentet ut digitale saksmapper? Hva skal de ansatte gjøre, og ikke minst – hva skal de si til kunder og omverden. Beslutningene som skal tas i virksomheten vil nå også kunne være på et nivå der det er naturlig at styret holdes informert, og trekkes inn i beslutningsprosessene der dette er naturlig.

I vurderingen av hva som skal kommuniseres er det i tillegg flere offentlige krav man skal forholde seg til. Eksempelvis vil GDPR-kravene (personvernforordningen) tilsi at ikke bare Datatilsynet skal varsles, men også den personen som opplysningene gjelder («den registrerte») dersom sikkerhetsbruddet medfører høy risiko for dennes «rettigheter og friheter», jfr. personvernforordningen artikkel 34 nr. 1. I det siste tilfellet krever bestemmelsen at den behandlingsansvarlige gir slik underretning *uten ugrunnet opphold*. Personvernforordningen artikkel 33 nr. 1 slår generelt fast at:

«Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til Datatilsynet, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Dersom bruddet ikke meldes til tilsynsmyndigheten innen 72 timer, skal årsakene til forsinkelsen oppgis.»

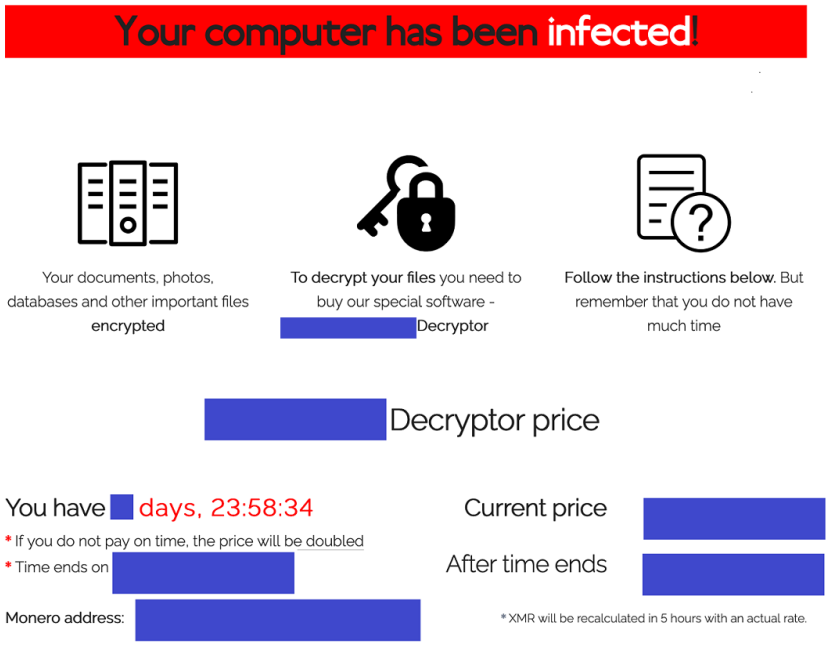
Forordningen tenker her på tre ulike typer kategorier av brudd på personopplysningssikkerheten, brudd på konfidensialitet, integritet og tilgjengelighet. Et brudd kan stå alene, eller kan bestå av en kombinasjon av disse tre kategoriene.

Hvem man skal kontakte vil bero blant annet på hva slags type informasjon og systemer som er rammet, og hvor omfattende og alvorlig angrepet er. Det er vanskelig å lage en uttømmende liste, men noe man raskt kan glemme i farten er å kontakte forsikringsselskapet. Dette ikke bare for å melde inn skaden og sørge for at man får veiledning med tanke på å ikke slette spor eller bevis som kan få betydning i et etterfølgende forsikringsoppgjør. Forsikringsselskapet vil i praksis kunne sitte på ressurser og kunnskap som kan være relevant for å håndtere angrepet på riktig måte. I forbindelse med varsling til politiet kan det være at man overser å sende inn en formell anmeldelse. Dette kan være et vilkår under en eventuell forsikringsavtale og bør i så fall følges opp.

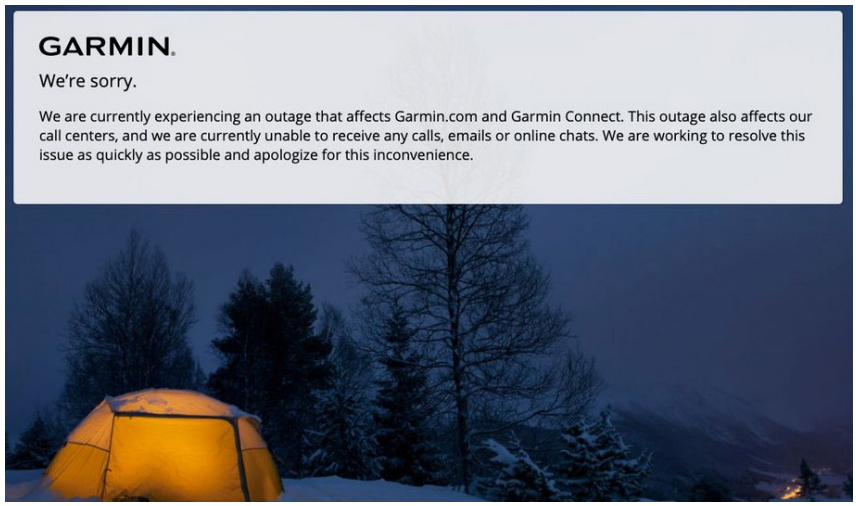
Som omtalt ovenfor er det nokså vanlig at hackerne også laster ned fildata i varierende mengder i forbindelse med et angrep. Det er da viktig å være klar over at det er opprettet ulike nettsider med auksjoner og direktesalg av slikt ulovlig nedlastet materiale. Her kan man finne alt fra budsjetter og forretningsstrategier til tekniske tegninger, eposter og interne saksdokumenter. I en periode etter et angrep vil det være fornuftig å overvåke slike nettsider med tanke på å følge opp eventuelle forsøk på salg av virksomhetens data.

De ulike fasene av angrepet glir nå raskt over i hverandre. Parallelt med at man innhenter informasjon om angrepet forsøker man nå å sette inn **mottiltak** i et forsøk på å begrense skaden og om mulig å uskadeliggjøre fremmede kodelinjer. Her vil IT-ressurser ofte måtte samarbeide, ved at det bør sjekkes hva man har tilgang til i sikkerhetskopier, hvordan dette kan hentes opp igjen med sikte på å gjenetablere normal drift. Har man et eget miljø for hjemmekontor kan man kanskje gå over til dette også på faste arbeidsstasjoner på kontoret – det gjelder å tenke raskt og kreativt.

Det ville være uheldig om man gjenopprettet systemene, bare for å se sikkerhetskopien korrumperes kort tid senere. Det er derfor viktig at oversikt og mottiltak gjøres i en kontrollert prosess, slik at man i størst mulig grad får renset ut eller isolert systemer som er angrepet før man introduserer gjenoppretting og normalisering. I tillegg er det jo en nærliggende tanke at hvis det først har vært en åpning for et slik angrep, så vil muligheten være tilstede for at flere angrep allerede har infiltrert systemet. Det kan derfor være ønskelig å gjøre en sanering også utover det ene aktuelle angrepet som har funnet sted.



4. Et konkret eksempel – Sodinokibi



Skjermbildet viser løsepengeviruset Sodinokibi i aksjon. Bildet er fra et reelt angrep. Blå sladding er gjort for å fjerne informasjon som kan identifisere angrepet. Bildet gir offeret informasjon om at angrepet er pågående og at datafiler er blitt kryptert. For å gjenåpne tilgang må brukeren kjøpe en nøkkel som er spesifikt koblet mot dette konkrete angrepet. Dette vil si at en nøkkel som åpner opp krypterte filer i et tilfelle ikke vil fungere mot andre tilfeller av Sodinokibi-krypterte filer.

Informasjon om angrepet vil også bli plassert i egne tekst-filer som lagres i samme mappe som de krypterte filene befinner seg. Beløpet som angis i feltet «Current price» vil kunne variere fra sak til sak. Løsepengevirus anvendes både mot privatpersoner og virksomheter, og Sodinokibi er blitt brukt i begge tilfeller. Det finnes eksempler på at beløpet kan være noen tusenlapper, mens i dette tilfellet var det snakk om flere millioner kroner. Dersom løsepengene ikke blir betalt inn den angitte fristen, angir feltet «After time ends» en dobling av prisen.

Selv om man betaler løsepengene har man ingen garanti for at man mottar nøkkelen for å dekryptere filene eller at denne vil fungere. Normal prosedyre bør i stedet være å isolere og rense ut infiserte områder, for deretter å gjenopprette fra sikkerhetskopi.

5. To pay or not to pay

Politiet, enten det er Kripos, Økokrim eller en annen enhet vil selvsagt anbefale at man ikke betaler det utpresseren krever. Det er mange gode grunner for dette. Ved å betale belønner man jo den kriminelle og er i prinsippet med på å finansiere det jeg ovenfor omtalte som en voksende kriminell bransje med global utstrekning. I tillegg vil man ikke ha noen kontroll over hvor midlene ender, og disse kan gå til å finansiere alvorlige kriminelle handlinger. Problemstillingen kan minne om spørsmålet om utbetaling til pirater som har kapret norske skip i utenlandske farvann. En kortsiktig løsning der man betaler er med på å finansiere flere kapringer i fremtiden.

Utgangspunkt må være at man ikke betaler ved utpressing. La oss være enige i det.

I praksis kan dette stille seg som et umulig valg. Angrepet kan ramme så hardt at virksomheten vil kunne bli satt alvorlig tilbake, kanskje gå helt under, om dette ikke løses raskt. Det er flere eksempler på at virksomheter har sett seg nødt til å gjøre store utbetalinger for å gjenopprette sine interne systemer. Garmin leverer blant annet smart-klokker der brukerne kan lage egne profiler og synkronisere sine data med en sentral server gjennom programmet Garmin Connect. Mot slutten av juli 2020 gikk tjenesten til Garmin ned for full telling. Brukerne fikk først ingen informasjon om hva som hadde skjedd. Det var ikke mulig å ringe inn, eposter forble ubesvart og til og med chatte-robotene var nede. Etter hvert kom det frem at Garmin var blitt utsatt for et løsepengevirus, og sannsynligvis måtte betale ut et betydelig beløp for å kunne gjenåpne sine tjenester og funksjoner[6]. Sikkerhetsansvarlig hos Garmin, Sam Curry, ga følgende karakteristikk av angrepet til CNN: *«the corporate equivalent of a heart attack.»*

Uklarheten knyttet til om Garmin faktisk betalte ut løsepenger understreker kompleksiteten knyttet til både juridiske og etiske vurderinger ved slike overføringer. Garmin selv har ikke avklart hva som skjedde, utover å bekrefte at man fikk en nøkkel som kunne dekryptere berørte filer. Bakgrunnen for diskusjonen knytter seg til spekulasjoner om at selve løsepengeviruset var av en art med navnet WastedLocker[7] som stammer fra en russisk hacker-gruppe som kaller seg Evil Corp.

Det amerikanske finansdepartementet har et eget kontor som håndterer sanksjoner overfor fremmede land og organisasjoner: The U.S Treasury Department's Office of Foreign Assets Control (OFAC). Ved at OFAC har plassert Evil Corp og flere av medlemmene på sanksjonslisten[8] er det i praksis forbudt for amerikanske rettssubjekter å overføre midler i denne retning. Sanksjonen åpner også for såkalte

6 *https://edition.cnn.com/2020/07/27/tech/garmin-coming-back-online/index.html*

7 *https://www.tek.no/nyheter/nyhet/i/8mrdWr/ogsaa-canon-skal-ha-blitt-angrepet-av-loesepengevirus*

8 *https://home.treasury.gov/news/press-releases/sm845*

sekundærsanksjoner for utenlandske personer som medvirker til slike transaksjoner:

«As a result of today's designations, all property and interests in property of these persons subject to U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with them […] Foreign persons may be subject to secondary sanctions for knowingly facilitating a significant transaction or transactions with these designated persons.»

Sanksjonssystemet fra OFAC regulerer i utgangspunktet ikke de opplistede land eller organisasjoner slik mange kanskje tror, men pålegger i stedet begrensninger på *amerikanske* rettssubjekter. Såkalte sekundære sanksjoner ble opprinnelig innført kun overfor Iran, men bruken har tiltatt og har som vi så ovenfor fått videre anvendelse. Sekundære sanksjoner fra OFAC er rettet mot ikke-amerikanske rettssubjekter (typisk finansinstitusjoner) som handler med land eller organisasjoner på sanksjonslisten. OFAC vil da kunne reagere med å oppstille forbud for amerikanske rettssubjekter å handle med det utenlandske rettssubjektet.

I tillegg til Evil Corp har OFAC laget sanksjonslister som omfatter en rekke andre grupper og enkeltpersoner knyttet opp mot hacking og løsepengevirus. Høsten 2020 gikk OFAC også ut med en særskilt Ransomware Advisory[9] rettet mot virksomheter som bidrar til betaling av løsepenger. I notatet pekes det på en rapport fra FBI som dokumenterer en vekst i USA på denne typen angrep fra 2018 til 2019 på 37% og understreker sanksjonssystemets anvendelse på dette området. Bakgrunnen for dette notatet fra OFAC er at ofre for løsepengevirus ofte vil søke bistand fra bankforbindelser eller ulike mellomledd som kan fasilitere irregulære overføringer av pengesummer, samt konvertere midlene til kryptovaluta som normalt kreves av utpresseren ut i fra et ønske om anonymitet. Ved å gå på mellomleddet forsøker OFAC å hindre at det gjøres utbetalinger i saker om løsepengevirus, i alle fall der mottakeren står på sanksjonslisten. Fordi mellomleddet ofte ikke vil ha klarhet i hvem som egentlig står bak angrepet, vil dette skape risiko for mellomleddet – som er noe OFAC spiller aktivt på. Hvorvidt det foreligger brudd på sanksjonsreglene vil kunne være avhengig av en totalvurdering, noe OFAC bruker som virkemiddel til å presse frem rapportering av angrep. Statistikken på dette området spriker enormt, men det virker som om alle er enige om at det foreligger en enorm underrapportering av angrep med løsepengevirus. Dette er nok også bakgrunnen for at OFAC skriver følgende om innrapportering av hendelser i sitt notat:

«Under OFAC's Enforcement Guidelines, OFAC will also consider a company's self-initiated,

timely, and complete report of a ransomware attack to law enforcement to be a significant

mitigating factor in determining an appropriate enforcement outcome if the situation is later

determined to have a sanctions nexus.»

Når det amerikanske sanksjonssystemet får så vidt mye plass, er dette for å understreke kompleksiteten i de vurderinger som offeret i en norsk utpressingssak må gjøre der man av ulike årsaker vurderer å betale løsesummen. Det er altså av flere grunner ikke tilrådelig å betale ut til en gruppe som står på sanksjonslistene, og den som forestår oppgjøret vil kunne rammes under bestemmelsene som sekundære sanksjoner.

Bruken av sanksjoner som virkemiddel mot løsepengevirus har i tillegg begynt å bre om seg også i andre jurisdiksjoner. EU nedkom med sin første sanksjonsliste rettet mot cyber-angrep 30. juli 2020. Dette tiltaket omfattet seks enkeltpersoner og tre grupper som har stått bak flere slike angrep. Konkret omfattet dette tiltaket reiserestriksjoner og frysing av økonomiske midler, samt et forbud for rettssubjekter innen EU-området å gjøre økonomiske midler tilgjengelig for de som står oppført på listen[10]. Hjemmelen for dette tiltaket stammer fra det såkalte «cyber diplomacy toolbox» som ble innført i juni 2017. Dette er et rammeverk som åpner for flere ulike tiltak *«to prevent, discourage, deter and respond to malicious cyber activities targeting the integrity and security of the EU and its member states.»*[11]

I norsk sammenheng må offeret ikke bare forholde seg til myndighetenes oppfordring om å avstå fra betaling til utpresseren, men også flere internrettslige regler. Her kan nevnes at de generelle reglene om heleri og hvitvasking i straffeloven §§ 332 til 341 etter omstendighetene vil kunne ramme overføringer av løsepenger. Helt kort handler heleri om å motta eller skaffe seg eller andre del i utbytte av en straffbar handling, mens hvitvasking beskriver handlinger som gjøres for å sikre utbyttet av en straffbare handling eller bidrar til å at utbyttet framstår som lovlig. Ved at skyldkravet både for heleri og hvitvasking kun er uaktsomhet, øker den faktiske risikoen ved å bistå ved betaling av løsepenger.

Rådgivere eller hjelpere som blir trukket inn i en eventuell overføring til utpresserne må altså gjøre flere vurderinger opp mot egen deltakelse. For advokater som rådgir i slike situasjoner skal man hjelpe klienten å navigere i et vanskelig landskap og samtidig unngå en rolle

9 *https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf*

10 *https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/*

11 *https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/*

som pådrar advokaten eget ansvar. Det kan fort oppstå uklare gråsoner, hvor det vil være naturlig å holde politiet informert. Rettspraksis i sammensatte saker om heleri viser hvor vanskelig grensene kan være å trekke, for eksempel i Skrik-saken (Rt-1998-407), som endte med frifinnelse for heleri under henvisning til at heleriforsøket var fremprovosert av politiet gjennom en rotete etterforskningsprosess. På et generelt plan er dommen lesverdig fordi den beskriver redningen av Skrikmaleriet som i seg selv var en spektakulær sak: *«Da politiet fikk opplysninger om tyvenes planer, ble sjefsinspektør Butler og de to engelske agentene brakt inn i saken, og politiet la sammen med dem en felle hvor de to engelske agentene under dekke skulle spille de sentrale roller som representanter for Paul Getty Foundation som finansør av løsesummen».*

Som en innledende betraktning fastslår førstvoterende at *«…den aksjon politiet iverksatte i «Skrik»-saken, hadde som overordnet og prisverdig mål å bringe maleriet i uskadet stand tilbake til Nasjonalgalleriet. Som redningsaksjon var politiets handlemåte vellykket, og jeg ser ikke noe ulovlig eller urettmessig ved den som redningsaksjon betraktet».* Høyesterett legger altså til grunn at det som objektivt sett kunne være en ulovlig helerihandling likevel kan være rettmessig. Dette synes å åpne for en rettsstridsvurdering i helerisaker der det overordnede formålet kan rettferdiggjøre handlingen. Dette kan få betydning ved betaling av løsepenger for eksempel for å avverge uønskede og alvorlige samfunnskonsekvenser av et IT-angrep. Det kan da anføres at dette ikke er rettsstridig heleri, og en slik anførsel vil måtte stå sterkere i saker der politiet er blitt holdt informert.

I tillegg til de generelle bestemmelsene om helere og hvitvasking har vi en egen lov mot hvitvasking og finansiering av terrorvirksomhet. Denne oppstiller en rekke plikter og begrensninger der det gjøres irregulære overføringer av et visst omfang. Hvitvaskingsloven tar sikte på å ramme nettopp det underliggende finansielle og økonomiske systemet som er nødvendig for å overføre midler forbundet med kriminalitet. Ved å regulere aktører som har funksjoner og roller i denne forbindelse gjøres det også vanskeligere å overføre løsepenger til kriminelle hackere. Loven gjelder for både juridiske personer og definerte yrkesgrupper. Førstnevnte er typisk ulike finansaktører som banker, forsikringsselskap, låneforetak og lignende. Sistnevnte er rådgivere og aktører som kommer i befatning med ulike typer pengeoverføringer, herunder advokater, revisorer, eiendomsmeglere, regnskapsførere osv.

Loven oppstiller tiltak, rutiner og varslingsplikt som kan få betydning dersom man blir bedt om å bidra til en overføring av løsepenger. Eksempelvis vil reglene om undersøkelsesplikt og rapporteringsplikt i henholdsvis §§ 25 og 26 samlet sett innebære et pålegg om å varsle Økokrim der det er grunnlag for mistanke om hvitvasking eller terrorfinansiering. Etter reglene i § 27 kan Økokrim gå inn i en konkret sak og forby gjennomføringen av en konkret transaksjon eller overføring.

Samlet sett innebærer reglene beskrevet ovenfor at det kan være vanskelig for offeret å få bistand til gjennomføring av selve transaksjonen der løsemidlene skal overføres. Dette er en tilsiktet virkning av disse reglene.

I Shakespeares Hamlet ligger problemstillingen nettopp i valgets kval, problemet med å velge når det ene betyr liv og det andre død. Pest eller kolera. Dette vil kunne være realiteten i en situasjon der den kommersielle virksomheten ikke får tilgang til sin egen informasjon. I de helt desperate situasjonene vil nødretten kunne gi grunnlag for å utføre handlinger som ellers ville være mer problematiske. Selv om nødretten kan øke handlingsrommet for offeret, vil tilgangen til hjelpere være begrenset avhengig av omstendighetene og anvendelsen av rettsreglene vi har sett på ovenfor.

Min vurdering er at aktsomhetsnivået knyttet til reglene om hvitvasking og heleri, samt en lojal oppfølgning av regelverket som en helhet tilsier at man uansett bør varsle myndighetene om hacking og dataangrep. Ved betaling av løsepenger må man også være klar over at dette ikke medfører noen garanti for at angrepet avsluttes eller at man får filene sine tilbake.

Dersom man først har betalt løsepenger, vil det kunne være aktuelt å vurdere om dette kan kreves erstattet dersom det kan påvises et ansvarsgrunnlag hos en tredjepart. Dette vil typisk kunne være IT-leverandøren. Et slikt krav må selvsagt vurderes konkret ut ifra kontrakt og faktum, men det er verdt å se på det bredere spørsmål om domstolene skal støtte opp under slike krav. Vi har flere eksempler i rettspraksis der Høyesterett understreker at et grunnvilkår for erstatning at den interessen som krever erstattet har et erstatningsrettslig vern, jfr Sterilseringsdommen (Rt-1999-203), Fostervannsdiagnostikk-saken (Rt-2013-1689) og Prostitusjonserstatnings-dommen (HR-2017-2352-A). Det er da ikke snakk om å gjøre et unntak fra erstatningsvernet, men om erstatningskravet i det hele tatt faller inn under lovens forståelse av hva som kan utgjøre et rettmessig krav. I den sistnevnte saken ble dette formulert slik i avsnittene 36-37:

«Den overordnede problemstillingen er etter mitt syn om interessen fortjener rettsordenens beskyttelse, jf. også Hagstrøm og Stenvik, Erstatningsrett (2015) side 48.

Hvorvidt en interesse har erstatningsrettslig vern er i de nevnte dommene avgjort etter en bred helhetsvurdering. Også erstatningsvernet for prostitusjonsinntekter må avgjøres etter en slik helhetsvurdering. Den vil måtte bero på en konkret bedømmelse av hensynet til de skadelidtes og samfunnets interesser vurdert generelt»

Det er altså ikke åpenbart at domstolene skal håndheve erstatningskravet der skadelidte har over-

ført løsepenger til kriminelle som har begått en straffbar handling, og rettspraksis antyder at det kan være nødvendig å avgjør dette etter en slik bred helhetsvurdering som Høyesterett har anvist.

6. Hvordan hindre at dette skjer (igjen)

Dette formatet tillater ikke noen uttømmende redegjørelse for sikringstiltak, men det er på sin plass med noen overordnede betraktninger. En lokal fiskehandler vil ha andre behov for IT-sikkerhet enn det multinasjonale konsernet med hundretusenvis av IT-transaksjoner hver eneste dag. Utgangspunktet må være en kost-nytte betraktning basert på en analyse av eksisterende løsninger og sikkerhetsnivå. Det videre arbeidet må ta utgangspunkt i en forståelse av at IT-sikkerhet dreier seg om flere ulike elementer som f. eks. *gode rutiner*, et sikkerhetsnett bestående av ulike *programmoduler*, systemets *arkitektur*, *kultur* hos alle som bruker systemet osv.

For å definere et nedre nivå pleier jeg å anbefale at man i alle fall bør forsøke å unngå uaktsomhet. Uaktsomhet vil kunne medføre en risiko for avkorting av forsikringsoppgjør, kritikk og eventuell bot knyttet opp mot GDPR-kravene, negativ medieomtale og omdømmetap, erstatningansvar overfor kunder og/eller tredjeparter osv.

I forhold til programvare er det helt sentralt at man har på plass antivirus, brannmur og tilsvarende løsninger for sikkerhet. Sikkerhetsoppdateringer må kjøres regelmessig – ikke bare oppdateringer av signaturfiler for antivirus. Like viktig er oppdateringer av de øvrige applikasjonene som kjøres på systemet. Det oppdages regelmessig svakheter og åpninger som tettes ved bruk av oppdateringen. Ligger man på etterskudd her, er det en sikker oppskrift på at det før eller siden går galt. I samme retning ligger eldre operativsystemer som Windows XP og Windows 7 som i dag må regnes for å være svakere mot angrep enn nyere tilskudd på stammen.

Rettigheter og autorisering av programmer er viktig for å sikre et ensartet miljø som er lettere å forvalte. I tillegg hindrer man bruk av makroer i ulike Office-produkter, som har vært en kjent svakhet brukt i flere angrep. Videre unngår man samtidig at brukerne installerer egne applikasjoner eller kjører ukjente eksekverbare filer som i seg selv kan gjøre stor skade.

En risikoanalyse vil avdekke hvilken informasjon og enkeltsystemer som er spesielt sårbare. I tillegg til å beskytte disse, kan det være naturlig å innføre rutiner for sikkerhetskopiering og gjenoppretting som begrenser skaden om angrepet først er der. Lokale datamaskiner koblet til mobile rutere kan sikre nettilgang om bedriftsnettet går ned. Mulighet for å koble skrivere fra lokalnettet gir mulighet for å scanne dokumenter og produsere utskrifter. I det hele tatt er det mange funksjoner som kan løftes ut av det sentrale systemet om man er godt forberedt. En god oversikt over risikoelementer og sårbarhet kan være grei å ha med seg når man sjekker omfanget av eksisterende forsikringsdekning – før skaden skjer.

Like viktig som alt det tekniske er kultur og bevissthet hos de ansatte. Ikke åpne ukjente vedlegg sendt per e-post. Ikke klikke seg inn på mistenkelige nettsider. Ikke laste ned datafiler fra Internett man ikke er helt sikre på. Opprettholde et visst nivå på passord, låsing av skjerm og data som lagres på mobilen. Dette gjelder like mye på hjemmekontor som på jobben.

For å begrense skaden når noe først skjer skal man ha på plass en plan for hvem som gjør hva. Dette er på samme nivå som å ha en plan for rømningsveier og møtepunkt når brannalarmen går. Det viktigste er å ha en oversikt over hvem man skal ringe til – og gjerne ha kontaktet disse ressursene på forhånd. Man vil stå langt bedre rustet om man har hatt de eksterne ressursene på besøk og befaring, og diskutert seg gjennom et par ulike scenarier for hva som kan dukke opp. Når det først er en krise er det utrolig hvor mye mer effektivt alt blir med en slik inngang. Hva gjør man for eksempel når man som Garmin opplever at telefontjenester og e-post går ned? Uten en plan blir det unødvendig spennende.

Digital sikkerhet

Håkon Bergsjø (red.), Ronny Windvik (red.), Lasse Øverlier (red.). Universitetsforlaget – 296 s. Oslo 2020 – ISBN: 9788215034225

Arbeidsplasser, hjem, utdanninger og sosiale arenaer er i stor grad blitt avhengige av IKT-systemer og internett. Overalt i samfunnet er det derfor et økende behov for kompetanse innen digital sikkerhet.

Digital sikkerhet er høyt prioritert av regjeringen, og i 2019 kom den med en nasjonal strategi for digital sikkerhet. Et viktig kompetansemål i strategien er at digital sikkerhet skal inngå i relevante yrkes- og profesjonsutdanninger.

Et sterkt lag av norske fagfolk har derfor skrevet denne grunnleggende læreboken om digital sikkerhet. Boken er lettlest og oppslagsvennlig og gir studentene en innføring i sentrale temaer som sikkerhetskultur, digital etikk, personvern, lover, verdivurdering, risiko, sårbarhet, trusler, autentisering, den kommersielle IKT-sikkerhetsbransjen, overvåking og deteksjon, hendelseshåndtering og opprydding. Dette er sentrale temaer som ikke bare de som tar digital sikkerhet som hovedemne, men også studenter innen ingeniørfag og tekniske fag bør ha kjennskap til.

I tillegg til bokens redaktører bidrar følgende medforfattere til boken: Leonora Bergsjø, Kjersti Brattekås, Janita Bruvoll, Kristian Eie, Gullik Gundersen, Martin Gilje Jaatun, Geir Køien, Bjarte Malmedal, Eirik Nesbakken, Nils Nordbotten, Kjell Olav Nystuen, Lasse Rosenvinge og Thomas Tømmernes.

Chrsitian Nordve i Cicsco anbefaler «Digital sikkerhet» (25:40) i Lørn. Tech podkast: *https://www.lorn.tech/lorn-pod/0637-network-christian-nordve-hjemmekontor-sikkert-og-effektivt*

Kunstig intelligens og big data i helsesektoren

Rettslige perspektiver

Redaktører: Anne Kjersti Befring, Inger-Johanne Sand. Universitetsforlaget – 656 s. Oslo 2020 – ISBN/EAN: 9788205531963

Bruk av kunstig intelligens og big data i helsesektoren og i medisinen må kunne kalles et paradigmeskifte.

Den nye teknologien kan for eksempel føre til at truende epidemier eller pandemier blir oppdaget langt tidligere, eller at riktig diagnose kan stilles raskere, slik at pasienter kan få mer presis og effektiv medisinsk behandling. Samtidig kan den ha uheldige konsekvenser – pasienter kan bli utsatt for skader eller krenkelser eller miste kontroll over spredningen av sine personopplysninger.

Innenfor helseretten oppstår spørsmål om hvordan denne teknologien skal kategoriseres og vurderes ut fra gjeldende rett, og om dagens rettstilstand er tilpasset den nye teknologien. Hvis ikke, hvilke endringer bør gjøres for at kunstig intelligens og big data kan bli bedre regulert?

Gorrissen Federspiel

Tue Goldschmieding

Samtykkeløsning på hjemmeside opfyldte ikke kravene til gyldigt samtykke

Det danske Datatilsyn ('Datatilsynet') har den 13. november 2020 ved afgørelse i sag med journalnummer 2020-31-3354 udtalt alvorlig kritik af DGU Erhverv A/S ('DGU'), vedrørende en ugyldig samtykkeløsning på hjemmesiden *www.golf.dk*, der ejes og administreres af DGU.

En borger klagede den 12. maj 2020 til Datatilsynet over DGU's behandling af oplysninger om ham på hjemmesiden *www.golf.dk*. Hjemmesiden brugte en samtykkeløsning, hvor hjemmesidebrugeren havde mulighed for at klikke på »Tillad alle cookies« eller »Vis detaljer«. Ved valg af »Vis detaljer« fik hjemmesidebrugeren præsenteret information om, hvilke cookies hjemmesiden brugte. Det fremgik yderligere, at hvis man fortsatte med at anvende hjemmesiden, samtykkede hjemmesidebrugeren til brug af cookies. Klageren gjorde dermed gældende, at med hjemmesidens samtykkeløsning, var det umuligt at undgå/fravælge cookies.

Det fremgår af artikel 6, stk. 1, litra a i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'), at behandling af personoplysninger er lovlig, hvis den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål. Ved et samtykke forstås enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, jf. databeskyttelsesforordningens artikel 4, nr. 11.

Da klageren ved besøg på hjemmesiden, *www.golf.dk*, ikke kunne afvise at give samtykke, vurderede Datatilsynet, at samtykket ikke kunne anses for frivilligt. Et gyldigt samtykke forudsætter også, at dette er granuleret således at den registrerede frit kan vælge mellem behandlingsformål. Ved samtykket på hjemmesiden blev oplysningerne om klager dog behandlet til flere formål, herunder statistik og markedsføring. Klagerens samtykke var heller ikke udtryk for en utvetydig viljestilkendegivelse, da dette kræver en aktiv handling, jf. sag C-673/17 (Planet49). På baggrund af disse forhold fandt Datatilsynet, at der var grundlag for at udtale alvorlig kritik af DGU's behandling af oplysninger om klager på hjemmesiden *www.golf.dk*, da behandlingen ikke var sket i overensstemmelse med databeskyttelsesforordningens artikel 6, stk. 1, litra a.

Datatilsynet noterede i sin afgørelse, at DGU i medio august 2020 implementerede en ny samtykkeløsning på hjemmesiden, hvor den hjemmesidebesøgende kan vælge mellem »Kun nødvendige« og »Jeg accepterer«.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/nov/ugyldigt-samtykke-paa-hjemmeside

Guldborgsund Kommune indstilles til bøde på 50.000 kr.

Det danske Datatilsyn ('Datatilsynet') har den 9. december 2020 ved politianmeldelse indstillet Guldborgsund Kommune, til en bøde på 50.000 kr. Politianmeldelsen er sket på baggrund af Datatilsynets vurdering af, at Guldborgsund Kommune i forbindelse med et sikkerhedsbrud ikke har udvist den fornødne agtpågivenhed

Datatilsynet blev opmærksom på Guldborgsund Kommunes sikkerhedsbrud, efter de modtog en klage fra en borger i kommunen. Guldborgsund Kommune havde ved en fejl i 2018 sendt en afgørelse via Digital Post, indeholdende oplysninger om klagerens barns opholdssted til barnets far, selvom faren var frakendt forældremyndigheden. Sikkerhedsbruddet medførte store konsekvenser for klageren og klagerens barn. Guldborgsund Kommune havde ikke anmeldt sikkerhedsbruddet til Datatilsynet, eller behørigt underrettet klageren.

Ved indstilling til bødestørrelse har Datatilsynet bl.a. lagt vægt på overtrædelsens karakter og alvor og kravet om, at en bøde i hver enkelt sag skal være effektiv, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning, jf. Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 artikel 83, stk. 9.

Læs hele nyheden her:
https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/dec/kommune-indstillet-til-boede

Datatilsynet udtaler kritik af Køge Kommune

Det danske datatilsyn ('Datatilsynet') har den 8. december 2020 ved afgørelse i sag med journalnummer 2019-423-0207 udtalt kritik af Køge

Kommune, for i et enkelt tilfælde ikke at havde overholdt kravet om anmeldelse af brud på persondatasikkerheden, jf. Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 33, stk. 1.

Afgørelsen blev truffet som led i Datatilsynets planlagte skriftlige tilsyn af Køge Kommune som fokuserede på, om Køge Kommune foretog anmeldelse af brud på persondatasikkerheden i overensstemmelse med databeskyttelsesforordningens artikel 33, stk. 1, og om kommunen opfyldte kravet om at dokumentere alle brud på persondatasikkerheden, jf. artikel 33, stk. 5.

Datatilsynet fandt at Køge Kommune i et enkelt tilfælde ikke levede op til kravet om anmeldelse af brud på persondatasikkerheden til Datatilsynet. Hændelsen blev registreret den 18. juni 2018, hvor der på grund af opbevaring af oplysninger på et fællesdrev uden adgangskontrol, var fri adgang til patientoplysninger i form af tandlægedata, herunder navn, cpr. oplysninger, patientdata og røntgenbilleder.

Køge Kommune anmeldte ikke hændelsen til Datatilsynet med begrundelsen, at der var tale om »ren« informationssikkerhedshændelse samt at det var usandsynligt, at bruddet indebar en risiko for de registrerede og deres rettigheder, da der var minimal risiko for, at nogen ville kende til den specifikke sti til mappen, der indeholdt personoplysningerne.

Datatilsynet vurderede dog, at der henset til kategorierne af de berørte oplysninger og den manglende adgangskontrol var tale om brud på persondatasikkerheden, jf. databeskyttelsesforordningen artikel 4, nr. 12 samt at det ikke var usandsynligt, at der var risiko for de registreres rettigheder. Bruddet skulle dermed have været anmeldt til Datatilsynet, jf. databeskyttelsesforordningen artikel 33, stk. 1.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/dec/tilsyn-med-anmeldelse-af-brud-paa-persondatasikkerheden-koege-kommune

Datatilsynet udtaler alvorlig kritik af Zoologisk Have

Det danske datatilsyn ('Datatilsynet') udtalte den 18. november 2020 alvorlig kritik af Zoologisk Have i København ('København Zoo') i sag med journalnummer 2020-441-4364. Sagen omhandlede et sikkerhedsbrud i et loginsystem, som København Zoo havde udviklet for årskortholdere.

En person tilegnede sig den 2. januar 2020 adgang til København Zoos system. Systemet krævede for log-in en kombination af to numeriske værdier, uden begrænsning i antallet af loginforsøg, hvilket gav personen mulighed for at prøve sig frem til et gyldigt login (brugernavn og adgangskode). Dermed opnåede personen adgang til årskortholderens navn, adresse, kortnummer og e-mail. København Zoo havde på dette tidspunkt 140.000 årskortholdere registreret. Det var herved alt for let at få uretmæssig adgang til personoplysninger om årskortholderne gennem loginsystemet, og loginsystemet var derfor ikke i overensstemmelse med Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 32 om etablering af passende sikkerhedsniveau.

Datatilsynet udtalte endvidere kritik af Københavns Zoos beskrivelse af de foretagne foranstaltninger i forbindelse med databruddet til Datatilsynet samt kommunikation med de registrerede.

Af databeskyttelsesforordningens artikel 33 fremgår det, at den dataansvarlige skal beskrive de foranstaltninger, som den dataansvarlige har truffet for at håndtere et brud på persondatasikkerheden. Dette levede Københavns Zoos kommunikation ikke op til i sagen. København Zoo oplyste, at der var sendt underretning til alle 140.000 årskortholdere men det kom senere frem, at der var sendt underretning til 26.662 e-mailadresser. Det var København Zoos opfattelse, at de registrerede, som ikke fik denne e-mail, blev underrettet via websiden og gennem pressens omtale af sagen. Ved den oprindelige anmeldelse af bruddet til Datatilsynet fremgik denne sondring om underretningens karakter ikke.

Af databeskyttelsesforordningens artikel 34 fremgår det, at den dataansvarlige skal underrette de registrerede om en databrud, hvis databruddet indebærer en høj risiko for de registrerede. Ved København Zoos vurdering af, om bruddet udgjorde en risiko for de registreredes rettigheder, nåede København Zoo frem til, at situationen ikke var omfattet af kravet om underretning efter databeskyttelsesforordningens artikel 34, stk. 1. Datatilsynet vurderede derimod, at bruddet på persondatasikkerheden udgjorde en høj risiko for personer med beskyttet adresse, hvorfor der i hvert fald skulle ske underretning til disse registrerede. Tilmed var de øvrige registrerede blevet udsat for en øget konkret risiko, da København Zoo selv offentliggjorde oplysninger om sikkerhedsbruddet på deres hjemmeside, hvorved disse registrerede fejlagtigt kunne tro at deres oplysninger ikke var i fare for at blive kompromitteret. Efter princippet i databeskyttelsesforordningens artikel 5, stk. 1, hvorefter fejlagtig eller ikke fyldestgørende givet information berigtiges, fandt Datatilsynet, at der også forelå en overtrædelse af artikel 5, stk. 1, litra a.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/nov/sikkerhedsbrud-hos-zoo

Datatilsynet opdaterer vejledning om databeskyttelse i ansættelsesforhold

Det danske datatilsyn ('Datatilsynet') offentliggjorde den 1. decem-

ber 2020 en revideret udgave af vejledningen om regler om databeskyttelse i ansættelsesforhold.

Af de væsentligste ændringer, har Datatilsynet for det første lavet konsekvensrettelser gennem vejledningen på baggrund af tilsynets ændrede praksis om fortolkning af henholdsvis artikel 6 og 9 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'). Den ændrede praksis er fra 2019, og går ud på, at en dataansvarlig, der behandler følsomme oplysninger omfattet af forbuddet i databeskyttelsesforordningens artikel 9, stk. 1, skal kunne identificere en undtagelse til dette forbud i enten forordningens artikel 9, stk. 2, samt et lovligt grundlag for behandling i databeskyttelsesforordningens artikel 6.

For det andet, er der tilføjet et afsnit om tillidsrepræsentantens anvendelse af arbejdsgivers IT-udstyr. Det følger heraf, at tillidsrepræsentanten er selvstændig dataansvarlig for sin behandling. Tillidsrepræsentantens brug af arbejdsgiverens IT-udstyr vil derfor udgøre en særlig form for videregivelse af personoplysninger. Som konsekvens heraf, anbefaler Datatilsynet, at arbejdsgiveren indgår en aftale med tillidsrepræsentanten om adgangen til de personoplysninger, som tillidsrepræsentanten har. Eksempelvis kan aftalen gå ud på, at arbejdsgiver kun kan tilgå personoplysningerne, hvis der sket et sikkerhedsbrud, således at tillidsrepræsentantens fortrolighed ikke undermineres.

For det tredje, har Datatilsynet lavet en række tilføjelser vedrørende kontrol af medarbejdere. Der er tilføjet et nyt afsnit om behandlingshjemlen til at foretage behandling af personoplysninger i forbindelse med en kontrolforanstaltning. Hvis behandlingen sker med baggrund i en DA/LO aftale om kontrolforanstaltninger findes behandlingshjemlen i lov nr. 502 af 23. maj 2018 ('den danske databeskyttelseslov') § 12, stk. 1. Hvis en privat virksomhed, der ikke er omfattet af DA/LO aftale om kontrolforanstaltninger, ønsker at indføre kontrolforanstaltninger af medarbejdere, skal virksomheden finde hjemlen i databeskyttelsesforordningens artikel 6, stk. 1, litra f.

Datatilsynet forventer desuden at påbegynde en yderligere gennemgang og revision af vejledningen i ultimo 2021.

Læs hele nyheden her:
https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/dec/vejledning-om-databeskyttelse-og-ansaettelsesforhold-revideret

Læs den reviderede vejledning her:
https://www.datatilsynet.dk/Media/0/8/Vejledning%20om%20databeskyttelse%20i%20forbindelse%20med%20ans%C3%A6ttelsesforhold.pdf

Datatilsynet udsender vejledning til virksomheder om optagelse af telefonsamtaler

Det danske datatilsyn ('Datatilsynet') offentliggjorde i november 2020 en vejledning om optagelse af telefonsamtaler. Spørgsmålet om optagelse af telefonsamtaler har været forelagt det danske Dataråd, og Datatilsynet har på denne baggrund udarbejdet den nye vejledning.

Formålet med vejledningen er, at imødekomme virksomhedernes ønske om at optage ind- eller udgående telefonsamtaler samt at sikre, at optagelser sker i overensstemmelse med Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') og lov nr. 502 af 23. maj 2018 ('den danske databeskyttelseslov').

Overordnet præciserer den nye vejledning, at der som udgangspunkt sker behandling af personoplysninger, når en virksomhed optager en telefonsamtale f.eks. i forbindelse med virksomhedens telefoniske kundeservice. Da hverken databeskyttelsesforordningen eller den danske databeskyttelseslov indeholder særregler om optagelse af telefonsamtaler, skal eventuelle optagelser ske i overensstemmelse med de generelle databeskyttelsesregler.

Vejledningen fremhæver derfor, at en virksomhed der ønsker at optage en telefonsamtale nøje skal overveje, om det er nødvendigt at indhente et samtykke fra de personer, der deltager i telefonsamtalerne. Nødvendigheden af et samtykke afhænger af formålet med optagelsen. Ifølge vejledningen er de oftest forekomne formål enten uddannelse af medarbejdere eller dokumentation af f.eks. indgåede aftaler. Vejledningen sondrer derfor mellem optagelser i dokumentationsøjemed og optagelser i uddannelsesøjemed, hvor vejledningen gennemgår henholdsvis det lovlige grundlag, opbevaring af telefonsamtaler og de registreredes rettigheder for begge formål.

Overordnet er det ifølge vejledningen Datatilsynets opfattelse, at der kan ske optagelse af telefonsamtaler i dokumentationsøjemed uden samtykke, hvis behovet for at kunne dokumentere samtalens indhold i praksis reelt ikke kan opfyldes på anden vis end ved optagelse af telefonsamtaler. Optagelser i uddannelsesøjemed kan ifølge vejledningen derimod kun ske med den registreredes samtykke, idet optagelse af telefonsamtaler generelt kan være indgribende for den registrerede.

Datatilsynet forventer at komme med vejledning omkring optagelsen af andre former for samtaler, herunder f.eks. optagelse af møder på Zoom, Skype, Teams m.v.

Læs hele vejledningen her:
https://www.datatilsynet.dk/Media/B/F/Optagelse%20af%20telefonsamtaler.pdf

Datatilsynet udtaler alvorlig kritik af Rejsekort for at bruge forkert behandlingsgrundlag

Det danske Datatilsyn ('Datatilsynet') afsagde den 3. november 2020 afgørelse med journalnummer 2019-32-0709 i en sag vedrørende

forkert behandlingsgrundlag samt fortsat behandling af personoplysninger efter samtykke var trukket tilbage.

Sagen startede, da en borger den 19. marts 2019 klagede til Datatilsynet over Rejsekorts manglende sletning af oplysninger om klager. Klager gav i 2015 samtykke til Rejsekorts behandling af dennes oplysninger i forbindelse med bestilling af et personligt rejsekort. Behandlingsgrundlaget for Rejsekorts behandling af personoplysninger om klager var dermed samtykke, jf. artikel 6, stk. 1, litra a i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen').

Den 19. marts 2019 trak klager sit samtykke tilbage. Rejsekort meddelte i den forbindelse, at de var forpligtet til at gemme økonomiske data samt rejsedata i medfør af henholdsvis bogføringsloven og som dokumentation for aftaleforholdet. Rejsekort havde tilrettelagt sin behandling af personoplysninger således, at der skulle ske skift af behandlingsgrundlaget, hvis samtykket blev trukket tilbage, idet Rejsekort fortsat ville behandle oplysninger om klager i medfør af forordningens artikel 6, stk. 1. Rejsekort ville således anvende artikel 6, stk. 1, litra b, c og f, vedrørende klagers aftaleindgåelse, rejsedata, træk/indbetalinger på kortet i forbindelse med klagers benyttelse af sit rejsekort.

Datatilsynet udtalte, at en dataansvarlig som hovedregel ikke må ændre behandlingsgrundlag efter behandlingen er påbegyndt. Herudover fandt Datatilsynet, at behandling af klagers oplysninger fra aftaleindgåelse kunne have været sket på baggrund af artikel 6, stk. 1, litra b, c og f i Databeskyttelsesforordningen, hvorfor samtykke ikke var det mest passende behandlingsgrundlag. Idet samtykke ikke anses som det mest passende behandlingsgrundlag, fandt Datatilsynet, at Rejsekort havde behandlet oplysninger i strid med princippet om lovlighed, rimelighed og gennemsigtighed, jf. artikel 5, stk. 1, litra a i databeskyttelsesforordningen. Dette gav anledning til at udtale alvorlig kritik af rejsekort.

Efter klager havde trukket sit samtykke tilbage fortsatte Rejsekorts behandlingen af klagers oplysninger om aftaleindgåelsen og rejsedata på baggrund af artikel 6, stk. 1, litra b i Databeskyttelsesforordningen. Dette gav også anledning til alvorlig kritik af Rejsekort. Datatilsynet lagde her vægt på, at den fortsatte behandling ikke var i overensstemmelse med Databeskyttelsesforordningen, idet aftaleforholdet mellem rejsekort og klager ophørte, da klager trak sit samtykke tilbage. Herudover var det ikke rimeligt over for klager, da hendes oplysninger oprindeligt blev behandlet på baggrund af samtykke.

Rejsekorts fortsatte behandling af økonomiske oplysninger var derimod i overensstemmelse med databeskyttelsesforordningen. Datatilsynet lagde her vægt på, at det skete med henblik på overholdelse af en retlig forpligtelse i bogføringsloven, hvilket er i overensstemmelse med Databeskyttelseslovens artikel 6, stk. 1, litra c.

Som resultat af sagen skal Rejsekort lave en ny vurdering af behandlingsgrundlaget for personoplysninger om andre end klager. Herudover har Rejsekort fået et påbud om at slette alle oplysninger om klager, som de ikke er forpligtet til at opbevare efter bogføringsloven.

Læs hele afgørelsen her: https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/nov/forkert-behandlingsgrundlag

Datatilsynet afgiver ny vurdering om ukrypterede forbindelser

Det danske datatilsyn ('Datatilsynet') har den 22. oktober 2020 udsendt en nyhed, hvor Datatilsynet har vurderet, at myndigheder og virksomheder ikke bør opfordre borgere til at sende personoplysninger af følsom eller fortrolig karakter over en ukrypteret forbindelse, når myndigheden/virksomheden optræder som dataansvarlig. I relation til indhentning af personoplysninger hos borgerne, kan dette indebære at de dataansvarlige skal etablere sikre transmissionsløsninger.

I sin vurdering tager Datatilsynet for det første stilling til, hvorvidt en myndighed eller virksomhed betegnes som dataansvarlig i situationer, hvor disse opfordrer borgerne til at sende personoplysninger til brug for sagsbehandling. For det andet vurderer datatilsynet, hvilke passende sikkerhedsforanstaltninger dataansvarlige bør træffe i de omtalte situationer.

Datatilsynet vurderer, at man som myndighed og virksomhed betegnes som dataansvarlig for indhentning af personoplysninger hos borgeren, når myndigheden og virksomheden har opfordret borgeren til at sende personoplysninger til brug for sagsbehandling. Her lægger Datatilsynet vægt på, at *»myndighederne og virksomhederne bestemmer formålet med indsamlingen af oplysningerne, herunder eksempelvis hvilke oplysninger der er nødvendige for behandlingen af sagen eller tjenesteydelsen, og med hvilke midler de pågældende oplysninger skal indsamles.«*

Når myndigheder og virksomheder indhenter personoplysninger hos borgerne er disse derfor ansvarlige for at etablere passende sikkerhedsforanstaltninger. I denne sammenhæng vurderer Datatilsynet, at myndigheder og virksomheder på den ene side er ansvarlig for at anbefale borgerne at sende personoplysninger af følsom eller fortrolig karakter via en krypteret forbindelse. På den anden side er myndigheder og virksomheder ikke ansvarlige i en situation, hvor borgeren uopfordret sender oplysninger af fortrolig eller følsom karakter via en ukrypteret forbindelse eller i en situation, hvor borgeren benytter en

ukrypteret forbindelse til trods for en opfordring til at undlade dette.

Afslutningsvist opfordrer Datatilsynet borgere, der er i tvivl om sikkerhedsniveauet på den forbindelse som en myndighed eller virksomhed har opfordret vedkommende til at sende personoplysninger af følsom eller fortrolig karakter igennem, til at kontakte den pågældende myndighed eller virksomhed. Hvis ikke tvivlen afklares, opfordres der til at tage kontakt til Datatilsynet.

Læs hele nyheden her:
https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/okt/maa-man-opfordre-borgere-til-at-bruge-en-ukrypteret-forbindelse

Datatilsynet udtaler alvorlig kritik af NCC's behandling af personoplysninger om en opsagt medarbejder

Det danske datatilsyn ('Datatilsynet') har den 18. juni 2020 ved afgørelse i sag med journalnummer 2019-31-2250 udtalt alvorlig kritik af NCC Danmark A/S ('NCC') for behandlingen af oplysninger om en opsagt medarbejder ('klager') samt manglende opfyldelse af oplysningspligten.

Efter NCC opsagde klager verserede en sag om opsigelsen ved Arbejdsretten, som fik betydelig mediedækning. I den forbindelse udsendte NCC en e-mail til intern orientering til 17 tømrersvende, hvori oplysninger om klager indgik, herunder bl.a. navn, årsag til afskedigelse og fagforeningsmæssigt tilhørsforhold.

Klager gjorde gældende, at NCC's videregivelse af personoplysningerne om klager i e-mailen var i strid med databeskyttelsesforordningen, idet videregivelsen gik ud over, hvad der var nødvendigt for at forfølge en legitim interesse, jf. artikel 6, stk. 1, litra f i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'). Desuden mente klager, at NCC ikke havde opfyldt sin oplysningsforpligtelse overfor medarbejdere, jf. databeskyttelsesforordningens artikel 13 og 14.

NCC bestred, at der var sket videregivelse af oplysningerne med henvisning til, at e-mailen blev sendt til en beskeden kreds af ansatte. I øvrigt anførte NCC, at den interne orientering skyldtes den uro på arbejdspladserne, som fulgte af sagens mediedækning. I forhold til oplysningspligten henviste NCC til, at persondatapolitikken lå på intranettet. Dog erkendte NCC, at ikke alle timeansatte havde adgang til intranettet, hvorfor man fremover ville sende persondatapolitikken særskilt på e-Boks.

Datatilsynet har i sin vurdering af sagen set på, om NCC havde en legitim interesse i at behandle personoplysningerne, jf. artikel 6, stk. 1, litra f i databeskyttelsesforordningen. I øvrigt bemærkede Datatilsynet, at behandling om fagforeningsmæssigt tilhørsforhold er forbudt, medmindre forholdet falder under en af undtagelserne i databeskyttelsesforordningens artikel 9, stk. 2. Ifølge Datatilsynet var forholdet ikke omfattet af artikel 6, idet Datatilsynet lagde vægt på, at NCC's behandling ikke bundede i et hensyn, der knyttede sig til selve afskedigelsen, men nærmere til konflikten ved Arbejdsretten, hvorfor NCC ikke havde en legitim interesse i den interne orientering om afskedigelsen. I øvrigt udtalte Datatilsynet, at behandlingen af samtlige personoplysninger i den pågældende e-mail udgjorde en overtrædelse af artikel 9 om følsomme personoplysninger, idet e-mailen havde overskriften, »3F i pressen«, som i sig selv indebar, at der var tale om behandling af følsomme personoplysninger om fagforeningsmæssigt tilhørsforhold.

Datatilsynet anerkendte, at NCC havde en legitim interesse i at orientere sine medarbejdere om konflikten ved Arbejdsretten. Datatilsynet vurderede dog, at denne orientering godt kunne være sket uden, at der blev behandlet personoplysninger.

For så vidt angår oplysningspligten efter artikel 13 og 14 i databeskyttelsesforordningen bemærkede Datatilsynet, at det ikke er tilstrækkeligt, at persondatapolitikken er tilgængelig på intranettet, hvis ikke den registrerede har modtaget den særskilt eller er blevet henvist til den.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/jun/behandling-af-oplysninger-om-opsagt-medarbejder

Manglende basale test anses som en skærpende omstændighed af Datatilsynet

Det danske Datatilsyn ('Datatilsynet') afsagde den 22. september 2020 afgørelse med journalnummer 2019-431-0037, i en sag vedrørende et sikkerhedsbrud i systemet Fælleskommunalt Ledelsesinformationssystem ('FLIS'), ved levering af data til de danske kommuner.

I perioden december 2018 til februar 2019, modtog Datatilsynet en række anmeldelser fra de danske kommuner vedrørende FLIS, der drives af Kombit A/S. I forbindelse med levering af data fra FLIS til kommunerne, udelod Kombit A/S' underdatabehandler Netcompany A/S ved en fejl et filter i systemet, der skulle begrænse de enkelte kommuners data til kun at omfatte de borgere, som kommunen har ret til at se data på. Fejlen betød, at 84 kommuner og deres tredjepartsleverandører, fik uretmæssigt adgang til personnumre og beskæftigelsesrelaterede oplysninger om op mod 4,2 mio. borgere.

Det følger af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 28, stk. 3, litra f, at databehandleren skal bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af Databeskyttelsesforordningens artikel 32-36, under hen-

synstagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren. Den dataansvarlige og databehandleren skal gennemføre passende tekniske og organisatorisk foranstaltninger for at sikre vedvarende fortrolighed af behandlingssystemer og -tjenester jf. databeskyttelsesforordningens artikel 32, stk. 1. Datatilsynet fandt, at fejlen medførte en uretmæssig videregivelse af bl.a. personnumre og beskæftigelsesrelaterede oplysninger, og at Kombit A/S ikke udførte de fornødne tests i forbindelse med dataudtræk fra FLIS, for at kunne opdage det fejlopsatte filter, der medførte den uretmæssige videregivelse.

På baggrund af dette, fandt Datatilsynet, at der var grundlag for at udtale alvorlig kritik af, at Kombit A/S' behandling af personoplysninger ikke var sket i overensstemmelse med databeskyttelsesforordningens artikel 28, stk. 3, litra f, jf. artikel 32.

For så vidt angår graden af kritik, lagde Datatilsynet i skærpende retning vægt på, at Kombit A/S ved dataudtræk fra FLIS, ikke havde implementeret basale tests, der sikrede at kommunerne kun modtog de nødvendige data. I formildende retning lagde Datatilsynet bl.a. vægt på formålet med kommunernes behandling af personoplysningerne, som er at indsamle ledelsesinformation med henblik på at evaluere kommunens drift, og at videregivelsen kun skete til fagpersoner, der var indforstået med, at oplysningerne skulle behandles med fortrolighed.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/sep/sikkerhedsbrud-i-systemet-flis

EDPB udgiver anbefalinger om yderligere foranstaltninger ved overførsel af personoplysninger til tredjelande

Det Europæiske Databeskyttelsesråd ('EDPB') offentliggjorde den 10. november 2020 anbefalinger om iværksættelse af supplerende foranstaltninger ved overførsel af personoplysninger til tredjelande. Anbefalingerne kommer baggrund af EU-Domstolens dom afsagt den 16. juli 2020 i sag C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ('Schrems II dommen').

I Schrems II dommen understregede EU-Domstolen, at dataeksportører fortsat skal foretage en konkret vurdering af, om beskyttelsesniveauet i det tredjeland, hvor personoplysningerne overføres til, svarer til det beskyttelsesniveau, der er sikret i EU og EØS. Såfremt beskyttelsesniveauet i modtagerlandet ikke er tilstrækkeligt, kræver det »passende supplerende foranstaltninger«, for at overførelsen er lovlig. EDPB's anbefalinger vejleder dataeksportørerne i, hvornår det er nødvendigt at iværksætte de supplerende foranstaltninger samt i givet fald hvilke foranstaltninger, der er passende.

Anbefalingerne indeholder en 6-trins guide ('Roadmap'), som kan hjælpe dataeksportørerne til at vurdere, om der skal iværksættes supplerende foranstaltninger, når de skal overføre personoplysninger til tredjelande. Dataeksportørerne anbefales, at (i) skabe overblik over alle overførelser, (ii) sikre lovligt overførelsesgrundlag, (iii) undersøge modtagerlandets beskyttelsesniveau, (iv-v) udvælge og implementere supplerende foranstaltninger samt (vi) løbende revurdere beskyttelsesniveauet.

EDPB's anbefalinger indeholder endvidere en række eksempler på, hvad en passende supplerende foranstaltning kunne udgøre, og en række betingelser for, hvornår disse anses som effektive. Der fremlægges også en række specifikke scenarier, hvor supplerende foranstaltninger kan være nødvendige. De oplistede eksempler er både af teknisk, kontraktuel og organisatorisk karakter. En supplerende foranstaltning udgør f.eks. kryptering eller pseudonymisering af personoplysningerne, en kontraktmæssig klausul, der binder importøren til ikke have indbygget bagdøre samt forpligtende anvendelse og efterlevelse af standarder og codes of conduct. Listen er ikke udtømmende, og andre foranstaltninger kan efter en konkret vurdering godt være passende.

Læs hele vejledningen her:
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202 001_supplementarymeasurestransferstools_en.pdf

EU Kommissionen præsenterer udkast til reviderede standardkontraktbestemmelser

EU-kommissionen offentliggjorde den 12. november sit udkast til reviderede standardkontraktbestemmelser (SCC'er) for kontrakter mellem databehandlere og dataansvarlige, samt kontrakter om overførsel af personoplysninger til tredjelande.

EU-Kommissionens udkast til SCC'er for overførsel af personoplysninger til tredjelande lægger, i tråd med EU-Domstolens afgørelse i Schrems-II sagen, op til at dataeksportøren skal foretage en vurdering af tredjelandets beskyttelsesniveau, og at der skal foretages en vurdering af, hvilke supplerende foranstaltninger, der vil være hensigtsmæssige at implementere for at beskytte den registreredes rettigheder.

EU-Kommissionens udkast til SCC'er mellem dataansvarlige og databehandlere regulerer behandlingen af personoplysninger inden for EU og har til formål at hjælpe den dataansvarlige med at overholde kravene i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') om indgåelse af databehandleraftaler, herunder de specifikke krav til indholdet af disse aftaler.

Udkastene var indtil den 10. december 2020 i høring. Det Europæiske Databeskyttelsesråd (EDPB)

har sammen med Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) offentligt høringssvar til de to reviderede SCC'er. I udtalelserne foreslås en række konkrete tiltag til forbedringer, herunder at der i SCC'erne for tredjelandsoverførsler uddybes, at det kan være nødvendigt for dataeksportøren at implementere yderligere supplerende foranstaltninger for at sikre et beskyttelsesniveau, der i det væsentligste svarer til beskyttelsesniveauet inden for EU/EØS. Derudover nævner EDPB og EDPS, at det bør forklares tydeligere, hvornår parterne kan anvende SCC'erne som databehandleraftale samt anvendelsen af den såkaldte docking-klausul, som giver tredjeparter adgang til at tiltræde SCC'er og dermed blive forpligtet som en dataansvarlig eller databehandler.

Udkastene forventes vedtaget i starten af 2021.

Find de to udkast her:

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12 741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12 740-Data-protection-standard-contractual-clauses-between-controllers-processors-located-in-the-EU-implementing-act-

EDPB vedtager første artikel 65-afgørelse

Det Europæiske Databeskyttelsesråd ('EDPB') offentliggjorde den 10. november 2020 under det årlige plenarmøde sin første bindende afgørelse om tvistbilæggelse på baggrund af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 65.

Afgørelsen fra EDPB angik en sag hvor den irske tilsynsmyndighed i egenskab af ledende tilsynsmyndighed udstedte udkast til afgørelse mod Twitter International Company ('Twitter') samt de efterfølgende relevante og begrundede indsigelser, som en række af de berørte tilsynsmyndigheder fremsatte, jf. databeskyttelsesforordningens artikel 60, stk. 3. Blandt andet fremsatte de berørte tilsynsmyndigheder relevante og begrundede indsigelser om de overtrædelser af databeskyttelsesforordningen, som det irske datatilsyn havde identificeret, og den rolle, som Twitter spillede som den (eneste) dataansvarlige samt fastlæggelsen af størrelsen af den foreslåede bøde. Særligt databeskyttelsesforordningens artikel 33, stk. 1 og artikel 33, stk. 5 blev undersøgt med hensyn til mangelfuld advarsel om brud på persondatasikkerheden hhv. mangelfuld dokumentation af bruddet.

Da den irske tilsynsmyndighed afviste indsigelserne fra de berørte tilsynsmyndigheder og/eller fandt, at de ikke var »relevante og begrundede«, blev sagen henvist til EDPB i overensstemmelse med artikel 60, stk. 4, i databeskyttelsesforordningen og indledte dermed tvistbilæggelsesproceduren. EDPB fandt i sin afgørelse, at den forslåede bøde var for lav og at det irske datatilsyn skulle revurdere bødeniveauet.

Den irske tilsynsmyndighed kunne derefter meddele Twitter, at man havde fundet brud på databeskyttelsesforordningens artikel 33, stk. 1 og artikel 33 og kvitterede disse med en bøde på 450.000 EUR som et effektivt, proportionalt og afskrækkende tiltag.

Læs hele afgørelsen her:

https://edpb.europa.eu/news/news/2020/first-edpb-art-65-decision_da

Tue Goldschmieding er partner i Gorrissen Federspiel og en av de danske redaktørene for Lov&Data.

Delphi

Lovisa Lennström

Sanktionsavgift mot Polismyndigheten för användning av applikation för ansiktsigenkänning

Den svenska Integritetsskyddsmyndigheten (IMY) meddelade den 11 februari 2021 efter tillsyn enligt brottsdatalagen att Polismyndigheten ska betala en sanktionsavgift om 2,5 miljoner kronor efter att ha använt applikationen Clearview AI för ansiktsigenkänning. IMY förelade vidare Polismyndigheten att informera de registrerade vars personuppgifter matats in i Clearview AI, radera uppgifter som matats in i applikationen i den utsträckning det är möjligt samt vidta utbildningsåtgärder och övriga organisatoriska åtgärder för att säkerställa att personuppgifter inte behandlas i strid med gällande dataskyddslagstiftning.

Applikationen Clearview AI tillhandahålls av en amerikansk leverantör och möjliggör för användare att ladda upp bilder som genom biometri matchas mot ett mycket stort antal bilder på internet, inklusive från sociala medier. Användaren får sedan ett resultat i form av webbadresser där eventuella matchningar kan hittas.

IMY:s tillsyn inleddes under våren 2020 efter uppgifter i media om att svenska myndigheter kunde ha använt applikationen. Polismyndigheten ombads besvara om myndigheten använt sig av applikationen och med stöd av vilken rättslig grund behandlingen i så fall genomförts. Av yttranden från Polismyndigheten framgick att applikationen hade använts av vissa anställda inom myndigheten, men att applikationen inte tillhandahållits av Polismyndigheten.

En fördjupad tillsyn genomfördes därefter av IMY som kom fram till att Polismyndigheten var ansvarig för tre överträdelser av brottsdatalagen. IMY uttalade i beslutet att den stora mängden personuppgifter, även känsliga sådana, som myndigheten behandlar samt de långtgående maktbefogenheter Polismyndigheten har gör att myndigheten har ett särskilt ansvar för att personuppgifter behandlas korrekt. IMY konstaterade vidare att behandlingen föll inom Polismyndighetens personuppgiftsansvar trots att anställda självständigt använt applikationen utan att den tillhandahållits av myndigheten.

Den första överträdelsen som IMY identifierade var att polisen inte vidtagit tillräckliga tekniska och organisatoriska säkerhetsåtgärder vid användningen av Clearview AI. Polismyndigheten hade inte kunnat dela med sig av fullgott underlag såsom styrdokument för anställda avseende personuppgiftsbehandling, utbildningar för interna rutiner eller andra instruktioner avseende hur anställda får använda program och applikationer inom verksamheten. Faktumet att anställda använt sig av applikationen i strid med gällande reglering visade enligt IMY även att gällande interna rutiner inte varit tillräckliga.

Den andra överträdelsen bestod i att biometriska uppgifter (i form av ansiktsigenkänning) hade hanterats i strid med brottsdatalagen. IMY konstaterade att inga rättsliga bedömningar hade gjorts innan applikationen började användas. Exempel på bedömningar som borde ha gjorts är hur länge uppgifterna sparas, hur matchningarna går till och om uppgifterna överförs till länder utanför EU/EES. IMY betonade även det strikta krav på nödvändighet som uppställs i brottsdatalagen för behandling av biometriska personuppgifter. Mot bakgrund av att användningen av applikationen innebar att enskildas biometriska uppgifter matchades mot stora mängder bilder som ofiltrerat inhämtats från internet ansågs enligt IMY:s bedömning det strikta kravet på nödvändighet inte vara uppfyllt.

Slutligen bedömde IMY att Polismyndigheten borde ha genomfört en konsekvensbedömning innan behandlingen påbörjades. Detta mot bakgrund av den risk för den personliga integriteten som behandlingen medförde då användningen av tjänsten innebar att biometriska uppgifter, innefattande ansiktsigenkänning, behandlades med ny teknik tillhandahållen av en extern aktör i ett tredje land.

Ansiktsigenkänningsteknik har blivit alltmer populärt och fått fler användningsområden de senaste åren. IMY:s beslut visar dock på hur känslig sådan teknik är ur ett integritetsperspektiv.

Lovisa Lennström är associate i Advokatfirman Delphi, Stockholm.

Gorrissen Federspiel

Tue Goldschmieding

Højesteret afgør, at Ørsted A/S ikke kan forbydes at benytte navnet »Ørsted«

Den danske Højesteret (»Højesteret«) har den 30. november 2020 afgjort, at selskaber hverken med henvisning til lov nr. 767 af 7. august 2019 ('den danske navnelov'), lov nr. 88 af 29. januar 2019 ('den danske varemærkelov'), lov nr. 763 af 23. juli 2019 ('den danske selskabslov') eller lov nr. 164 af 26. februar 2014 ('den danske internetdomænelov') kan forbydes at bruge navnet »Ørsted«

DONG Energy A/S skiftede i efteråret 2017 navn til Ørsted A/S, og de øvrige selskaber i energikoncernen optog også »Ørsted« eller »Orsted« som en del af deres selskabsnavne m.v. Appellanterne i sagen bærer alle efternavnet Ørsted og er direkte efterkommere af videnskabsmanden Hans Christian Ørsted eller hans bror, Jacob Albert Ørsted. Sagen angik spørgsmålet om, hvorvidt anvendelsen af navnet »Ørsted« som selskabsnavne, binavne, varemærker og internetdomæner, hvori indgår navnet Ørsted eller Orsted, er i strid med appellanternes ret til efternavnet Ørsted.

Højesteret fandt, at selvom navnet Ørsted er et beskyttet efternavn efter den danske navnelov, angår navnelovens forbud mod uberettiget benyttelse af en andens navn alene krænkelser, der består i anvendelsen af en andens navn som personnavn, eller hvad der må sidestilles hermed, og ikke som selskabsnavn eller varemærke. Højesteret tiltrådte derudover, at der ved anvendelsen af navnet Ørsted sigtes til den for længst afdøde videnskabsmand Hans Christian Ørsted, hvorfor varemærket »Ørsted« ikke er udelukket fra registrering efter den danske varemærkelov. Højesteret tiltrådte endvidere, at der ikke er grundlag for at fortolke en snævrere adgang til at benytte en andens efternavn i et selskabsnavn end der er for at benytte varemærker efter varemærkeloven. Der var herunder ikke grundlag for at nægte et kapitalselskab at benytte sit varemærke som selskabsnavn efter den danske selskabslov. Sidst fandt Højesteret ikke grundlag for at forbyde at bruge varemærkerne Ørsted og Orsted som domænenavne, da Ørsted A/S m.fl. aktivt anvendte de omtvistede domænenavne, og da der ikke var nedlagt påstand om, at domænenavnene skulle overføres til appellanterne.

Appellanterne fik derfor ikke med henvisning til hverken navneloven, varemærkeloven, selskabsloven eller lov om internetdomæner medhold i deres påstande om, at de indstævnte selskaber skulle slette registreringen af deres selskabs- og binavne, eller at det skulle forbydes dem at bruge disse navne eller deres varemærker. Den danske Sø- og Handelsret var nået til samme resultat.

Læs resume af afgørelsen her: https://domstol.fe1.tangora.com/Domsoversigt-(H%C3%B8jesteretten).31 478.aspx?recordid31 478=2027

Et ophavsretligt beskyttet værk er ikke »overført til almenheden« ved elektronisk indgivelse til en domstol

EU-Domstolen afsagde den 28. oktober 2020 dom i sag C-637/19 mellem BY og CX. Sagen angik et præjudicielt spørgsmål fra den svenske appeldomstol i patent- og handelsretlige sager, angående fortolkningen af begrebet »overføring til almenheden« i artikel 3, stk. 1 i direktiv 2001/29/EF af 22. maj 2001 om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet (»InfoSoc-direktivet«).

Ved første instans i Sverige blev det fastslået, at et fotografi, der var indgivet til en domstol som et procesdokument, var spredt til almenheden i den svenske ophavsretslovs forstand. Alle kunne anmode om at få adgang til det, på grundlag af de gældende svenske regler om aktindsigt.

EU-Domstolen præciserede, at der ved fremsendelse af en elektronisk kopi via e-mail ikke er tale om »spredning«, men »overføring«.

Efter EU-Domstolens praksis skal et værk, for at være overført til almenheden, være overført til et betydeligt antal potentielle modtagere. EU-Domstolen fandt, at en overførsel til en domstol anses for at være rettet mod en klart defineret og lukket kreds af mennesker, der udøver deres funktioner i offentlighedens interesse og ikke et ubestemt antal potentielle modtagere. At der er adgang til aktindsigt i det pågældende dokument er uden betydning, da InfoSoc-direktivets arti-

kel 9 fastslår, at direktivet ikke vedrører reglerne om aktindsigt i offentlige dokumenter. Desuden fremhævede EU-Domstolen, at ophavsretten ikke er absolut, men skal afvejes i forhold til de andre grundlæggende rettigheder, herunder retten til effektive retsmidler.

På den baggrund konkluderede EU-Domstolen, at artikel 3, stk. 1 i InfoSoc-direktivet skal fortolkes således, at begrebet »overføring til almenheden« ikke omfatter elektronisk indgivelse af et beskyttet værk til en domstol som bevismiddel i et søgsmål mellem privatpersoner.

Læs hele afgørelsen her:

http://curia.europa.eu/juris/document/document.jsf?text=&docid=233 005&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=17 795 389

EU-Domstolen afsiger dom i sag om »reel brug« af varemærker

EU-Domstolen har den 22. oktober 2020 truffet afgørelse i de forenede sager C-720/18 og C-721/18 mellem Ferrari SpA og DU. Sagerne, der fra den regionale appeldomstol i Düsseldorf i Tyskland var anmodninger om præjudiciel afgørelse, drejede sig om fortolkningen af artikel 12, stk. 1 om fortabelsesgrunde i tidligere gældende Europa-Parlamentets og Rådets direktiv 2008/95/EF af 22. oktober 2008 om indbyrdes tilnærmelse af medlemsstaternes lovgivning om varemærker ('varemærkedirektivet').

De forelagte spørgsmål skulle benyttes til at behandle Ferraris appel af Landgericht Düsseldorfs afgørelse, hvoraf Ferraris varemærke »testarossa«, som var registreret i to forskellige registre i klasse 12, blev dømt til at skulle slettes, idet Ferrari inden for en sammenhængende periode på fem år, ikke havde gjort reel brug af disse og derfor havde fortabt retten til varemærkerne. Bortset fra en enkelt model i år 2014 havde Ferrari alene benyttet varemærkerne siden år 1996 til at sælge reservedele og brugte modeller mv. Hovedspørgsmålet var derfor, om salg af disse varer kunne udgøre reel brug.

Det første og tredje spørgsmål forelagt EU-Domstolen angik, hvorvidt et registreret varemærke i en bred kategori af varer, her motorbiler, også ville kunne udgøre reel brug af varemærket i tilfælde, hvor varemærket kun benyttes for nogle varer i kategorien, herunder luksus sportsvogne. Hertil bemærkede EU-Domstolen, at forbrugerens opfattelse af markedssegmentet vil være afgørende.
EU-Domstolen overvejede varemærkeindehaverens legitime interesse i at kunne udvide sit sortiment inden for kategorien og betydningen af, at produktet kan have flere formål. I nærværende afgørelse anskuedes, at en Ferrari både tjener et formål som sportsvogn, herunder kan anvendes til bilsport, men samtidig også kan benyttes som enhver anden motorbil til almindelig vejtransport. EU-Domstolen kom frem til, at der ikke tydeligt kunne identificeres en underkategori uden at dette ville begrænse Ferraris rettigheder. Desuden var det af betydning, at der, selvom der blev produceret et mindre antal af varer i kategorien, ikke var tale om et symbolsk registreret varemærke, men at der faktisk skete brug i overensstemmelse med varemærkets funktion.

Om det andet spørgsmål, hvorvidt varemærkeindehaverens salg af brugte varer ville udgøre en reel brug af varemærket, i forhold til den omhandlede artikel, bemærkede EU-Domstolen, at et varemærke som udgangspunkt bruges, når det af indehaveren anbringes på en ny vare ved første markedsføring af denne vare. EU-Domstolen konkluderede dog på baggrund af artikel 7 i det tidligere gældende varemærkedirektiv om konsumption af rettigheder, at eftersom varemærkeindehaveren ikke kan forbyde tredjemand i at bruge varemærket ved videresalg, kan et varemærke ved indehaverens eget videresalg være genstand for reel brug, når dette bruges til at garantere oprindelsen af varerne.

Det fjerde spørgsmål omhandlede, hvorvidt tjenesteydelser relateret til de varer, der tidligere var blevet markedsført under varemærket, men uden at varemærket blev benyttet i forbindelse med tjenesteydelsen, kunne udgøre reel brug af varemærket fra indehaverens side. EU-Domstolen bemærkede i den forbindelse, at dette ville være tilfældet for tjenesteydelser, der er direkte forbundet med de varer, der har været omfattet under den tidligere brug af varemærket.

Afslutningsvist blev det af EU-Domstolen konstateret, at det er varemærkeindehaveren, der har bevisbyrden for, at et varemærke har været genstand for reel brug efter art. 12, stk. 1, i direktiv 2008/95.

Læs hele afgørelsen her:

http://curia.europa.eu/juris/document/document.jsf?text=&docid=232 724&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=17 795 389

Novo Nordisk idømt bøde på 500.000 kr. og skal betale erstatning for sammenlignende markedsføring uden fagligt belæg

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 1. december 2020 dom i sagen BS-230/2020-SHR, med Sanofi A/S og Sanofi-Aventis Deutschland GmbH ('Sanofi') som sagsøger og Novo Nordisk A/S ('Novo Nordisk') som sagsøgte. Sanofi havde nedlagt erstatnings- og bødepåstand mod Novo Nordisk på baggrund af en pressemeddelelse udsendt af Novo Nordisk i september 2019, hvor Novo Nordisk sammenlignede sit eget basalinsulinpræparat, Tresiba, med Sanofis tilsvarende præparat, Toujeo.

Pressemeddelelsen omhandlede resultaterne fra CONCLUDE-studiet, og angav at Tresiba havde en generelt lavere risiko for hypoglykæmi (for lavt blodsukker) og lavere HbA1c sammenlignet med insulin glargin E300 (Toujeo) for type 2-diabetikere. Sanofi nedlagde derfor påstande om, at Novo Nordisk skulle forbydes at anvende denne formulering, at Novo Nordisk skulle berigtige meddelelsen, og at Novo Nordisk skulle betale erstatning og vederlag på 1.149.112 kr. til Sanofi samt en bøde for overtrædelse af lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov') §§ 20 og 21.

Sagen skulle vurderes efter lovbekendtgørelse nr. 99 af 16. januar 2018 ('den danske lægemiddellov') og den danske markedsføringslov. Den danske lægemiddellov § 66, stk. 1, nr. 1 foreskriver, at der ikke må reklameres for receptpligtige lægemidler, hvilket omfatter både Tresiba og Toujeo. Den danske markedsføringslov indeholder i § 20, stk. 1 og 3 forbud mod henholdsvis vildledende handelspraksis mellem erhvervsdrivende og aggressiv eller utilbørlig handelspraksis over for andre erhvervsdrivende, § 21, stk. 2, nr. 2 og 5 foreskriver, at sammenlignende reklame bl.a. er tilladt, når sammenligningen angår produkter, der tjener samme formål, og når sammenligningen ikke miskrediterer eller nedvurderer en konkurrents varemærker, firmanavne, aktiviteter etc.

Novo Nordisk bestred hverken Sanofis to første påstande om, at Novo Nordisk skulle forbydes at benytte den nævnte formulering om sammenligning af de to præparater, eller at offentliggørelse af meddelelsen var retsstridig. Novo Nordisk bestred dog de øvrige påstande om berigtigelse, erstatning og bødestraf. Retten nåede frem til, at pressemeddelelsen var i strid med den danske lægemiddellovs § 66, stk. 1, nr. 1, hvorfor den ligeledes var i strid med god markedsførings- og erhvervsskik, jf. den danske markedsføringslovs § 3, stk. 1 og 4. Retten fandt, at pressemeddelelsen var egnet til at vildlede og påvirke efterspørgslen af Toujeo i en negativ retning og skade Sanofis renommé, hvorfor Novo Nordisk havde overtrådt markedsføringslovens § 20, stk. 1 og 3 samt § 21, stk. 2, nr. 2 og 5.

Sø- og Handelsretten dømte herved i overensstemmelse med Sanofis påstande og idømte Novo Nordisk, at selskabet skulle berigtige pressemeddelelsen gennem de samme informationskanaler, som den oprindelige meddelelse var sendt ud gennem. Tilmed tilpligtedes Novo Nordisk at betale erstatning og vederlag på 500.000 kr. til Sanofi samt en bøde på 500.000 kr.

Læs hele afgørelsen her:
https://domstol.fe1.tangora.com/media/-300 011/files/Dom.pdf

Dansk virksomhed havde misbrugt finsk virksomheds forretningshemmeligheder angående måleapparater

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 21. august 2020 dom i sagen BS-9719/2017-SHR mellem Valmet Automation Inc ('VA') og EMCO Controls A/S ('EC'). Sagen angik spørgsmålet om, hvorvidt EC's salg og markedsføring af visse måleapparater, samt måleapparater med tilhørende software til ledningsevnemåling, krænkede VA's rettigheder efter lov nr. 309 af 25. april 2018 ('den danske lov om forretningshemmeligheder'), lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov') eller lovbekendtgørelse nr. 1144 af 23. oktober 2014 ('den danske ophavsretslov'), idet EC angiveligt havde brugt VA's forretningshemmeligheder i udviklingen af sin software.

For så vidt angår lov om forretningshemmeligheder fandt Sø- og Handelsretten, at VA's software var et resultat af en kompliceret og tidskrævende udviklingsproces, der efter det oplyste hos VA samlet strakte sig over fire år, og som VA tilstrækkeligt havde forsøgt at hemmeligholde. Oplysningerne var derfor omfattet af den danske lov om forretningshemmeligheder § 2, nr. 1.

I spørgsmålet om softwaren sondrede retten mellem EC's ældre (1511-1705) og nyere (1711-1903) softwareversioner. Det blev vurderet, at de ældre af EC's softwareversioner (1511-1705) lignede VA's software så meget, at det var usandsynligt, at softwaren var udviklet helt uafhængigt af hinanden, samt at EC har gjort brug af VA's software på en sådan direkte måde, at der har været tale om en egentlig kopiering af softwarens funktionalitet. EC fandtes herefter, at have overtrådt den danske lov om forretningshemmeligheder § 4, stk. 2-4. Den nyere software afveg så meget fra VA's software, som man kunne forvente for uafhængigt udviklet software, hvorfor retten vurderede, at EC ikke havde draget en sådan fordel af VA's forretningshemmeligheder, at EC havde overtrådt den danske lov om forretningshemmeligheder § 4. Med henvisning til EC's overtrædelse af lov om forretningshemmeligheder fandt retten, at EC havde handlet i strid med god markedsføringsskik og dermed overtrådt den danske markedsføringslovs § 3. Om den ophavsretlige beskyttelse bemærkede Sø- og Handelsretten, at ophavsretlig beskyttelse ikke knytter sig til idéer eller principper, hvorfor VA's software ikke var ophavsretligt beskyttet.

Sø- og Handelsretten tog herefter VA's påstand om forbud mod salg, og påbud om tilbagekaldelse til følge, for så vidt angår softwareversionen 1511-1705, og fandt ligeledes, at VA var berettiget til rimeligt vederlag og erstatning som følge af EC's ulovlige udnyttelse af VA's forretningshemmeligheder, jf. den danske lov om forretningshemmeligheder § 15 og den danske markedsføringslovs § 24, stk. 2 og 3.

Læs hele afgørelsen her:

http://domstol.fe1.tangora.com/media/-300 011/files/BS-9719-2017-SHR_-_Dom.pdf?rev1

Influent har betalt en bøde på 60.000 kr. for at lave skjult reklame på sin blog og Instagram

Forbrugerombudsmanden anmeldte i 2019 en dansk influent til politiet for at have overtrådt forbuddet mod skjult reklame i lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov') ved ikke at have markeret kommercielle opslag tilstrækkeligt på vedkommendes blog og Instagram. Influenten accepterede at betale en bøde på 60.000 kr.

Forbrugerombudsmanden vurderede i sin behandling af sagen, at influenten i perioden fra marts 2017 til december 2018 havde offentliggjort 17 kommercielle opslag om blandt andet skønhedsbehandlinger, restaurantbesøg og tøj- og skomærker på sin blog og Instagram-profil, der ikke var tilstrækkeligt markeret som reklame. I ét tilfælde var det slet ikke oplyst, at opslag indeholdt reklame, mens den danske influent i andre tilfælde eksempelvis havde markeret kommercielle opslag med »#Ad«, »#spons« eller »#GAW«. Ifølge Forbrugerombudsmanden var markeringerne ikke tilstrækkelige til at sikre, at opslagene ville blive opfattet som reklame af dem, der læste opslagene.

Forbrugerombudsmanden vurderede samtidig, at den danske influent, der havde et stort antal følgere, måtte anses som værende erhvervsdrivende i den danske markedsføringslovs forstand. Dermed havde den danske influent et selvstændigt ansvar for at sikre, at det tydeligt fremgik, hvis et opslag indeholdt kommercielle budskaber, jf. den danske markedsføringslovs § 6, stk. 4.

Fremover anbefaler Forbrugerombudsmanden, at såfremt et opslag indeholder reklame, uden det fremgår tydeligt af opslaget, bør influenten tydeligt markere opslaget med »reklame«, »annonce«, eller et lignende ord, som modtagerne klart opfatter som en reklamemarkering.

Læs pressemeddelelsen her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2020/influent-betaler-boede-paa-60 000-kroner-for-skjult-reklame/

Tre webbutikker er blevet stævnet og politianmeldt, idet de har trukket DKK 89 om måneden fra brugernes konti uden at oplyse herom

Den danske forbrugerombudsmand ('Forbrugerombudsmanden') valgte den 9. november 2020 på baggrund af flere end i alt 450 klager, at politianmelde tre webbutikker, »buuks.dk«, »pluus.dk« og »sayve.dk« for vildledende markedsføring af abonnementer, idet webbutikkerne havde trukket DKK 89 på sine kunders konti for en abonnementsservice uden, efter Forbrugerombudsmandens opfattelse, at have oplyst kunderne tydeligt herom.

Forbrugerombudsmandens stævning var rettet mod de tre virksomheder alle med den samme ejerkreds og direktør, der drev webbutikkerne, og sagen blev anlagt ved den danske Sø- og Handelsret med krav om, at virksomhederne skulle tilbagebetale alle indbetalinger fra forbrugerne, der inden for en periode på tre år, havde betalt for et abonnement eller en vare på en af de tre webbutikker.

Forbrugerombudsmanden henviste i sin stævning til lov nr. 1457 af 17. december 2013 ('den danske forbrugeraftalelov') § 12, stk. 2, hvor det fremgår, at såfremt en fjernsalgsaftale bliver indgået ved hjælp af elektroniske midler, og forbrugeren bliver pålagt en betalingsforpligtelse, skal dette være angivet klart og tydeligt på det sted, hvor bestillingen afgives. Desuden følger det af den danske forbrugeraftalelovs § 12, stk. 1, at det skal fremgå tydeligt på den webbutik, hvor bestillingen afgives, at forbrugeren pålægges en betalingsforpligtelse, såfremt dette er tilfældet. Tilmed skal forbrugeren oplyses om abonnementets pris pr. måned, bindingsperiode og betingelserne for at opsige abonnementet, inden vedkommende afgiver den endelige bestilling.

Læs pressemeddelelsen her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2020/forbrugerombudsmanden-staevner-tre-webbutikker/

Domænenavnet »joy-mogensen.dk« skulle overdrages til klageren

Det danske klagenævn for domænenavne ('Klagenævnet for Domænenavne') traf den 11. september 2020 afgørelse i sag 2020-0161, mellem Kultur- og kirkeminister, Joy Mogensen og Socialdemokratiet ('klager') og rapperen, Nikoline ('indklagede'). Klagenævnet for Domænenavne fandt frem til, at domænet 'joy-mogensen.dk' skulle overføres til klager.

Klager gjorde gældende, at indklagedes brug af domænenavnet stred imod god domænenavnsskik, jf. § 25, stk. 1 i lov nr. 164 af 26. februar 2014 ('den danske domænelov'). Til støtte herfor bemærkede klager, at domænenavnet blev brugt kommercielt til at vise musikvideo til indklagedes sang 'Gourmet', hvilket ifølge klager udgjorde uberettiget snyltning på klagers navn. Indklagede havde ingen reel, beskyttelsesværdig eller anerkendelsesværdig interesse i at bruge domænenavnet. Desuden havde indklagede ingen tilknytning til navnet 'Joy Mogensen'.

Indklagede gjorde gældende at domænet ikke havde et kommercielt formål, men nærmere et kunstnerisk tilsnit. Derved kunne der ifølge indklagede ikke være tale om snyltning. Desuden bemærkedes, at domænet ikke i sig selv kan skabe indtjening for indklagede. Formålet med musikvideoen såvel som registreringen af domænet var at skabe

samfundsdebat og *»omgå sociale mediers drabende censurregler«*. I øvrigt gjorde indklagede en række politiske argumenter gældende og kritiserede i den forbindelse både Joy Mogensen, Regeringen og politikere i øvrigt.

Klagenævnet for Domænenavne diskuterede først om der forelå en krænkelse af § 27 i lovbekendtgørelse nr. 767 af 7. august 2019 ('navneloven') om brug af navne og betegnelser, som er egnet til at sætte navnet eller betegnelsen i forbindelse med bestemte individer, og som er egnet til at skabe forveksling. Klagenævnet for Domænenavne bemærkede, at der ifølge Danmarks Statistik er to eller færre personer i Danmark med navnet 'Joy Mogensen', og at klager gennem sit politiske virke har gjort brug af navnet, således at navnet er blevet et identifikationsmiddel for netop klageren som person. Indklagede havde ikke gjort holdepunkter gældende, der talte for indklagedes retmæssige brug af navnet. Derved fandt Klagenævnet for Domænenavne, at indklagedes brug af domænet 'joy-mogensen.dk' var i strid med navnelovens § 27. Derfor havde indklagede ingen loyal interesse i registreringen, hvorfor registreringen var i strid med god domænenavnsskik.

Læs hele afgørelsen her: https://www.domaeneklager.dk/sites/default/files/2020-09/2020-0161%20joy-mogensen.dk%20-%20anonymiseret.pdf

Tue Goldschmieding er partner i Gorrissen Federspiel og en av de danske redaktørene for Lov&Data.


simonsen vogtwiig

Emile Schjønsby-Nolet og
Hedda Baumann Heier

Ikrafttredelse av lov om vern av forretningshemmeligheter

Lov nr. 15 av 27. mars 2020 om vern av forretningshemmeligheter trådte i kraft 1. januar 2021. Loven implementerer direktiv (EU) 2016/943 og avløser de tidligere bestemmelsene i markedsføringslovens §§ 28 og 29 og straffelovens §§ 207 og 208.

Les hele loven i Lovdatas database.

Ikrafttredelse av ny bestemmelse i kringkastingsloven

Kringkastingslovens § 4-7 trådte i kraft 1. januar 2021. Den nye lovbestemmelsen gir Medietilsynet adgang til å gi pålegg om å «hindre eller vanskeliggjøre» tilgangen til ulovlig markedsføring av pengespill, lotteri mv. Pålegg kan gis overfor «den som eier eller disponerer nett som formidler fjernsyn eller audiovisuelle bestillingstjenester». Pålegg kan ikke gis dersom Medietilsynet finner at det vil være «uforholdsmessig». Det er alminnelig antatt at Medietilsynet i første omgang vil søke å benytte bestemmelsen for å få norske TV-distributører til å stanse sending av spillreklame fra utenlandske kringkastere, men lovbestemmelsens nedslagsfelt er vidt nok formulert til at den i teorien også kan dekke tilbydere av internettilgang.

Les § 4-7 i kringkastingsloven i Lovdatas database.

Høring om norsk implementering av digitalmarkedsdirektivet mv.

At EU har rettet blikket mot den digitale økonomien i det indre markedet har resultert i flere direktiver og forordninger, herunder direktiv (EU) 2019/790 og 2019/789. Den norske regjeringen har igangsatt arbeidet med å gjennomføre disse direktivene i norsk rett, og publiserte den 18. desember 2020 en liste med spørsmål knyttet til direktivene og til visse andre temaer. Berørte aktører inviteres til å komme med skriftlige innspill innen 26. mars 2021.

Les Kulturdepartementets pressemelding og liste med spørsmål her: *https://www.regjeringen.no/no/aktuelt/kulturdepartementet-ber-om-innspill-til-gjennomforing-av-digitalmarkeds-direktivet-mv.-i-norsk-rett/id2 815 352/*

Høring om ny lov om digitale ytelser

Den 3. desember 2020 sendte Justisdepartementet forslag til ny lov om levering av digitale ytelser til forbrukere på høring. Lovforslaget er ment å gjennomføre direktiv (EU) 2019/770 i norsk rett. I tillegg til reglene fra direktivet foreslår lovgiver også flere særnorske regler, herunder regler om direkte krav mot tidligere salgsledd, at eventuell bindingstid normalt ikke skal overstige 6 måneder og at forbrukeren skal kunne kreve erstatning for «ikke ubetydelig ulempe» (altså selv om det ikke foreligger noe økonomisk tap). Høringsfristen er satt til 3. mars 2021.

Les Justisdepartementets pressemelding og høringsnotatet her: *https://www.regjeringen.no/no/aktuelt/foreslar-egen-forbrukerkjopslov-for-digitale-ytelser/id2 789 551/*

Ny dom om balansegangen mellom ytringsfrihet og retten til eget bilde

Den 4. januar 2021 avsa Borgarting lagmannsrett dom i sak LB-2019-111 926. Faktum av saken var, i korte trekk, at politiet stanset en kappkjøring mellom en hvit Porsche Carrera og en svart Audi (rundt 200 km/t). Sjåføren av Porschen var tidligere var anmeldt for å ha oppbevart våpen i bilen. Politiet valgte derfor å foreta en kroppsvisitering og sjåføren fant det passende å filme hendelsen. Politimannen som ble filmet gav beskjed om at han ikke ønsket at filmen skulle legges ut på sosiale medier. Sjåføren valgte likevel å publisere bildene på nettplattformen Instagram.

Saken reiste spørsmål om forholdet falt under unntaksbestemmelsene i åndsverkslovens § 104 bokstav a til e. Sjåføren viste særlig til at bokstav a åpner for publisering av fotografi der «avbildningen har aktuell og allmenn interesse». Sjåføren mente at politibetjenten «oppførte seg ufyselig» og skal ha vagt ubehag som «ikke var representativ for den måten politiet skal oppføre seg». Dette stod i skarp kontrast med de øvrige bevisene, bla. opptak fra dashbordkameraet i politibilen. Til tross for at alt pekte mot at politimannen *ikke* fremstod som truende, mente lagmannsretten at politiets utøvelse av offentlige tjeneste som utgangspunkt er i allmenhetens interesse. Dette ble begrunnet i ønsket om å sikre tillitten til politiets arbeid. Sammenholdt med at videoen kun viste ansiktet i noen få sekunder, og at politimannen for øvrig var anonymisert konkluderte retten med at sjåførens publisering av politimannen var lovlig.

Les hele avgjørelsen med saksnummer LB-2019-111 926 i Lovdatas database. I skrivende stund vites det ikke om avgjørelsen er rettskraftig.

Emile Schjønsby-Nolet er advokatfullmektig i Advokatfirmaet Simonsen Vogt Wiig AS, Oslo
Hedda Baumann Heier er senioradvokat i Advokatfirmaet Simonsen Vogt Wiig AS, Oslo.


Bird & Bird

Joel Tholin & Louise Kleerup

Medupphovsman döms för upphovsrättsbrott efter att olovligen ha tillgängliggjort kortfilmer via sin YouTube-kanal

Bakgrund

Patent- och marknadsöverdomstolen har nyligen meddelat dom där en medupphovsman döms för upphovsrättsintrång efter att olovligen ha tillgängliggjort kortfilmer via sin YouTube-kanal. Bakgrunden till fallet var ett hobbyprojekt där några vänner spelade in ett antal kortfilmer och tillgängliggjorde dessa via en gemensam YouTube-kanal. Efter en konflikt vännerna emellan, valde en av de inblandade att på egen hand till viss del redigera filmerna (huvudsakligen introt och eftertexterna) och därefter tillgängliggöra verken från sin egna YouTube-kanal, vartill denne även länkade från sin webbplats. Patent- och marknadsdomstolen hade tidigare gjort bedömningen att upphovsrätten till filmverken tillkom samtliga de inblandade gemensamt och att den tilltalade medupphovsmannen hade förfogat över verken utan samtliga övriga upphovsmäns samtycke, och därigenom av grov oaktsamhet hade begått upphovsrättsintrång. De inblandade parterna valde att överklaga domen till Patent- och marknadsöverdomstolen.

Patent- och marknadsöverdomstolens bedömning

Patent- och marknadsöverdomstolen fastslog inledningsvis, likt underrätten, att samtliga av kortfilmerna utgjorde upphovsrättsskyddade filmverk. Vad avser frågan vem eller vilka som kunde vara att anse som rättighetsinnehavare till verken konstaterade domstolen följande. I eftertexterna till originalversionerna av filmverken, som inledningsvis tillgängliggjordes via vännernas gemensamma YouTube-kanal, angavs de inblandade vännerna gemensamt som manusförfattare och regissörer. Av eftertexterna i originalversionerna framgick vidare att en av vännerna hade agerat som skådespelare medan en annan hade ansvarat för foto, ljus och musik. I de redigerade versioner som hade laddats upp på den tilltalades egna YouTube-kanal saknades dock denna information. Domstolen gjorde bedömningen att det inte fanns något i målet som gav stöd för att eftertexterna i originalversionerna inte återgav de verkliga förhållandena. De inblandades personliga bidrag i den skapande processen på det sätt som angavs i de ursprungliga eftertexterna ledde därför till slutsatsen att de inblandade personerna var att betrakta som upphovsmän och att upphovsrätten därför tillkom dem gemensamt.

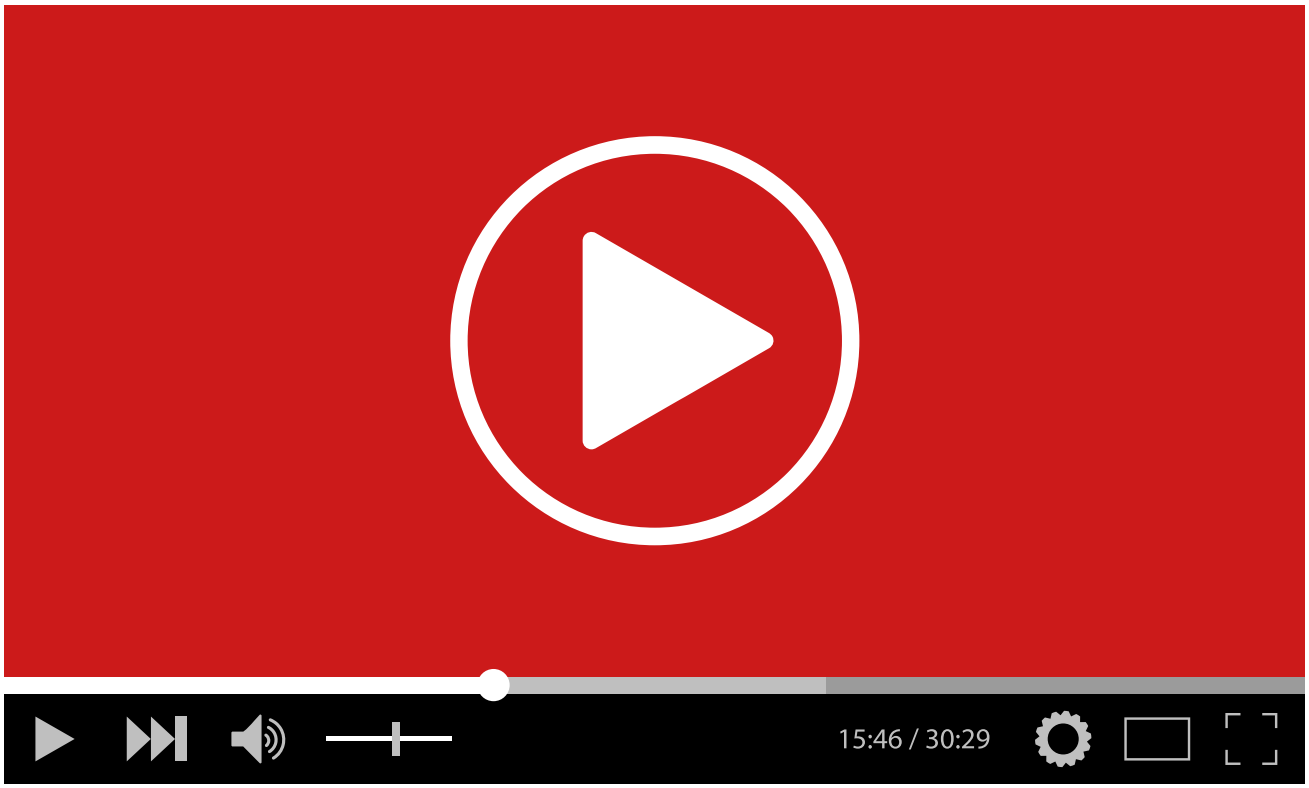
Nästa fråga som domstolen tog ställning till var om den tilltalade hade begått upphovsrättsintrång genom dennes förfoganden av filmverken. Domstolen fastslog i detta avseende att den tilltalade, genom att kopiera filmerna och till viss del redigera dessa samt att ladda upp de bearbetade verken på sina egna YouTube-kanal och länka till dem från sin webbplats, hade framställt exemplar och tillgängliggjort dessa för allmänheten i en upphovsrättslig mening. Då upphovsrätten till filmverken tillkom de inblandade parterna gemensamt skulle ett sådant förfogande förutsätta samtliga upphovsmäns medgivande. Den tilltalade gjorde här gällande att han hade rätt att förfoga över verken då det fanns ett sådant medgivande, alternativt att en överlåtelse av övriga medupphovsmäns förfoganderätt kunde anses ha skett. Domstolen konstaterade att medgivande till sådana förfoganden på upphovsrättens område som regel ska tolkas i ljuset av den så kallade specifikationsprincipen och att ett medgivande i form av överlåtelse eller upplåtelse, inte kan anses ha skett om det inte uttryckligen av omständigheterna framgår att så är fallet. Eventuella oklara överlåtelser eller upplåtelser ska tolkas restriktivt och till den överlåtande eller upplåtande upphovsmannens fördel. I förevarande fall konstaterade domstolen att det å ena sidan var fråga om ett icke-kommersiellt hobbyprojekt, där det kunde anses vara rimligt att avtal slöts muntligt eller konkludent. Upphovsmännen verkade dock båda inom filmbranschen vilket enligt domstolen å andra sidan, beaktat det karriärmässiga risktagande ett avstående av varje form av kontroll av tillgängliggörande av verken

innebar, talade emot att ett generellt medgivande till förfogande hade skett. Sammantaget gjorde domstolen bedömningen att det inte hade förelegat något samtycke.

Domstolen förde vidare fram att ett olovligt förfogande av ett verk i propagandasyfte eller i ett politiskt sammanhang som upphovsmannen vill ta avstånd ifrån generellt skulle kunna utgöra en försvårande omständighet. Av förhör med en av medupphovsmännen framgick att denne inte ville bli förknippad med den tilltalades YouTube-kanal som denne ansåg var av politisk karaktär. Domstolen konstaterade dock att det inte var visat vilket ändamål som den tilltalade hade haft med att driva kanalen. Tillgängliggörandet av kortfilmerna ansågs därmed inte ha främjat något visst politiskt syfte såsom en försvårande omständighet.

I likhet med underinstansen kom domstolen till slutsatsen att den tilltalade, genom att inte försäkra sig om att samtliga övriga medupphovsmän tillät exemplarframställning och överföringar till allmänheten, hade handlat grovt oaktsamt. Genom dessa olovliga förfoganden hade den tilltalade således gjort sig skyldig till upphovsrättsbrott för vilket denne dömdes till dagsböter. Därtill ålades även den tilltalade att till medupphovsman erlägga skälig ersättning för det otillåtna utnyttjandet. I påföljdsfrågan framhöll domstolen att förfogandet att en intrångsgörare själv framställer sig som producent och lanserar en annan upphovsmans verk i eget namn generellt är att anse som en försvårande omständighet. Detsamma i förhållande till att överföringen till allmänheten, under den tilltalades kontroll, hade skett över en lång tidsperiod, över tre år. Att den intrångsgörande parten själv var medupphovsman samt att de tidigare gemensamt hade offentliggjort filmverken, förvisso icke-bearbetade, gjorde det dock mindre allvarligt. Även att det olovliga förfogandet inte hade skett i vinstsyfte och att det var fråga om kortfilmer med låga produktionskostnader kunde betraktas som förmildrande omständigheter.

Joel Tholin, Associate & Louise Kleerup, Trainee, Bird & Bird Advokat.



Returadresse:
Lovdata
Pb. 6688 St. Olavs plass
NO-0129 Oslo
Norge

Nytt fra

LOVDATA

LOVDATA
PRO

Karnov Lovkommentarer – direkte integrert i Lovdata Pro

Karnov og Lovdata har inngått en unik samarbeidsavtale om å utvikle et digitalt oppslagsverk for juridisk litteratur, sømløst integrert i Lovdata Pro. Karnov vil lansere lovkommentarer til de største og mest brukte lovene i Norge høsten 2021. Kommentarene skrives av landets fremste jurister. Samtlige innehar spesialkunnskap om det rettsområdet de skriver om.

Noen av rettsområdene hvor de mest sentrale lovene blir dekket:

- Arbeidsrett
- Forvaltningsrett
- Strafferett
- Utdanningsrett
- Helserett
- EØS-rett
- Familierett

Skandinavisk tyngde

Med sin erfaring som ledende innen juridiske informasjonstjenester i både Danmark og Sverige, har Karnov Group Skandinavia en unik kunnskapsbase og kompetanse til å utvikle tilsvarende tjenester i Norge.

Med Karnov Lovkommentarer blir rettskildene i Lovdata Pro beriket med enda mer verdifullt innhold, som gjør Lovdata Pro til et komplett juridisk oppslagsverk og arbeidsverktøy.

Tilgang krever egen avtale med Karnov Group Norway AS.

pro.lovdata.no

Produksjon: 07 Media AS