Lov & Data

Nr. 139
September 2019
Nr. 3/2019

Innhold

Lov&Data

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

Lovdata
Postboks 2016 Vika
NO-0125 Oslo, Norge
Tlf.: +47 23 11 83 00
Faks: +47 23 11 83 01
E-post: lovogdata@lovdata.no
Nettside: www.lovdata.no

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

Abonnementspriser for 2019
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

Blant de viktigste nyhetene for tiden, finner man forliket inngått mellom Facebook og Federal Trade Commission. Bakgrunnen er først og fremst Cambridge Analytica-saken, hvor personopplysninger ble misbrukt for å påvirke utfallet av det amerikanske valget i 2016, i favør av Donald Trump. Cambridge Analytica ble for øvrig ledet av Alex Nix, som i 2018 ble filmet mens han forklarte hvordan man kan bruke bestikkelser og prostituerte for å diskreditere politiske motstandere.

Anklagene mot Facebook gjelder blant annet villedende opplysninger om bruk av ansiktsgjenkjenning. Facebook sin informasjon til brukerne fastslo at dette var basert på «opt-in», mens man i realiteten måtte skru funksjonen av dersom man ikke ønsket å være del av opplegget. Mer alvorlig var det at Facebook ga villedende opplysninger om hvordan apper fra tredjeparter samlet informasjon om Facebook-vennene til den som installerte appen. Det var dette som gjorde det mulig for Cambridge Analytica å innhente opplysninger om intetanende (og dermed ikke-samtykkende) Facebook-brukere.

Dette ble gjort ved at brukere ble invitert til å aktivere en app for å gjennomføre en personlighetstest. Det ble hevdet at opplysningene kun skulle brukes i akademisk øyemed. I realiteten samlet appen også informasjon om vennene til den som installerte appen, og informasjonen ble altså brukt til helt andre formål enn det som var oppgitt.

Forliket går ut på at Facebook skal betale en bot på 5 milliarder dollar, og skal underkaste seg enkelte restriksjoner i bruk av personopplysninger. Boten setter verdensrekord når det gjelder straff for misbruk av personopplysninger. Likevel reagerte markedet med å sende Facebooks aksjekurs opp. Dette har sammenheng med to forhold.

For det første, beløpet er egentlig ikke så stort, når man tar i betraktning at Facebook sin økonomi ligger på en helt annen skala enn vi er vant til å tenke på. For det andre, markedet hadde (med god grunn) forventet sterke restriksjoner i Facebooks bruk av personopplysninger. Som en amerikansk

demokrat ville ha sagt, FTC sin reaksjon er «too little, too late».

Det beste som kommer ut av Cambridge Analytica-saken er antakelig at naive sjeler som ofte har sagt «Jeg har da ikke noe å skjule», (kanskje) får en liten oppvåkning. Selv om man ikke har noe å skjule på individuelt nivå, kan summen av personopplysninger misbrukes på en samfunnsskadelig måte, som for eksempel å hjelpe Donald Trump til å bli verdens mektigste mann. Om du er blant de som aldri har åpnet Facebook sine innstillinger for personvern, så er du herved oppfordret! Og neste gang du får tilbud om å aktivere en tredjeparts-app som skal gjennomføre en «personlighetstest», bør du kanskje avstå.

Jarle Roar Sæbø

Styrets ansvar for aksjeselskapets etterlevelse av GDPR

Av Emilie Aasheim

Emilie Aasheim

Personvern er et viktig ideal å sikre og når selskaper behandler personopplysninger forvaltes viktige verdier. Dette har blitt enda tydeligere med innføringen av ny personvernforordning i EU (GDPR), som i Norge er inkorporert i ny personopplysningslov.[1] Det er i samfunnets interesse at de selskapene som forvalter disse verdiene ledes på en forsvarlig måte.[2] Når personopplysninger forvaltes og behandles i stadig større grad og på nye måter, samtidig som et nytt og strengere regelverk om personvern gjør seg gjeldende, aktualiseres spørsmålet om selskapenes ansvar for personvernet. Det er følgelig sentralt å se på om styrets plikt til forsvarlig forvaltning av selskapet etter aksjeloven § 6-12[3] også innebærer et ansvar for å sikre selskapets etterlevelse av GDPR.

Fokus skiftes med GDPR fra forhåndskontroll hos tilsynsmyndighetene etter tidligere regelverk til ansvarlighet hos selskapet selv.[4] Ansvarsprinsippet kommer til uttrykk i en rekke bestemmelser i forordningen. Det følger av forordningens fortale avsnitt 79 at vern av de registrertes rettigheter krever en tydelig fordeling av ansvar i henhold til forordningen. GDPR stiller strenge krav til at selskapene kan dokumentere at kravene i forordningen etterleves og til at selskapene kan vise at de har «orden i eget hus».

Pliktsubjekt og behandlingsansvarlig etter GDPR

Den behandlingsansvarlige er en «*fysisk eller juridisk person*» som «*alene eller sammen med andre bestemmer formålet med behandlingen*», jf. GDPR artikkel 4 nr. 7. Det er den behandlingsansvarlige som pålegges plikter etter GDPR.[5]

Det er selskapet som subjekt og juridisk person som anses å være ansvarlig for behandlingen av personopplysninger i henhold til personvernforordningen.[6] Når GDPR plasserer ansvaret hos selskapet selv, og det med selskap her siktes til aksjeselskap, må ansvarsplasseringen tolkes i lys av aksjelovgivningen. Styret er selskapets øverste ledelse, og har etter asl. § 6-12 et særskilt ansvar for forsvarlig forvaltning av selskapet. Det formelle ansvaret for at de plikter som pålegges den behandlingsansvarlige oppfylles ligger naturlig hos selskapets styre, som selskapets representant og øverste ledelse.[7] Personvern er en kritisk del av virksomhetens risikostyring og samfunnsansvar. Personvernspørsmål berører hele virksomheten.

> Når personopplysninger forvaltes og behandles i stadig større grad og på nye måter, samtidig som et nytt og strengere regelverk om personvern gjør seg gjeldende, aktualiseres spørsmålet om selskapenes ansvar for personvernet

1 Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven). Det følger av personopplysningsloven § 1 at personvernforordningen gjelder som norsk lov.

2 Norsk anbefaling for eierstyring og selskapsledelse (2018) s. 6.

3 Lov 13. juni 1997 nr. 44 om aksjeselskaper (aksjeloven).

4 Innst. 278 L (2017-2018) s. 8.

5 Rüker, Daniel og Tobias Kugler. *New European General Data Protection Regulation – A Practitioner's Guide,* 1. utg. Tyskland: C.H. Beck – Hart – Nomos, 2018, s. 24.

6 Rüker, Daniel og Tobias Kugler. *New European General Data Protection Regulation – A Practitioner's Guide,* 1. utg. Tyskland: C.H. Beck – Hart – Nomos, 2018, s. 105.

7 Ansvaret vil naturlig i praksis delegeres, men styret har det øverste ansvaret.

Dette i kontrast til en tradisjonell tankegang om at personvern sikres i IT-avdelingene. Nytt personvernregelverk gjør at ansvaret for å sikre selskapets etterlevelse av personvernregelverk må løftes inn på styrerommene.

Styrets ansvar etter aksjeloven § 6-12

Det følger av aksjeloven § 6-12 første ledd første punktum at «[f]orvaltningen av selskapet hører under styret». Styret skal sørge for «*forsvarlig organisering av virksomheten*». Bestemmelsen stadfester styrets forvaltningskompetanse og styrets forvaltningsplikt.

Styret har ansvaret for at selskapet drives innenfor de rammer som følger av lov, vedtekter og generalforsamlingens beslutninger.[8] Som generelt krav gjelder at forvaltningen av selskapet skal være forsvarlig. Dette forutsettes i lovens ansvarsbestemmelser, herunder reglene om styremedlemmenes erstatningsansvar i asl. § 17-1.[9] Når styret etter asl. § 6-12 gis ansvar for at selskapet drives innenfor rammene som følger av lov, ligger det i dette et ansvar for å forsikre seg om at selskapet implementerer og etterlever gjeldende regelverk.

Hva som anses å være forsvarlig forvaltning av selskapet, og hvilke krav som stilles til styret for å oppfylle denne plikten, må ses i lys av samfunnsutviklingen og de eksterne krav som stilles til selskapets virksomhet. Det er en kontinuerlig prosess å vurdere hva som ligger i forventningen om og plikten til forsvarlig forvaltning av selskapet fra styrets side. Endringer i rammlovgivningen, eksempelvis i personvernregelverket, kan medføre endringer i hvordan asl. § 6-12 tolkes og forstås.[10] Dette viser bestemmelsens dynamiske karakter og rolle som rettslig standard.

> Personvernspørsmål berører hele virksomheten

Styret har det øverste ansvaret for å ivareta selskapets samfunnsansvar.[11] GDPR har ført til bevisstgjøring rundt personvern i samfunnet, og tydeliggjort hvilke verdier selskapene forvalter når de behandler personopplysninger. Når samfunnet setter personvern på dagsorden medfører dette også en skjerpelse av forventningene til hvordan selskapet ledes. Varslingslovutvalget har anbefalt at brudd på personvernregelverket og informasjonssikkerhet anses som kritikkverdig forhold som arbeidstaker har rett til å varsle om.[12] Dette underbygger at brudd på personvernregelverket av samfunnet er ansett uønsket, og viser viktigheten av at selskapene etterlever gjeldende personvernregelverk på en tilfredsstillende måte.[13] De skjerpede forventningene fra samfunnet får betydning for hvor terskelen ligger for hva som anses som forsvarlig forvaltning av selskapet fra styrets side etter asl. § 6-12.

Styret forvalter selskapet på vegne av aksjonærene og styrevervet er et tillitsverv for hele selskapsinteressen.[14] Hvilke interesser som anses som legitime selskapsinteresser endres i takt med nye forventninger fra ansatte, samfunnet rundt og nye krav gjennom eksterne lovregler. Det er i selskapets samlede interesse at kravene i GDPR etterleves. Ved brudd på forordningens krav risikerer selskapet bøtelegging og økonomisk tap, hvilket igjen kan få betydning for aksjonærenes økonomiske interesser.[15] Videre vil det kunne være tale om omdømmetap for selskapet dersom det blir kjent at selskapet ikke etterlever kravene for å sikre personvernet. Sett hen til at personvern berører tilnærmet alle sider av selskapets virksomhet, er personvern å anse som en legitim selskapsinteresse styret kan og må ta hensyn til i sitt arbeid og under sitt forvaltningsansvar i medhold av asl. § 6-12.

Dersom styret ikke involveres i implementering og etterlevelse av personvernforordningen, øker risikoen for at etterlevelse av personvernregelverk ikke prioriteres nedover i organisasjonen. Styret anfører «the tone at the top» i selskapet og skaper holdninger for de ansatte i selskapet som står for den daglige behandlingen av personopplysningene.[16] Styret har således, i tillegg til sitt lovfestede forvaltningsansvar, et ansvar for å skape god personvernkultur i selskapet.

Sentrale bestemmelser etter GDPR hvor styrets ansvar aktualiseres

Artikkel 24 – den behandlingsansvarliges ansvar

Den behandlingsansvarlige skal etter artikkel 24 gjennomføre «*egnede tekniske og organisatoriske tiltak*» for å sikre etterlevelse av forordningen. Det følger av annet ledd at tiltak nevnt i første ledd bør omfatte den behandlingsansvarliges «*iverksetting*

8 Bråthen, Tore. (2015) «Kommentar til Aksjeloven» i *Norsk Lovkommentar, Gyldendal Rettsdata,* note 1082 og Woxholt, Geir. *Selskapsrett,* 4. utg., Oslo: Gyldendal, 2012, s. 201.

9 Knudtzon, Sigurd. "Corporate governance I et rettslig perspektiv, I *Corporate governance i et norsk perspektiv,* Øyvind Thorsby (red.), Oslo, 2004, s. 107.

10 Innholdet i styrets plikt til forsvarlig forvaltning av selskapet etter asl. § 6-12 får betydning for vurderingen av styremedlemmenes erstatningsansvar etter asl. § 17-1.

11 Norsk anbefaling for eierstyring og selskapsledelse (2018) s. 37.

12 NOU 2018: 6 s. 157.

13 NOU 2018: 6 s. 132.

14 Reiersen, Hedvig Bugge. *Ansvarsbegrensning og ansvarsfrihet i aksjeselskaper,* Bergen: Fagbokforlaget, 2007, s. 21.

15 Se GDPR artikkel 83 om Datatilsynets adgang til å ilegge bøter ved brudd på forordningen.

16 Skullerud, Åste Marie Bergseng, Cecilie Rønnevik, Jørgen Skorstad og Marius Eng Pellerud. *Personvernforordningen (GDPR) Kommentarutgave,* Oslo: Universitetsforlaget, 2018, s. 170.

av egnede retningslinjer for vern av personopplysninger».

Iverksetting av retningslinjer for behandling av personopplysninger etter artikkel 24 annet ledd må ses i sammenheng med asl. § 6-12 annet ledd, hvor det fremgår at styret i nødvendig utstrekning «*kan*» fastsette retningslinjer for virksomheten. Det følger av forarbeidene at styret selv må avgjøre om det skal gis retningslinjer, og hvilke spørsmål retningslinjene skal regulere.[17]

Det ble i forarbeidene til asl. § 6-12 annet ledd drøftet om fastsettelse av retningslinjer skulle gjøres obligatorisk for styret.[18] En slik plikt ble ikke lovfestet fordi en ville vinne erfaringer med bestemmelsen. Når GDPR stiller krav til utarbeidelse av retningslinjer ut over det som følger direkte av aksjeloven, tyder dette på at styret ikke «*kan*» men *må* fastsette retningslinjer for vern av personopplysninger. Personvernforordningen er lex specialis til aksjeloven slik at plikten for styret til å fastsette retningslinjer etter GDPR artikkel 24, går foran styrets skjønnsmessige adgang til å iverksette retningslinjer etter asl. § 6-12 annet ledd. Selskapets ulike retningslinjer for vern av personopplysninger må derfor forankres i styret. Dette støttes av en uttalelse fra EU-kommisjonen, hvor det fremgår at det i prosessen med å sikre etterlevelse av GDPR er viktig å involvere selskapets øverste ledelse i utarbeidelsen av retningslinjer for etterlevelse av forordningen.[19]

Artikkel 30 – protokoller over behandlingsaktiviteter

Den behandlingsansvarlige skal «*føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar*» jf. GDPR artikkel 30. Protokollen skal blant annet inneholde informasjon om formålet med behandlingen, kategorier av personopplysninger og registrerte, tidsfrister for sletting, og en beskrivelse av de tekniske og organisatoriske sikkerhetstiltak. Artikkel 30 representerer et viktig ledd i selskapets internkontroll, all den tid en oversikt over hvilke personopplysninger som behandles på hvilken måte er sentralt for å fastslå om forordningens krav etterleves.

> Dersom styret ikke involveres i implementering og etterlevelse av personvernforordningen, øker risikoen for at etterlevelse av personvernregelverk ikke prioriteres nedover i organisasjonen

God internkontroll og effektiv risikostyring bidrar på sikt til å sikre aksjonærenes investering og selskapets eiendeler, hvilket igjen er i styrets interesse. Protokollen gir styret en oversikt over hvordan selskapet behandler personopplysninger. Styret må kjenne sin virksomhet og de verdier som forvaltes for å kunne vite hvilke risiki selskapet må sikre seg mot, og hvordan. Forsvarlighetskravet i asl. § 6-12 første ledd annet punktum innebærer et generelt krav til løpende vurdering og håndtering av selskapets risikoforhold.[20] Styret skal påse at selskapet har god internkontroll og hensiktsmessige systemer for risikostyring, og bør årlig foreta en gjennomgang av selskapets internkontroll og risikoområder.[21]

Artikkel 32 – informasjonssikkerhet

Kravene til kontinuerlig arbeid med informasjonssikkerhet skjerpes med GDPR. Artikkel 32 fastslår at det skal gjennomføres «*egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet*» sett hen til risikoen.

Styret har det overordnede ansvaret for selskapets økonomi og et ansvar i selskapets ressursbruk jf. asl. § 6-12 tredje ledd. Når artikkel 32 stiller krav til at det skal oppnås et tilfredsstillende sikkerhetsnivå for behandling av personopplysninger, har styret et ansvar i å bevilge midler og allokere ressurser nettopp til disse formål i medhold av sitt forvaltningsansvar etter asl. § 6-12.

Forvaltningsansvaret pålegger styret aktiv handling på overordnet nivå i saker som er av uvanlig art eller vesentlig betydning, og som går ut over den vanlige drift av virksomheten, jf. asl. § 6-14 annet ledd jf. § 6-12. Dersom det foreligger brudd på informasjonssikkerheten etter GDPR artikkel 32 vil dette kunne ha store konsekvenser for selskapet, både for de registrertes rettigheter og for selskapets interne anliggender. Datainnbrudd vil i mange tilfeller være av stor betydning for selskapet, slik at dette må forelegges styret for behandling.

Artikkel 38 – personvernombudets stilling

Datatilsynet anbefaler alle virksomheter å utnevne personvernombud, uavhengig av om selskapet pålegges dette etter forordningen.[22] Personvernombudet skal informere og gi råd til den behandlingsansvarlige og de ansatte som behandler personopplysninger om de forpliktelser som pålegges selskapet etter forord-

17 NOU 1996: 3 s. 137 og Ot.prp. nr. 23 (1996-1997) s. 147.
18 Ot.prp. nr. 23 (1996-1997) s. 137.
19 Communication 52018DC0043 (2018) s. 9.
20 Eriksen, Birthe. *Arbeidstakers rett til å varsle om «kritikkverdige forhold» etter arbeidsmiljøloven § 2-4(1),* (Doktorgradsavhandling) Bergen, 2015, s. 344.
21 Norsk anbefaling for eierstyring og selskapsledelse (2018) s. 37.
22 Datatilsynets veileder. *Personvernombud etter nytt regelverk* (2017) s. 3 og GDPR artikkel 37.

ningen, jf. artikkel 39 første ledd a.[23] Personvernombudet er uavhengig i sin stilling og kan ikke instrueres av styret.[24]

Personvernombudet skal kontrollere etterlevelse og selskapets retningslinjer for etterlevelse. Styret har et ansvar i å sikre at personvernombudet gis de nødvendige ressurser for å utføre sine oppgaver. Også når et selskap har personvernombud hviler det overordnede juridiske ansvaret for at personvernlovgivningen følges på den behandlingsansvarlige, styret.[25]

Etter artikkel 38 nr. 3 siste setning skal personvernombudet rapportere «*direkte til det høyeste ledelsesnivået hos den behandlingsansvarlige*». Dette for å sikre at ledelsen holdes informert om relevante forhold som kan ha betydning for om selskapet etterlever sine plikter etter forordningen.[26] På denne måten overlates ansvaret for å følge opp mulige brudd på forordningen til selskapets styre.[27] I medhold av sin plikt til forsvarlig forvaltning av selskapet plikter styret å handle på rapport dersom personvernombudet rapporterer at det i selskapet foreligger brudd, eller forhold som kan lede til brudd, på forordningen.

Avsluttende betraktninger

Styret som organ, er, i medhold av sin plikt til forsvarlig forvaltning av selskapet i asl. § 6-12, primæransvarlig for selskapets etterlevelse av GDPR. Styret er behandlingsansvarlig etter GDPR og pålegges en rekke nye plikter. Mange av pliktene etter forordningen er likevel en videre utvikling av de plikter som allerede ligger til styret i dag. GDPR utvider og presiserer enkelte av disse pliktene, blant annet ved at det stilles strengere krav til dokumentert etterlevelse. Det kan få store konsekvenser dersom styret ikke involverer seg tilstrekkelig i virksomhetens håndtering av personopplysninger. Det gjelder både risikoen for omdømmetap og for økonomiske sanksjoner som bøter, personlig erstatningsansvar for styremedlemmene eller erstatningsansvar for tredjemannstap.[28]

Styremedlemmene har en generell plikt til å fremme selskapets interesse og til å forvalte selskapet etter asl. § 6-12. Styret handler på selskapets vegne og skal fremme hva som er best for selskapet og ivareta selskapets interesser.[29] Å drive et aksjeselskap innebærer økonomisk risiko, og styret har handlingsrom for å ta forretningsrisiko i beslutninger som gjelder driften av selskapet.[30] Her er det imidlertid tale om etterlevelse av lovverk. Den forretningsrisiko som styret kan ta kan ikke gå på akkord med lovpålagte plikter. Manglende implementering og etterlevelse av GDPR er ikke innenfor rammene av tillatt risiko.

Personvernforordningen er for mange av kravene risikobasert, slik at hvilke tiltak som må iverksettes for å sikre etterlevelse vil variere med typen selskap, typen og mengden av personopplysninger som behandles, hvilke risiki selskapet står overfor med videre. Det kan for styret i mange tilfeller være vanskelig å vite hva som er «godt nok». Styret har et overordnet ansvar og må holdes informert, være delaktig og stille de rette spørsmålene. Avvik fra forsvarlig forvaltning foreligger først der styret inntar en posisjon hvor de ikke vil engasjere seg, ikke legger til rette for eller ikke gir selskapet mulighet til å etterleve forordningens krav.

En mer overordnet konsekvens av rettsutviklingen er at personvernforordningen trolig vil få betydning for styrets sammensetning og kompetanse. Når det stilles nye krav til at styret skal arbeide aktivt med etterlevelse av personvernregelverket, vil det gi seg utslag i hvilket kompetansebehov som oppstår i styret. Kravet til styret er forankret i GDPR som eksternt lovkrav, men også fra samfunnet rundt når personvern er satt på agendaen. Det blir stadig viktigere å dyrke personvern som en del av selskapskulturen, og arbeidet må starte på toppen, hos styret.

GDPR innebærer en utvidelse og skjerpelse av styrets plikt til forsvarlig forvaltning av selskapet etter asl. § 6-12, ved at styret må innta en aktiv og temmelig konkret rolle i arbeidet med å sikre etterlevelse av GDPR. Styret må være bevisst sitt ansvar og være delaktig i prosessene med implementering og etterlevelse. På sikt vil dette tjene selskapet på flere måter, særlig viktig er det at solid etterlevelse av personvernregelverket vil styrke selskapets omdømme.

Emilie Aasheim er personvernrådgiver i Bane NOR, Oslo.

23 Rüker, Daniel og Tobias Kugler. *New European General Data Protection Regulation – A Practitioner's Guide,* 1. utg. Tyskland: C.H. Beck – Hart – Nomos, 2018, s. 175.

24 Datatilsynets veileder. *Hva betyr de nye personvernreglene for din virksomhet?* (2016) s. 10.

25 Datatilsynets veileder. *Personvernombud etter nytt regelverk* (2017) s. 13 og Skullerud, Åste Marie Bergseng, Cecilie Rønnevik, Jørgen Skorstad og Marius Eng Pellerud. *Personvernforordningen (GDPR) Kommentarutgave,* Oslo: Universitetsforlaget, 2018, s. 232.

26 Rüker, Daniel og Tobias Kugler. *New European General Data Protection Regulation – A Practitioner's Guide,* 1. utg. Tyskland: C.H. Beck – Hart – Nomos, 2018, s. 184.

27 Rüker, Daniel og Tobias Kugler. *New European General Data Protection Regulation – A Practitioner's Guide,* 1. utg. Tyskland: C.H. Beck – Hart – Nomos, 2018, s. 184 og Skullerud, Rønnevik, Skorstad m.fl. (2018) s. 233.

28 Se GDPR artikkel 82 og 83 og asl. § 17-1.

29 Aarum, Kristin Normann. *Styremedlemmers erstatningsansvar i aksjeselskaper*, Oslo: Gyldendal, 1994, s. 349.

30 Aarum, Kristin Normann. *Styremedlemmers erstatningsansvar i aksjeselskaper*, Oslo: Gyldendal, 1994, s. 120.

Legal tech-trender 2019

Av Fredrik Svärd

Undersökningar visar att innovativ förmåga, kostnadseffektivitet och transparens står högt i kurs hos köpare av juridisk rådgivning. Digitaliseringen av juristbranschen drivs inte bara på av förändrade klientbeteenden utan också av ökad komplexitet och regleringstakt. I kölvattnet av den europeiska dataskyddsreformen lanserades exempelvis en rad verktyg för att underlätta compliancearbetet, och idag talas det om privacytech som en egen bransch.

Reuters bedömer att legal techmarknaden kommer vara värd mer än en biljon kronor nästa år. Här är några av de viktigaste trenderna att hålla reda på 2019:

1. Advokatbyråerna – AI, smarta kontrakt och fasta priser

Artificiell intelligens kan användas för dokumentgranskning- och automation, för informationssökning och för att skapa ordning i stora informationsmängder. Andra tillämpningsområden är projekthantering, kostnadsprognoser, förutsägelser om utgången i processer samt kommunikation med omvärlden via chatbotar. Brottsbekämpande myndigheter och säkerhetsföretag har på sina håll börjat använda tekniken för att förutspå var brott kan komma att begås, och inom exempelvis IT-säkerhets- och försäkringsbranscherna används den för att upptäcka hot och bedrägerier.

Många advokatbyråer har nu investerat i AI-verktyg och inte sällan utsett innovationsansvariga. Samtidigt uppger byråledare och konsulter inte sällan att verktygen främst används i lärosyfte.

Advokatbyråer har också intresserat sig för blockchainbaserade smarta kontrakt, ett antal byråer har exempelvis anslutit sig till Enterprise Ethereum Alliance. Vid sidan av detta fortsätter implementeringen av andra verktyg, som klientportaler och verktyg för projekthantering.

Fredrik Svärd

Flera startups arbetar med att ta fram marknadsplatser för juridisk rådgivning, inte sällan med möjlighet för köpare att lämna omdömen. Fasta priser och andra alternativ till timdebitering fortsätter att vinna mark.

Skaran av rådgivare som av olika skäl ställer sig utanför advokatsamfunden är liten men växande. I Sverige har finska Fondia vuxit, liksom konsumenttjänster som Avtal24.

2. Bolagsjurister investerar i teknik

Företagens juristavdelningar investerar allt mer i IT-verktyg, åtminstone i USA. Verktyg för dokumentautomation förekommer, men i första hand rör det sig verktyg för e-signaturer, compliancearbete samt projekthantering.

Företrädare för teknikföretag har också bildat ett legal operations-konsortium med fokus på bl a KM, dataanalys, IT-investeringar och strategisk planering i syfte att optimera det juridiska arbetet. Rörelsen arrangerar nu konferenser även i Europa.

3. Investeringar och konsolidering

Investerare har historiskt närmat sig branschen med försiktighet, men för några år sedan såg vi något av ett trendbrott. I Sverige har företag som Assently och Scrive tagit in kapital, och förra året delade Vinnova ut 14 miljoner till en rad legal tech-satsningar.

Parallellt med detta har vi sett en rad uppköp och sammanslagningar. Som exempel kan nämnas att Imanage köpt RAVN, Internetbrands Avvo, Lexisnexis Ravel och Onetrust Dataguidance.

4. Mer teknik på Juristutbildningarna

Lärosäten i USA, och på sina håll även i Europa, har tagit fram program och kurser med inslag av teknik, entreprenörsskap och projektledning i syfte att göra studenterna bättre rustade för en förändrad yrkesroll. Köpenhamns universitet har inrättat en legal techhub, och vid Lunds universitet arrangerades nyligen ett program med föreläsare från näringslivet för teknikintresserade jurister.

5. Designtänk för ökad användarvänlighet

Legal design går ut på att förbättra juridikens gränssnitt, att sätta mottagaren i centrum och tillämpa principer hämtade från formgivning för att göra informationen mer intuitiv. Det finns numera konsulter på området, och advokatbyråer med heltidsanställda designers. I september går den tredje upplagan av Legal Design Summit av stapeln i Helsingfors.

6. Tvistlösningar utanför domstol

Företag som Ebay och Amazon har länge använt tekniska lösningar för att hantera dispyter, och i år inrättade Facebook en egen ”domstol” som ska pröva ärenden om regelbrott på plattformen. Numera finns också externa alternativ, som svenska Swiftcourt – som idag används av bl a Blocket.

Fredrik Svärd är IT-jurist, grundare av Legaltech.se och tidigare chefredaktör för Dagens Juridik samt generalsekreterare för Forum för dataskydd.

JusNytt

Halvor Manshaus

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

Integrerte sosiale moduler kan innebære felles behandlingsansvar

EU-domstolen avsa 29. juli 2019 prejudisiell uttalelse i saken mellom Fashion ID mot Verbraucherzentrale NRW (sak C-40/17). Saken omhandlet overføring av brukerdata til Facebook, og har betydning for integrerte moduler på nettsider som overfører brukerdata til andre aktører. Den underliggende saken verserer mellom disse partene for Oberlandesgericht Düsseldorf, som hadde forespurt EU-domstolens uttalelse.

Det er nødvendig først å forklare den type overføring av brukerdata som EU-domstolen diskuterer i denne saken. Facebook er kjent for sine integrerte *like*-knapper, som brukerne aktiverer ved å klikke på knappen. Dette har vært en viktig og velkjent funksjon hos Facebook som sosialt medium. Ved å klikke på denne knappen, markerer man ikke bare at man har lest eller gjort seg kjent med et tidligere postet innlegg, aktivering av knappen har også andre virkninger. Opprinnelig sørget algoritmer hos Facebook for at brukeren ble lagt til på en publisert liste over alle som hadde klikket på *like*, og forfatteren av innlegget ville få en melding om hvem som har «liket» innlegget. I tråd med at Facebook vokste seg større og utviklet seg til en viktig markedskanal, ble funksjonaliteten til like-knappen utvidet.

I dag er det ikke bare mulig å trykke på like-knappen på Facebooks egne nettsider, kommersielle aktører kan integrere knappen på sine egne nettsider. Brukeren på den eksterne siden kan nå klikke på Facebooks integrerte like-knapp, og derved opprette en personlig forbindelse til den eksterne aktøren. Facebook vil deretter sørge for at innhold fra denne aktøren presenteres på brukerens Facebook side. Virkningen har altså mye til felles med å skrive seg opp på en tradisjonell liste hvor man aksepterer å motta markedsføring. I tillegg vil Facebook også vise brukerens registrerte venner på Facebook at brukeren har «liket» den eksterne aktøren. Brukerens navn vil også kunne dukke opp i markedsføring på Facebook eller hos den eksterne aktøren som har integrert slik funksjonalitet. Da vil det typisk stå «**Peder Ås**, **Marte Kirkerud** and **Hans Tastad** like **NY Times**». Disse har da klikket «like» på nettsiden til NY Times, på en reklame hos Facebook eller på en annonse plassert på en nettside med integrert like-knapp.

Det er altså verdt å merke seg forskjellen mellom å klikke på like-knappen under innlegget fra en som brukeren er venn med på Facebook, og det å like en ekstern nettside eller annonse. Det første innebærer at du viser interesse for et innlegg, og at dette er synlig for andre. Det siste innebærer at algoritmer som styrer annonsering nå vil presentere innhold og annonser fra denne aktøren for brukeren. I tillegg vil brukerens navn presenteres for hennes venner på Facebook som ser annonser fra samme aktør, slik at brukeren nå benyttes i selve annonseringen. Som vi skal se i denne saken, er det ikke alltid engang nødvendig at brukeren klikker på knappen. Bare ved at knappen og den bakenforliggende programmodulen peker til Facebook, vil dette kunne være nok til at data overføres fra brukeren til Facebook.

Det er slik funksjonalitet som gjør at en bruker kan gå på en nettbutikk og se på et produkt, og senere motta markedsføring for dette produktet i andre sammenhenger. En periode etterpå vil brukeren kunne oppleve at bilde eller informasjon om akkurat dette produktet dukker opp på andre nettsider og nettapplikasjoner som Facebook, Instagram eller lignende. Informasjon om produktannonsen kobles opp mot brukerens identitet, og fremvises senere i håp om at tidligere interesse utløser kjøpsvilje. Systemet har en åpenbar svakhet der man har sett på et produkt uten at det foreligger noen kjøpsvilje, eller der man faktisk kjøper produktet i nettbutikken. I begge tilfeller gir det liten mening å motta markedsføring på dette produktet senere. Adferdsforskning og stadig nye algoritmer forbedrer imidlertid treffsikkerheten på denne typen markedsføring.

Nå tilbake til avgjørelsen i sak C-40/17. Fashion ID er en nettbutikk som selger klær. På nettsiden var det integrert en like-knapp fra Facebook. Slik integrering innebærer at like-knappen som vises ikke ligger lagret og presenteres fra Fashion ID, men at en underliggende modul kommunise-

rer med Facebooks egen server. Denne modulen kan i prinsippet være en enkel lenke som er integrert i nettbutikken, og som henter innhold fra Facebook. Det opprettes således en forbindelse mellom brukeren og Facebook i det samme han får fremvist nettsiden til nettbutikken. Dette er en vanlig måte å integrere innhold på. Eksempelvis vil mange ha sett videosnutter fra Youtube integrert i andre nettsider. Selve filmen ligger lagret og vises fra Youtube, men integreres hos siden som fremviser innholdet. Tilsvarende for eksterne reklamer og annonser på for eksempel en nettavis, som ofte hentes inn fra andre aktører og fremvises for brukeren som en del av nettavisen. Slike nettsider er altså modulbasert, og av andre praktiske grunner er dette blitt en vanlig måte å bygge opp nettsider på.

Fremvisning av nettsider innebærer i seg selv en utfordring, ved at den ene brukerens nettleser vil kunne skille seg fra nettleseren til en annen bruker. En stasjonær pc og en mobiltelefon vil ha ulike nettlesere, underliggende maskinvare og oppløsning på skjermen. Nettstedet må derfor hente inn informasjon om brukerens datamaskin, slik at bilder, filmer og annet innhold på nettsiden vises i riktig format, korrekt kvalitet/filstørrelse osv. Denne informasjonen vil også de eksterne innholdsleverandørene ha behov for, slik at de også laster opp riktig innhold til fremvisning av nettsiden.

Slik var det også med Fashion ID. I det brukeren gikk inn på nettsiden, ble hennes ip-adresse og spesifikasjoner for nettleser og maskinvare på vanlig måte sendt til Fashion IDs server. Tilsvarende informasjon ble også sendt til Facebook, som leverte likeknappen på nettsiden. Dette er som sagt nødvendig for å tilpasset fremvisning av nettsiden til brukerens nettleser. Det er verdt å merke seg at denne informasjonen altså blir sendt uten at brukeren har trykket på selve likeknappen som er integrert fra Facebook. Overføring av data til Facebook skjer bare ved at brukeren går inn på nettsiden. Det må understrekes at dette er helt vanlig praksis for å presentere nettsider med innhold som leveres fra tredjeparter.

Verbraucherzentrale NRW, som er en tysk forbrukerorganisasjon, gikk til rettslige skritt for å stanse den aktuelle overføringen av brukerinformasjon til Facebook med en forføyning. Det ble særlig vist til at brukerdata ble overført til Facebooks virksomhet i Irland i forbindelse med at like-knappen skulle vises på nettsiden til Fashion ID, og at dette skjedde uten at brukeren ble orientert. I den tyske underinstansen fikk Verbraucherzentrale NRW medhold. Fashion ID anket avgjørelsen videre til Oberlandesgericht Düsseldorf, og Facebook Irland trådte inn som partshjelper.

Henvendelsen til EU-domstolen gjaldt konkret spørsmål knyttet til overføring av brukeropplysninger opp mot personverndirektivet (95/46), samt spørsmål om informasjonskrav og andre tilstøtende problemstillinger. Når det gjaldt spørsmålet om overføring av brukeropplysninger, var det sentralt å avklare om Fashion ID ved sin passive rolle likevel måtte anses som behandlingsansvarlig etter artikkel 2 d i direktivet (definisjon av behandlingsansvarlig).

De fleste vil ha fått med seg at vår nye lov om behandling av personopplysninger trådte i kraft 20. juli 2018. Denne nye loven gjennomfører EUs personvernforordning (GDPR) i Norge og gjør personvernforordningen til norsk lov. EU-direktiv 95/46 (personverndirektivet) og personopplysningsloven fra 2000 er opphevet. Bakgrunnen for at EU-domstolen i denne saken anvender direktivet og ikke den nye forordningen ligger i sakens faktum, som ligger forut for den nye forordningen. Det er altså det gamle direktivet som anvendes i denne saken, ref. avsnitt 3 i avgjørelsen fra EU-domstolen.

Direktivets artikkel 2 d har blitt tolket vidt av EU-domstolen i tidligere saker, og angir definisjonen for hvem som anses å være behandlingsansvarlig:

> *«…den fysiske eller juridiske person, offentlige myndighet, byrå eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal benyttes; når formålet med og hjelpemidlene ved behandlingen er fastlagt ved nasjonale lover og forskrifter eller på fellesskapsplan, kan den behandlingsansvarlige, eller de særlige kriterier for utpeking av vedkommende, fastsettes i nasjonal lovgivning eller i fellesskapsretten…»*

EU-domstolen peker først på den vide ordlyden i direktivets definisjon, og viser deretter i avsnitt 66 til at den vide definisjonen av begrepet behandlingsansvarlig i ordlyd og domstolens egen praksis er nødvendig for å oppnå formålet om et effektivt og fullstendig vern av den berørte. Selv om en slik vid forståelse innebærer at flere vil stå ansvarlige som behandlere av personopplysninger, påpeker domstolen i avsnitt 70 at et slikt felles ansvar ikke nødvendigvis innebærer at de ulike aktørene har samme grad av ansvar for de ulike deler av behandlingen. De enkelte behandlingsansvarlige kan være ansvarlige for behandling av personopplysninger på forskjellige nivåer og i ulikt omfang. I dette ligger at den enkeltes ansvarsomfang må vurderes konkret og *«under hensyntagen til samtlige relevante omstændigheder i sagen.»*

Domstolen anvender deretter denne vide definisjonen av behandlingsansvarlig, og viser i avsnitt 75 til at nettbutikken Fashion ID:

> *«…ved at integrere 'synes godt om'-knappen fra Facebook på sit websted synes at have givet Facebook Ireland mulighed for at indhente personoplysninger vedrørende webstedets besøgende, idet denne mulighed opstår fra det tidspunkt, hvor den pågældende konsulterer webstedet, og dette finder sted uanset om disse besøgende er medlemmer af det sociale netværk Facebook, om de har klikket på 'synes godt om'-knappen fra Facebook, eller om de har kendskab til, at en sådan operation finder sted.»*

Spørsmålet fra den henvisende domstolen var om dette likevel kunne innebære ansvar, all den stund Fashion ID ikke hadde noen reell kontroll med den etterfølgende behandlingen av brukeropplysningene (avsnitt 42 og 64). Her trekker domstolen på nyansering av ansvarsforholdene som er omtalt ovenfor. Selv om både Fashion ID og Facebook kan anses å være behandlingsansvarlig, er det ikke gitt at dette ansvaret skal fordeles likt. I stedet er det naturlig å se hvem som utøver reell kontroll med opplysningene på de ulike stadier av overføring og behandling. Direktivets artikkel 2 b definerer hva som utgjør behandling av personopplysninger, og gir flere eksempler på flere ulike handlinger som er relevante, herunder innsamling, registrering, systematisering, oppbevaring, overføring, osv. I avsnitt 76 påpeker domstolen at Fashion ID i denne sakens kontekst foretar innsamling og overføring av personopplysninger, men trekker en grense mot den etterfølgende behandling:

> *«Med hensyn til nævnte oplysninger forekommer det derimod umiddelbart udelukket, at Fashion ID fastlægger, til hvilke formål og med hvilke hjælpemidler der efterfølgende foretages behandlingsoperationer vedrørende personoplysninger af Facebook Ireland efter deres transmission til dette selskab, hvorfor Fashion ID ikke kan anses for at være den registeransvarlige for disse operationer som omhandlet i nævnte direktivs artikel 2, litra d).»*

Når det gjelder innsamling og overføring av opplysninger, mener domstolen at Fashion ID ved å integrere den sosiale modulen fra Facebook har avgjørende innflytelse på innsamling og overføring av informasjonen. Domstolen viser i avsnitt 78 til at uten modulen fra Facebook ville det ikke skje noen innsamling eller overføring. Tanken er at Fashion ID har kontroll over hva slags innhold som ligger på nettbutikken, og at modulen er blitt bevisst integrert. Da har det ikke avgjørende betydning at Fashion ID ikke har noen styring med selve innsamlingen og oversending til Facebook. Slik jeg leser avgjørelsen vil dette kunne stille seg annerledes der man i god tro integrerer en modul som inneholder tilsvarende funksjonalitet for innsamling og overføring av personopplysninger, og dette er ukjent for den ansvarlige bak nettsiden. Det vil da neppe være tilstrekkelig at man ikke kjenner til den tekniske funksjonalitet knyttet til passiv overføring av data. Domstolens uttalelser peker i retning av en strengere aktsomhetsnorm enn dette.

Konklusjonen ble altså at Fashion ID er å anse som felles behandlingsansvarlig etter direktivets 2 d for innsamling og overføring av informasjon, men at dette ansvaret avgrenses opp mot den videre behandling av personopplysningene som gjøres hos Facebook. Det forelå flere spørsmål til prejudisiell vurdering, og den tyske domstolen hadde også tatt opp spørsmålet om informasjonsplikt og innhenting av samtykke. EU-domstolens drøftelse på dette punkt er illustrerende for hvordan det differensieres mellom det felles behandlingsansvar og det ansvar som pålegges den enkelte behandlingsansvarlige på de ulike trinn av prosessen. EU-domstolen konkluderer i avsnittene 102 og 103 med at informasjon og tilhørende samtykke fra brukeren må innhentes i forbindelse med innsamling og overføring av data. Ettersom det er besøket til nettbutikken som utløser innsamlingen og overføringen til Facebook, er det naturlig at det er nettbutikken som har ansvaret for denne delen av prosessen:

> *«Hvad angår det i artikel 2, litra h), og artikel 7, litra a), i direktiv 95/46 omhandlede samtykke fremstår det således, at dette skal være afgivet inden indsamlingen og videregivelsen ved transmission af den registreredes personoplysninger. På denne baggrund påhviler det webstedoperatøren og ikke udbyderen af det sociale modul at indhente dette samtykke, for så vidt som det er den omstændighed, at en besøgende konsulterer dette websted, der udløser behandlingen af personoplysninger.»*

Denne avgjørelsen følger opp EU-domstolens konklusjon i Wirtschaftsakademie-saken (C-210/16), som også omhandlet behandling av data i fellesskap med Facebook. I den saken ble det også konkludert med et felles behandlingsansvar. Resultatet i begge disse sakene er i tråd med behovet for å kunne informere brukeren om datainnsamlingen og innhente samtykke i henhold til direktivet og GDPR. Ved at informasjonen behandles av flere aktører, er det viktig at den enkeltes aktør tillegges et ansvar i tråd med den rolle og funksjon som utøves. Samtidig er det nok mange aktører som ikke har tenkt gjennom problematikken knyttet til informasjon og samtykke ved bruk av sosiale moduler, eller andre moduler som bruker nettkapsler (cookies), analyseverktøy og lignende som samler inn informasjon fra brukeren. En effekt av disse avgjørelsene vil nok være at det blir flere informasjonsbokser brukeren skal lese gjennom når hun besøker en nettside, og man må klikke på samtykke-knapper før man går videre. Det er nærliggende å tro at brukerne i løpet av kort tid vil bli så vant til slike bokser, at man bare klikker på «jeg samtykker» uten å lese teksten noe nærmere. Konsekvensen av slik samtykkeapati kan dermed bli at brukerne ender opp med å godta langt mer omfattende betingelser enn de ellers ville ha gjort.

En enklere modell ville være at førstegangs bruk av en nettleser utløste informasjon om at nettleseren utvekslet en del grunnleggende informasjon med nettsider brukeren besøker, og forklarte nøyaktig hva som ville bli utlevert. Dette kunne være en minstenorm for funksjonalitet av det store flertallet av nettsidene. Så kunne man sett for seg at mer omfattende datainnsamling krevde slike informasjonsbokser og samtykkeavgivelser som nå kreves av EU-regelverket. Det ville kunne føre til at brukerne satte seg mer inn i hva de faktisk samtykker til, enn det dagens ordning legger opp til.


Wiersholm

Rune Opdahl og Fredrik Wiker

Ett år med GDPR i Norge – hva har (ikke) skjedd?

Det har nå gått ett år siden den nye personopplysningsloven og personvernforordningen (GDPR) trådte i kraft i Norge. I tiden før ikrafttredelsen var det svært stort fokus på etterlevelse blant norske virksomheter, og vårt inntrykk er at dette har fortsatt.

Til tross for dette har større reaksjoner fra Datatilsynet latt vente på seg. Departementet har heller ikke vært aktive med å utarbeide nye forskrifter. I denne korte artikkelen skal vi se nærmere på hva som har skjedd i løpet av det siste året, og hva som ikke har skjedd.

Stor økning i antall saker hos Datatilsynet

Datatilsynet forvalter personvernregelverket og har myndighet til å foreta granskninger og utstede overtredelsesgebyr dersom brudd identifiseres.

Det har vært en stor økning i antall saker for, og henvendelser til, Datatilsynet. I 2018 hadde tilsynet 2654 saker mot 1807 saker i 2017. Meldinger om brudd på personopplysningssikkerheten har økt fra 349 i 2017 til hele 1276 i 2018.

Overtredelsesgebyrer knyttet til sikkerhet – en trend?

En økning i antall overtredelsesgebyrer har imidlertid latt vente på seg. Grunnen er trolig vesentlig økt arbeidspress hos Datatilsynet.

Datatilsynet har ilagt et rekordstort gebyr på 1,6 millioner kroner til Bergen kommune. Dessuten har tilsynet varsel om gebyr på 2 millioner kroner til Oslo kommune. Begge sakene dreide seg om brudd på personopplysningssikkerheten, hvilket også det britiske datatilsynet sitt varsel om rekordgebyr til British Airways på nesten 2 milliarder kroner gjorde. Dette kan være utslag av at sikkerhet er et særlig fokusområde, men skyldes nok vel så mye at Datatilsynet blir kjent med sikkerhetsbrudd gjennom meldinger eller medieoppmerksomhet og av den grunn har hatt en særlig oppfordring til å agere.

Det er grunn til å anta at det vil komme vesentlig flere overtredelsesgebyrer fremover. Datatilsynet har allerede varslet en tøffere linje med flere målrettede kontroller i vente.

Fokus på veiledning

Datatilsynet har lansert flere nye veiledere og rapporter i løpet av det siste året. Blant annet har tilsynet utarbeidet en liste over hvilke aktiviteter som etter GDPR art. 35 i alle tilfeller vil kreve at det gjennomføres en særskilt konsekvensutredning (DPIA). Listen baserer seg på EDPB (European Data Protection Board) sine retningslinjer og er dermed til en viss grad harmonisert med resten av Europa.

Bruk av målrettet reklame (adtech) er også behandlet i en nylig rapport fra Datatilsynet, som særlig ser på målrettede politiske budskap. I tillegg har Datatilsynet laget veiledere knyttet til kunstig intelligens, dataportabilitet, personvernprinsipper, innebygd personvern, atferdsnormer, databehandleravtaler, forholdet mellom behandlingsansvarlig og databehandler, behandlingsgrunnlag og informasjonskravet.

Fremdeles manglende regulering fra departementet

Personopplysningsloven åpner for at departementet kan treffe beslutninger eller utarbeide forskrifter relatert til behandlingen av særskilte personopplysninger. Imidlertid har personopplysningsforskriften foreløpig tilnærmet ingen materielle bestemmelser.

Dette innebærer at departementet, selv etter ett år med GDPR, enda ikke har funnet grunn til å regulere forhold som *behandling av særskilte personopplysninger for spesifikke forhold (§§ 7 og 8), bruk av entydige identifikasjonsmidler (§ 12), forhåndsdrøfting og forhåndsgodkjenning (§ 14), gjennomføring av delegerte rettsakter (§ 15), unntak fra informasjons- og innsynsretten og underretning om brudd på personopplysningssikkerheten (§ 16), plikt til å utpeke personvernombud (§ 19), dekning av Datatilsynets kontrollkostnader (§ 20) og bestemmelser om tvangsmulkt (§ 29).*

Trender fra øvrige land

Dersom vi kaster blikket utover til resten av Europa er det tydelig at de samme trendene vi kan spore i Norge også ser ut til å gjelde der. Det har vært en økning i avvikssaker, få store overtredelsesgebyrer og lite

regulering fra lovgivere i påvente av økt kunnskap om regelverket.

Nå som det første innkjøringsåret har passert blir det spennende å se hvordan Datatilsynet, departementet og sentrale tilsynsorganer i Europa fremover vil følge opp GDPR.

Rune Opdahl er partner og advokat i Advokatfirmaet Wiersholm, Oslo.

Fredrik Wiker er advokatfullmektig i Advokatfirmaet Wiersholm, Oslo.

Delphi

Rebecka Harding

Initial rättslig analys från EDPB och EDPS av Cloud Acts effekt på GDPR

Sammanfattning

Av EDPB och EDPS:s initiala rättsliga analys, som publicerades i juli 2019, framgår att de ser mycket begränsade möjligheter för en IT-tjänsteleverantör, i sin egenskap av personuppgiftsansvarig i EU i den specifika situationen, att följa en direktbegäran från amerikansk brottsbekämpande myndighet om utlämnande av personuppgifter enligt Cloud Act på ett sätt som är förenligt med GDPR.

Konflikt mellan Cloud Act och GDPR

European Data Protection Board (”EDPB”) och European Data Protection Supervisor (”EDPS”) har på EU-parlamentets begäran gjort en initial rättslig analys av vilka möjligheter leverantörer av allehanda typer av elektroniska kommunikations- och molntjänster (”IT-tjänsteleverantörer”), i egenskap av personuppgiftsansvariga i EU i den specifika situationen, har att följa en direktbegäran från amerikansk brottsbekämpande myndighet om utlämnande av personuppgifter under US Clarifying Lawful Overseas Use of Data Act (“Cloud Act”) dvs. inte en begäran som ställts till IT-tjänsteleverantörens kunder.

EDPB och EDPS har i sin analys utgått från att IT-tjänsteleverantörer är att anse som personuppgiftsansvariga när en amerikanska brottsbekämpande myndighet riktar en sådan direktbegäran till dem. EDPB och EDPS har i sin analys inte tagit hänsyn till artikel 28(3) i GDPR som reglerar hur ett personuppgiftsbiträde, vilket IT-tjänsteleverantörer ofta bedöms vara i relation till sina kunder, får behandla personuppgiftsansvariges personuppgifter för egna ändamål.

Cloud Act trädde ikraft i USA den 23 mars 2018 och gör det möjligt för amerikanska brottsbekämpande myndigheter att i vissa fall direkt begära att IT-tjänsteleverantörer, som står under amerikansk jurisdiktion, lämnar ut data som lagras utanför USA. För att kunna begära ut data från en IT-tjänsteleverantör måste den amerikanska brottsbekämpande myndigheten enligt Cloud Act vända sig till domstol med en begäran om att domstolen ska utfärda en ”warrant” om att viss data lagrad utanför USA ska överlämnas till den brottskämpande myndigheten. För att en domstol ska utfärda en warrant krävs enkelt förklarat att det måste föreligga sannolika skäl för att ett konkret brott har begåtts och att den begärda datan är relevant för och har koppling till brottet.

I analysen redogör EDPB och EDPS för sin bedömning av möjligheterna för IT-tjänsteleverantörer, i egenskap av personuppgiftsansvariga i EU, att överföra personuppgifter enligt Cloud Act utifrån det tvåstegstest som följer av GDPR och som måste tillämpas vid alla typer av överföringar av personuppgifter till tredje land (land utanför EU/EES), nämligen följande:

Steg 1: Behandlingen av personuppgifterna måste vara laglig enligt artikel 6 i GDPR.

Steg 2: Överföringen av personuppgifterna till tredje land måste vara förenlig med kapitel V (artikel 44–50) i GDPR.

I analysen kommer EDPB och EDPS fram till att en IT-tjänsteleverantörs överföring av personuppgifter med anledning av en direktbegäran enligt Cloud Act i dagsläget i princip enbart är tillåten vid exceptionella fall när behandlingen jämte överföringen av personuppgifterna är nödvändig för att skydda den registrerades vitala intressen i enlighet med artikel 6(1)(d) jämte artikel 49(1)(f) i GDPR. Som exempel anges att kidnappade barns personuppgifter lagligen kan behandlas respektive överföras i samband med utredning av brottet.

EDPB och EDPS resonerar i sin analys att om en warrant utfärdad av amerikansk domstol enligt Cloud Act hade erkänts och kunnat verkställas enligt artikel 48 i GDPR hade behandlingen av personuppgifterna med anledning av denna warrant kunnat grunda sig på artikel 6(1)(c) i GDPR (behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige). Artikel 48 i GDPR föreskriver att domstolsbeslut och myndighetsbeslut i tredje land enbart får erkännas och verkställas om de baseras på en internationell överenskommelse såsom det MLAT-avtal (mutual legal assistance treaty) EU och USA har ingått. Av MLAT-avtalet följer en särskild process som normalt ska tillämpas när brottsbekämpande myndigheter vill få data från ett annat land. På grund av Cloud Acts extraterritoriella effekter kringgås dock processen som följer av MLAT-avtalet mellan EU och USA varför en warrant inte uppfyller artikel 48 i GDPR.

Givet att Cloud Act gör det möjligt för en myndighet att vända sig direkt till ett företag/organisation med sin begäran om att få ut data kan varken Privacy Shield eller paraplyavtalet mellan EU och USA bli tillämpligt varför EDPB och EDPS inte tog hänsyn till dem i sin analys.

Övrigt

Avslutningsvis konstaterar EDPB och EDPS bland annat att Cloud Act kan även innebär andra utmaningar med såväl medlemsstaters nationella rätt som unionsrätt. Exempelvis har vissa medlemsstater lagstiftning som förhindrar tjänsteleverantörer inom EU från att lämna ut information till ett tredje land.

Vidare noterar EDPB och EDPS i sin analys att förhandlingar pågår mellan Europeiska Kommissionen och USA om ett nytt internationellt avtal för gränsöverskridande tillgång till elektroniska bevis. I analysen påpekas att ett ingående av ett internationellt avtal måste för att vara förenligt med EU:s primärlagstiftning under alla omständigheter föreskriva lämpliga skyddsåtgärder för överföringar, säkerställa att registrerades rättigheter är verkställbara och att effektiva rättsmedel för registrerade finns tillgängliga.

Avslutning

Vi tycker att det är bra att EDPB och EDPS sett över vilka möjligheter IT-tjänsteleverantörer har att följa en direktbegäran enligt Cloud Act med hänsyn till GDPRs regelverk.

Däremot hade vi gärna sett att EDPB och EDPS även hade tagit hänsyn till artikel 28(3) i GDPR i sin analys. Detta eftersom att IT-tjänsteleverantörer typiskt sett är att anse som personuppgiftsbiträden i relation till sina kunder varför artikel 28(3)s har central betydelse för frågan om deras möjligheter att lämna ut personuppgifter som kunder tillhandahållit dem med med anledning av en direktbegäran från amerikansk myndighet.

Rebecka Harding är senior associate och advokat i Advokatfirman Delphi, Stockholm.

Gorrissen Federspiel

Tue Goldschmieding

1. Det danske datatilsyn udtaler alvorlig kritik af vaskehal i forbindelse med behandling af indsigtsanmodning i tv-overvågningsoptagelser

Det danske datatilsyn ('Datatilsynet') behandlede i marts 2019 en klage over vaskehallen Wash World ApS. Klager havde i forbindelse med en tingsskadesag fremsat anmodning om indsigt i tv-overvågningsoptagelser af sig selv, sin søn og bil i Wash World ApS.

Indledningsvist afviste selskabet klagers anmodning om indsigt med den begrundelse, at det ville stride imod virksomhedens politik for udlevering til private, idet der i optagelserne indgik andre personer. Wash World ApS imødekom dog efterfølgende anmodningen, men først efter gentagne forespørgsler fra klager og mere end tre måneder efter klagers anmodning.

Datatilsynet udtalte, at såfremt der i tv-overvågningsoptagelser indgår andre personer end den registrerede, skal den dataansvarlige sløre eller på anden måde fjerne dem f. eks. ved billedbeskæring. På den baggrund fandt Datatilsynet grundlag for at udtale alvorlig kritik af, at Wash World ApS indledningsvist havde afvist klagers anmodning om indsigt og herefter først imødekommet klagers anmodning om indsigt efter tre måneder.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/mar/klage-over-wash-world-aps-haandtering-af-den-registreredes-anmodning-om-indsigt-i-tv-overvaagningsoptagelser/

2. Det danske datatilsyn forbyder TDC at optage telefonsamtaler uden samtykke og udtaler alvorlig kritik af TDC's manglende sletning af personoplysninger

Det danske datatilsyn ('Datatilsynet') traf den 28. marts 2019 afgørelse i en sag om sletning af personoplysninger. Teleselskabet TDC A/S havde ud fra en midlertidig database sendt markedsføringsmateriale ud til en række personer, der på et tidspunkt havde givet samtykke til at modtage markedsføringsmateriale over e-mail.

Datatilsynet udtalte alvorlig kritik af, at TDC A/S ikke løbende havde foretaget sletning af personoplysninger i den midlertidige database efter gennemførelsen af en specifik markedsføringskampagne. Det var ifølge Datatilsynet problematisk i henhold til Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 5, stk. 1, litra e, og artikel 6, stk. 1, litra a. Datatilsynet fandt desuden, at TDC A/S havde opbevaret personoplysninger i et længere tidsrum end det, der var nødvendigt for at foretage databehandlingen, og at TDC A/S ikke kunne påvise, at behandling af de pågældende personoplysninger var sket på baggrund af de registreredes samtykke.

Datatilsynet traf den 8. april 2019 afgørelse i en anden sag vedrørende TDC A/S. Selskabet havde optaget klagers telefonsamtale med en af TDC A/S' kundekonsulenter, uden at klager havde givet samtykket til optagelsen.

Datatilsynet udtalte alvorlig kritik og lagde i den forbindelse vægt på, at der ikke i sagen forelå omstændigheder, som kunne begrunde en fravigelse af tilsynets praksis om, at optagelse og lagring af telefonsamtaler til uddannelsesmæssige formål som udgangspunkt ikke kan ske uden samtykke fra den registrerede. Da TDC A/S havde meddelt, at det ikke var teknisk muligt at indhente samtykke, fandt Datatilsynet endvidere grundlag for at meddele TDC A/S et midlertidigt forbud imod at optage telefonsamtaler til internt uddannelsesmæssigt formål, indtil en teknisk løsning var tilvejebragt.

Læs afgørelserne her:
https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/apr/ny-afgoerelse-forbud-til-tdc-om-optagelse-af-telefonsamtaler-uden-samtykke/
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/mar/yousee-as-tdc-as-behandling-af-personoplysninger/

3. Det danske datatilsyn meddeler DK Hostmaster påbud om at offentliggøre personoplysninger om fuldmægtige for domænenavnsregistranter

Den 10. juli 2018 klagede en registreret ('klager') til det danske datatilsyn ('Datatilsynet') over, at DK Hostmaster A/S offentliggjorde personoplysninger om ham i

WHOIS-databasen i forbindelse med hans funktion som fuldmægtig for en række domænenavnsregistranter.

DK Hostmaster A/S argumenterede for, at personoplysningerne kunne offentliggøres med hjemmel i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 6, stk. 1, litra e. DK Hostmaster A/S anførte, at offentliggørelsen var nødvendig for at skabe åbenhed om, hvem der stod bag indholdet på et domænenavn, og at dette af kriminalpræventive hensyn var en opgave, der udførtes i samfundets interesse og af så væsentlig karakter, at hensynet til enkeltpersoners interesse i ikke at få vist deres kontaktoplysninger offentligt burde vige herfor.

Datatilsynet traf den 28. marts 2019 afgørelse i sagen og meddelte DK Hostmaster A/S påbud om at ophøre med at offentliggøre personoplysninger om klager som fuldmægtig for domænenavnsregistranter samt personoplysninger om andre fuldmægtige for domænenavnsregistranter i øvrigt.

Datatilsynet fandt, at offentliggørelsen af personoplysningerne ikke var nødvendig af hensyn til udførelse af en opgave i samfundets interesse i henhold til databeskyttelsesforordningens artikel 6, stk. 1, litra e.

Datatilsynet henviste i den forbindelse til, at et eventuelt ansvar for indhold på et domænenavn som udgangspunkt vil skulle gøres gældende over for registranten af hjemmesiden og ikke dennes fuldmægtige. Ifølge Datatilsynet var DK Hostmaster A/S' behandling af personoplysninger om klager desuden ikke begrænset til, hvad der var nødvendigt i forhold til de formål, hvortil oplysningerne skulle behandles, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra c.

Læs hele afgørelsen her:

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/mar/offentliggoerelse-af-personoplysninger-om-fuldmaegtige-for-domaeneregistranter/

4. Det danske datatilsyn vurderer, at personoplysninger noteret på papir med henblik på elektronisk registrering allerede fra indsamlingsfasen er omfattet af databeskyttelsesreglerne

Det danske datatilsyn ('Datatilsynet') behandlede i april 2019 en klage over en kommunal sagsbehandler, som ifølge klager havde behandlet personoplysninger på fysisk papir på en sådan måde, at udefrakommende kunne tilgå oplysningerne, og at de fysiske papirer med personoplysninger blev smidt ud i en almindelig skraldespand.

Datatilsynet fastlog, at oplysninger der indsamles med henblik på umiddelbart bagefter at blive elektronisk registreret i et journalsystem, er omfattet af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') allerede i indsamlingsfasen.

Datatilsynet fandt ikke, at der var grundlag for at udtale kritik af kommunen, hvor sagsbehandleren var ansat. Datatilsynet lagde vægt på, at noterne med personoplysninger blev opbevaret utilgængeligt for uvedkommende, og at noterne efter indskrivning i sagssystemet blev lagt i en aflåst papircontainer med henblik på destruktion.

Datatilsynet noterede endvidere, at kommunen havde oplyst, at klagen havde givet anledning til en række generelle overvejelser om, hvorledes kommunen kunne sikre en tillidsbaseret atmosfære, herunder at gøre bortskaffelsen af notater mere synlig for den enkelte borger og imødekomme en eventuel tilkendegivelse fra en borger om, at denne ikke ønsker notater på papir ved blot at indskrive oplysningerne i sagssystemet undervejs.

Læs hele afgørelsen her:

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/apr/klage-over-manglende-behandlingssikkerhed/

5. Det danske datatilsyn indstiller taxaselskab til bøde på 1,2 mio. kr.

Den 18. marts 2019 blev det danske taxaselskab Taxa 4x35 politianmeldt af det danske datatilsyn ('Datatilsynet') for brud på Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen').

Datatilsynet havde efter et tilsynsbesøg hos Taxa 4x35 bemærket, at kundernes telefonnumre først blev slettet efter fem år. Det var derfor muligt at henføre oplysninger om næsten ni millioner taxature med blandt andet dato, tidspunkt og afhentnings- og afleveringssted til bestemte fysiske personer, selvom kundernes navne var blevet anonymiseret efter allerede to år.

Datatilsynet indstillede taxaselskabet til en bøde på 1,2 mio. kr. Det er dermed den første danske sag, hvor Datatilsynet har indstillet en bøde for brud på databeskyttelsesforordningen. Datatilsynet lagde vægt på, at der var tale om store mængder personoplysninger, som var blevet gemt uden et sagligt formål.

Derudover fastslog Datatilsynet, at taxaselskabet ikke havde levet op til databeskyttelsesforordningens krav om ansvarlighed. Taxaselskabet havde ikke skabt klarhed over, efter hvilket grundlag oplysningerne var blevet behandlet. Taxaselskabet havde heller ikke dokumenteret tilstrækkelige procedurer for logning af allerede foretagne sletninger. Disse to forhold gav Datatilsynet anledning til at rette alvorlig kritik af taxaselskabet ud over den indstillede bøde.

Da det efter det danske retssystem ikke er muligt for Datatilsynet at pålægge administrative bøder, skal den endelige bødestraf afgøres ved de danske domstole, jf. databe-

skyttelsesforordningens artikel 83, stk. 9.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/mar/datatilsynet-indstiller-taxaselskab-til-boede-paa-1-2-mio-kr/

6. Det danske datatilsyn udtaler alvorlig kritik og meddeler påbud til Rejsekort A/S

Det danske datatilsyn ('Datatilsynet') udtalte den 16. april 2019 på baggrund af en klage fra en registreret alvorlig kritik af Rejsekort A/S' it-systemer. Klagesagen omhandlede en rejsendes klage over Rejsekort A/S' manglende berigtigelse af lokalitetsdata ved busrejser.

Den manglende berigtigelse skyldtes den måde, hvorpå Rejsekort A/S som dataansvarlig havde indrettet deres it-system. It-systemet fejlregistrerede de rejsendes lokalitetsoplysninger og var indrettet på en sådan måde, at disse ikke kunne berigtiges, men at der alene kunne tilføjes supplerende erklæringer med korrekte oplysninger.

Da lokalitetsoplysningerne omhandlede faktuelle oplysninger, havde den registrerede rejsende efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 16, ret til at få berigtiget oplysninger om sig selv hos den dataansvarlige uden unødig forsinkelse. Hertil bemærkede Datatilsynet, at databeskyttelsesforordningens artikel 16, 2. pkt., ikke indebar en ret for Rejsekort A/S som dataansvarlig til at foretage berigtigelsen ved at tilføje supplerende oplysninger uden at ændre de oprindelige oplysninger.

Datatilsynets udtalte derfor alvorlig kritik af Rejsekort A/S både angående den konkrete klagesag og de generelle forhold angående indsamlingen, hvortil den berettigede ikke fik oplysningerne om behandlingen på en letforståelig og lettilgængelig måde som påkrævet, jf. databeskyttelsesforordningens artikel 12.

Som følge heraf meddelte Datatilsynet i medfør af databeskyttelsesforordningens artikel 58, stk. 2, litra c og d, påbud om, at Rejsekort A/S i overensstemmelse med databeskyttelsesforordningens artikel 16, 1. pkt., berigtiger klagerens lokalitetsdata og ligeledes udfærdiger en plan for, hvorledes it-systemet bliver bragt i overensstemmelse med databeskyttelsesreglerne.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/maj/ny-afgoerelse-alvorlig-kritik-og-paabud-til-rejsekort-as/

7. Det danske datatilsyn udtaler alvorlig kritik af Fredericia Gymnasiums behandling af personoplysninger

Den 16. maj 2019 traf det danske datatilsyn ('Datatilsynet') afgørelse i en sag mod Fredericia Gymnasium og deres brug af programmet "Examcookie". Examcookie er et program, der installeres på elevers computere, således at undervisningsinstitutioner kan monitorere elevernes computeraktivitet under en eksamen for at opdage og forhindre eksamenssnyd.

Datatilsynet fandt, at Fredericia Gymnasium ikke havde haft et overblik over den samlede mængde af indsamlet data, og dermed ikke kunne redegøre for, at de indsamlede personoplysninger var nødvendige for at opfylde formålet.

Derudover fandt Datatilsynet, at Fredericia Gymnasium ikke havde iagttaget deres oplysningspligt, idet eleverne alene havde fået en generel introduktion til programmet ved et fællesmøde og i øvrigt alene var blevet henvist til yderligere oplysninger, der følger af Examcookies' egen hjemmeside.

Dette medførte, at Datatilsynet udtalte alvorlig kritik af Fredericia Gymnasium, da behandlingen af personoplysningerne ikke var sket i overensstemmelse med artikel 5, stk. 1, litra c, og artikel 13 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen').

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/maj/fredericia-gymnasiums-behandling-af-personoplysninger-ved-brug-af-programmet-examcookie/

8. Det danske datatilsyn offentliggør spørgeskemaer og eksempler på spørgsmål som stilles på tilsyn

Det danske datatilsyn ('Datatilsynet') offentliggjorde i april 2019 en række eksempler på spørgeskemaer, som Datatilsynet benytter i forbindelse med deres tilsyn. De offentliggjorte spørgeskemaer er de skemaer, som Datatilsynet har benyttet på tilsyn foretaget i det første halvår af 2019.

Spørgeskemaerne blev offentliggjort på baggrund af stor interesse for de spørgsmål, som Datatilsynet stiller på tilsyn. Datatilsynet understregede imidlertid, at eksemplerne på spørgeskemaer ikke kan benyttes som tjeklister, da spørgsmålene variererer fra tilsyn til tilsyn og i øvrigt revideres løbende.

Datatilsynet har offentliggjort eksempler på spørgeskemaer vedrørende henholdsvis autorisation af medarbejdere, brud på persondatasikkerheden hos offentlige myndigheder og private virksomheder samt kryptering.

Se spørgsmålene her:
https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/apr/se-hvad-datatilsynet-spoerger-om-paa-tilsyn/

9. De nordiske datatilsyn forsætter tæt samarbejde og vedtager ny erklæring om styrket nordisk samarbejde

Den 6.-7. maj 2019 afholdtes det årlige nordiske møde om databeskyttelse, hvor de nordiske databeskyttelsesmyndigheder fra Dan-

mark, Færøerne, Finland, Island, Norge, Sverige og Åland deltog. Mødets fokus var navnlig fælles strategier for overholdelse af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'), samarbejdet med EU og udveksling af information.

På mødet vedtog myndighederne en række trin for det videre samarbejde, der blandt andet omfattede bidrag til Det Europæiske Databeskyttelsesråd ('EDPB'), revision af databeskyttelsesrådgivere og sikring af overholdelse af reglerne i databeskyttelsesforordningen ved støtte af databeskyttelsesrådgivere.

Læs hele erklæringen her: https://www.datatilsynet.dk/media/6973/stockholm-declaration-2019.pdf

10. Efterspurgt dansk vejledning om cyber- og informationssikkerhedsstrategi for sundhedssektoren udgives på engelsk

En engelsk version af det danske sundheds- og ældreministerie, Danske Regioner og Kommunernes Landsforenings strategi for cyber- og informationssikkerhed på sundhedsområdet blev udgivet i maj 2019.

I 2018 blev det i Danmark fastslået, at sundhedssektoren var én ud af seks sektorer, hvor truslen fra cyberspionage og cyberkriminalitet blev vurderet til at være meget høj, hvorfor der blev udarbejdet en samlet strategi på området. Efter offentliggørelsen var der fra blandt andet World Economic Forum stor interesse i en engelsk oversættelse af strategien, som nu er udgivet.

Strategien indeholder 17 initiativer, der skal implementeres på tværs af sundhedssektoren og sætter fokus på nødvendigheden af et styrket system for at forudse, forebygge, opdage og håndtere cyber- og informationssikkerhedshændelser. Der lægges især vægt på sundhedssektorens seks sårbarheder, heraf en stor medarbejderkreds der håndterer følsomme personoplysninger, et komplekst it-landskab, afhængighed af fælles digital infrastruktur, legacy-systemer og Internet of Things-enheder, store datasamlinger og en uensartet sektor.

Læs hele vejledningen her: https://sundhedsdatastyrelsen.dk/da/nyheder/2019/cyberstrategi_engelsk_03052019

11. Det danske folketing vedtager lovforslag om ændring af reglerne vedrørende helbredsoplysninger og andre fortrolige oplysninger

Den 14. marts 2019 vedtog det danske folketing ('Folketinget') lov nr. 273 af 26. marts 2019 om bedre digitalt samarbejde i sundhedsvæsenet mv. Formålet med den vedtagne lov er, at det skal blive lettere at dele relevante oplysninger om patienters forløb mellem de sundhedspersoner, der behandler patienten. Loven trådte i kraft den 1. juli 2019.

Loven etablerer en ny fælles digital infrastruktur, der samler udvalgte oplysninger om patienten med henblik på at skabe en oversigt for patientens behandlingsforløb. Det vil fremover være lettere for borgerne at få indsigt i, hvem der har adgang til sundhedsoplysningerne. Formålet er endvidere at sikre, at alle sundhedspersoner har mulighed for at få adgang til patientjournaler, såfremt det er nødvendigt i forbindelse med behandlingen.

Det fremhæves i lovforslaget, at reglerne suppleres af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'), herunder især reglerne om behandlingssikkerhed.

Se lovændringen her: https://www.retsinformation.dk/Forms/R0710.aspx?id=208120

12. EDPS udgiver udtalelse om det andet tillæg til Budapestkonvention om cyberkriminalitet

Den Europæiske Tilsynsførende for Databeskyttelse ('EDPS') udgav den 2. april 2019 en udtalelse vedrørende det andet tillæg til Budapestkonventionen samt EU-Kommissionens deltagelse i forhandlingerne.

EU-Kommissionen forelagde en anbefaling for Rådet for Den Europæiske Union ('Rådet') til en rådsafgørelse, som skulle bemyndige EU-Kommissionen til at indgå i forhandlingerne på vegne af Den Europæiske Union ('EU').

EDPS støttede op om denne bemyndigelse og udtalte, at det er nødvendigt med en aftale, som gør det muligt at dele personoplysninger med tredjelande af retshåndhævelsesmæssige årsager i forbindelse med sager om cyberkriminalitet, og at en sådan aftale bør være i overensstemmelse med EU-traktaterne og EU's Charter om grundlæggende rettigheder. Formålet med udtalelsen var at komme med konstruktive og objektive råd til EU's institutioner, inden Rådet skulle afgøre, hvorvidt EU-Kommissionen skulle bemyndiges til at deltage i forhandlingerne.

Derudover opstillede EDPS tre overordnede anbefalinger til det andet tillæg. EDPS anbefalede, at tillægget skulle være obligatorisk, at der skulle indføres særlige sikkerhedsforanstaltninger og at man bestred enhver bestemmelse om direkte adgang til personoplysninger.

Den 6. juni 2019 besluttede Rådet at give EU-Kommissionen de nødvendige mandater til at indgå i forhandlingerne.

Læs hele udtalelsen her: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_budapest_convention_en.pdf

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


simonsen vogtwiig

Hedda Baumann Heier
og Rune Ljostad

Borgarting lagmannsrett: Import av telefonskjermer med tildekkede eple-logoer utgjør varemerkeinngrep

Borgarting lagmannsrett avsa 21. juni 2019 dom i sak mellom Apple Inc. og Henrik Huseby som driver enkeltpersonsforetaket PC-Kompaniet som blant annet utfører reparasjoner på smarttelefoner fra Apple. Lagmannsretten kom til motsatt resultat av tingretten (tingrettsdommen er omtalt i Lov&Data nr. 134 Juni/2018).

Bakgrunnen for saken var at tolletaten i juli 2017 stanset en postforsendelse fra Hong Kong til PC-Kompaniet med 63 mobilskjermer. Tolletaten begrunnet tilbakeholdelsen med at alle skjermene var påført Apples karakteristiske eple-logo som deretter var tildekket med tusj (som kunne fjernes med sprit). Alle de tildekkede eple-logoene befant seg på den delen av skjermen som vil være skjult innvending etter at skjermen er montert på telefonen.

I saken var det ikke bestridt at de importerte skjermene hadde en (tildekket) eplelogo lik Apple's varemerke, at importen skjedde i næringsvirksomhet og at Apple ikke hadde gitt Huseby tillatelse til å bruke varemerket. Uenigheten i saken knyttet seg til hvorvidt bruksvilkåret var oppfylt, jf. varemerkeloven § 4.

Spørsmålet i saken, slik lagmannsretten så det, var først og fremst hvorvidt skjermene var piratkopier eller om de var såkalt «refurbished», altså at de inneholder autentiske deler fra Apple som Apple i sin tid satt sitt varemerke på. Dersom sistnevnte hadde vært tilfellet, ville det kunne reist spørsmål skjermene var bragt i omsetning i EØS-området av Apple eller med Apple's samtykke på en slik måte at varemerketen ble konsumert. Lagmannsretten kom imidlertid ikke inn på dette, noe som kan ses i sammenheng med at retten etter en konkret bevisvurdering kom til at det var sannsynliggjort at skjermene var ulovlige kopier.

Etter lagmannsrettens syn var det ikke av betydning at varemerket befant seg på den delen av skjermen som vil være skjult for forbrukere etter montering, fordi den relevante omsetningskretsen ikke var forbrukere men næringsdrivende som importører, forhandlere og autoriserte reparatører. Lagmannsretten anså det heller ikke nødvendig å ta stilling til betydningen av tildekkingen når den først hadde funnet at det var snakk om vareforfalskninger. Retten velger likevel å knytte visse kommentarer til dette og finner blant annet støtte i Rt 1975 s. 951. Etter lagmannsrettens syn var det heller ikke grunnlag for noen innskrenkende fortolkning da det nødvendigvis var fare for skade.

Resultatet ble at lagmannsretten fant at det forelå varemerkeinngrep etter varemerkeloven § 4. Apple ble gitt medhold i krav om destruksjon og erstatning. Ved utmålingen ble en lisensavgift på 17,5 % ansett rimelig. Retten gav også Apple medhold i krav om dekning av lager- og destruksjonskostnader.

Les hele dommen med saksnummer LB-2018-62352 i Lovdatas database. I skrivende stund er det ukjent om dommen er anket.

Portabilitetsforordningen trer i kraft i Norge fra 1. august 2019.

Forordningen er inkorporert gjennom § 112a i åndsverksloven.

Les Kulturdepartementets pressemelding her: https://www.regjeringen.no/no/aktuelt/fra-1.-august-kan-du-se-favorittseriene-dine-i-utlandet/id2661289/

Hedda Baumann Heier er advokatfullmektig i Advokatfirmaet Simonsen Vogt Wiig AS, Oslo.

Rune Ljostad er partner i Advokatfirmaet Simonsen Vogt Wiig AS, Oslo.


Bird & Bird

Karin Söderberg
och Kajsa Zenk

Nyheter, parodier och upphovsrätten

Bakgrund

Förhållandet mellan yttrande- och informationsfrihet å ena sidan och upphovsrätt å andra sidan har ofta varit föremål för diskussioner, inte minst i relation till det nya upphovsrättsdirektivet. Att just denna avvägning kan ge upphov till diskussioner är inte svårt att föreställa sig, för visst är det svårt att säga vilken av två grundläggande rättigheter som bör väga tyngst då de ställs mot varandra.

En situation där förhållandet mellan yttrande- och informationsfrihet och upphovsrätt är högst aktuellt är i de fall då nyhetskanaler använder material som de inte äger rättigheterna till i samband med att de informerar om en viss händelse. Just en sådan situation prövades nyligen av Patent- och marknadsöverdomstolen i mål PMT 1473-18.

Målet grundar sig på en händelse som utspelade sig år 2010 och som i media benämnts som "järnrörsskandalen". Händelsen spelades in via en mobiltelefon av en privatperson, som även var politiker, som sedan gav tillstånd åt det politiska partiet Sverigedemokraterna att offentliggöra delar av mobilfilmen. En tid senare visade Sveriges Television (SVT) delar av mobilfilmen, och stillbilder tagna vid samma tillfälle, som inte ingått i den tidigare offentliggjorda versionen, via både TV och internet på sin websida och streamingsajt.

Personen som spelat in mobilfilmen väckte talan mot SVT och yrkade att SVT skulle betala ersättning för deras användning av mobilfilmen. SVT svarade med att upphovsrättens regler om ersättning inte skulle tillämpas på den aktuella användningen av mobilfilmen och stillbilderna då de omfattades av inskränkningarna i upphovsrättslagen gällande användning av material i samband med rapportering av dagshändelser och parodier. SVT menade också att användningen av skyddat material i ett fall som det aktuella måste vara tillåtet med beaktande av yttrande- och informationsfriheten. Som argument därför anfördes att händelsen som dokumenterats rörde ledande politiker och utspelade sig inför ett riksdagsval samt att händelserna förnekades av företrädare för det involverade politiska partiet.

Bedömning

Skyddade verk

Patent- och marknadsdomstolen hade vid sin prövning ansett att någon upphovsrätt inte kan anses omfatta den aktuella typen av dokumenterade videor och bilder då de endast utgör en bild- och ljudupptagning av ett skeende som den som filmar/fotograferar inte närmare har kunnat förutse eller styra över. Istället angavs att mobilfilmen och bilderna skyddades genom upphovsrättslagens närliggande rättigheter. Att mobilfilmen och bilderna åtnjöt sådant skydd var ostridigt i Patent- och marknadsöverdomstolen. Det skydd som ges sådana rättigheter är i stort det samma som ges ett upphovsrättsskyddat verk. Den som innehar den närstående rättigheten har exklusiv rätt att framställa exemplar av upptagningen, och göra upptagningen tillgänglig för allmänheten.

Efter att ha konstaterat att det material som SVT visat på sina olika kanaler inte tidigare offentliggjorts slog Patent- och marknadsöverdomstolen även fast att SVT framställt exemplar av delar av mobilfilmen och att delar av mobilfilmen har gjorts tillgängliga för allmänheten.

Nyhetsrapportering

Vid sin prövning av frågan om en inskränkning i upphovsrätten kunde föreligga med stöd i 23 § 3 st. upphovsrättslagen som ger en tidning rätt att återge bland annat fotografiska bilder i samband med en redogörelse för en dagshändelse, påpekade Patent- och marknadsöverdomstolen att paragrafen ska tolkas direktivkonformt. Enligt direktivet får medlemsstaterna föreskriva inskränkningar i ensamrätten för användning i samband med nyhetsrapportering, i den mån det är motiverat av informationssyfte. Vid den bedömningen noterades att det för att inskränkningen ska vara tillämplig enligt upphovsrättslagen ställs krav på att den fotografiska bilden i fråga ska vara offentliggjord (det vill säga lovligen tillgängliggjorts för allmänheten), ett krav som inte ställs i motsvarande artikel i direktivet. Inskränkningen som ges genom upphovsrättslagen är således snävare än inskränkningen av samma slag som framgår av direktivet.

Efter att ha konstaterat detta angav Patent- och marknadsöverdomstolen dock att den svenska lagen inte kan tolkas utanför sin ordalydelse varför kravet på att alstret måste vara offentliggjort ska stå fast.

Även vid bedömningen av tillämpligheten av inskränkningen som presenteras i 25 § upphovsrättslagen, som anger att verk som syns eller hörs under en dagshändelse får återges vid information om dagshändelsen i vissa medier, noterades vissa skillnader till motsvarande inskränkning i direktivet. Som exempel angavs att det i direktivet inte finns samma begränsning som i 25 § upphovsrättslagen angående att det ska vara fråga om alster som ”syns eller hörs under en dagshändelse”. Patent- och marknadsöverdomstolen konstaterade att upphovsrättslagen är mer begränsande än direktivet även när det gäller denna inskränkning. Samma bedömning gjordes dock även här som i förhållande till 23 § upphovsrättslagen och domstolen angav att paragrafen inte kan tolkas direktivkonformt i sådan utsträckning att det går emot den svenska lagens ordalydelse.

Parodier

Det kan även kort nämnas att några av SVT:s programinslag enligt Patent- och marknadsöverdomstolen var parodier och därför tillåtna enligt parodiundantaget. Parodiundantaget finns inte uttryckligen reglerat i upphovsrättslagen och nämns inte heller i förarbetena till genomförandet av direktivet vari parodiundantaget framkommer. Patent- och marknadsöverdomstolen anförde dock att det i de ursprungliga förarbetena till upphovsrättslagen uttalades att det av gammal hävd har ansetts tillåtet att göra en parodi av att verk och att det inte fanns någon avsikt att ändra på det även om det inte ansågs vara nödvändigt att särskilt reglera det. Även praxis från Högsta domstolen har bekräftat uttalandena i förarbetena om att parodier ska vara tillåtna enligt svensk rätt (se bland annat NJA 1975 s. 679, NJA 2005 s. 905 och NJA 2017 s. 75). Dock anförde domstolen att det synsätt som tidigare kommit till uttryck i svensk rätt avseende parodier, det vill säga att parodin ses som självständiga verk, inte längre kan tillämpas. Parodiundantaget måste istället tolkas konformt med EU-rätten, vilket innebär att parodin inte måste uppvisa egen originalitet, utan endast skilja sig märkbart från det originalverk som parodieras. I detta fall bedömdes parodierna skilja sig märkbart från mobilfilmen och omfattades således av parodiundantaget.

Yttrande- och informationsfriheten

Patent- och marknadsöverdomstolen inledde sin bedömning av om yttrandefriheten kan användas som ett argument för att inskränka upphovsrätten med att konstatera att närliggande rättigheter enligt upphovsrättslagen har ställning som grundläggande rättighet i och med rätten till egendom. I en situation som denna, då två grundläggande rättigheter ställs emot varandra, måste en proportionalitetsbedömning göras. Domstolen påpekade vidare att Europadomstolen, när den har prövat konflikter mellan yttrandefriheten och upphovsrätten, har framhållit att de nationella myndigheterna har stor frihet vid avvägningen av de olika intressena. Enligt Patent- och marknadsöverdomstolen utgör upphovsrättslagen med sina uttryckliga undantag och inskränkningar i ensamrätten, bland annat 23 och 25 § upphovsrättslagen, resultatet av en noggrann avvägning mellan dessa olika intressen.

Å enda sidan framhöll Patent- och marknadsöverdomstolen att det faktum att rättighetshavaren, det vill säga personen som filmat och fotograferat händelsen, inte velat offentliggöra de aktuella delarna av mobilfilmen och fotografierna starkt talade till förmån för egendomsintresset. Principen om rättighetshavarens ensamrätt att förfoga över sitt skyddade alster och avgöra om alstret ska behållas inom den privata sfären förstärks av att den korresponderar med rätten till skydd för privatliv. Å andra sidan angavs till förmån för intresset av yttrandefrihet att SVT:s användning av alstren har skett i journalistiskt syfte för att granska ett klandervärt beteende hos politiker i ledande ställning. Det som slutligen verkar avgöra domstolens avvägning är dock att domstolen menar att inget har hindrat SVT från att rapportera om händelserna. Domstolen menar därmed att SVT:s yttrande- och informationsfrihetsintressen hade kunnat tillgodoses utan att det var nödvändigt för SVT att, utan rättighetshavarens samtycke, framställa exemplar av mobilfilmen eller göra den tillgänglig för allmänheten.

Patent- och marknadsöverdomstolen bedömde således att rättighetshavarens intresse av egendomsskydd i detta fall vägde tyngre än SVT:s yttrande- och informationsfrihetsintresse.

Sammanfattning

Det aktuella målet visar på bedömningar avseende tolkning av svensk rätt i förhållande till EU-rättsliga direktiv och speciellt gällande intressanta avvägningar mellan viktiga rättigheter där upphovsrätten i detta fall har getts en stark ställning i förhållande till yttrande- och informationsfriheten.

Gällande nyhetsrapportering fann Patent- och marknadsöverdomstolen vissa skillnader i uttrycksätt mellan upphovsrättslagen och motsvarande artikel i aktuellt direktiv, där Sverige vid införande av direktivet gett de respektive inskränkningarna ett snävare utrymme än motsvarande inskränkning i direktivet. Skillnaderna i uttryckssätt kunde anses ligga i linje med att Europadomstolen har gett staterna stor bedömn-

ingsfrihet gällande avvägningen i konflikter mellan immaterialrättsliga intressen och yttrandefrihetsintressen, men att syftet med direktivet, det vill säga att uppnå en skälig avvägning mellan å ena sidan egendomsskyddet och å andra sidan yttrande- och informationsfriheten, ska beaktas.

Även gällande parodier finns vissa skillnader mellan den EU-rättsliga och den svenska bedömningen. I denna del valde emellertid Patent- och marknadsöverdomstolen att göra ett intressant avsteg från tidigare svensk praxis genom att konstatera att en parodi inte längre ska bedömas som självständigt verk. Parodier ska istället bedömas med utgångspunkt i EU-rätten och därmed måste en parodi inte uppvisa egen originalitet, men den ska märkbart skilja sig från det originalverk som parodieras.

Det sista ordet avseende frågan om hur intresseavvägningarna och tolkningarna av svensk rätt och EU-rätt ska göras är ändå troligtvis inte ännu sagt. Patent- och marknadsöverdomstolens domar kan som huvudregel inte överklagas, men i detta mål har domstolen beviljat en så kallad ventil, vilket innebär att överklagande till Högsta domstolen kan ske. Detta eftersom målet ansågs röra frågor där det är av vikt för ledning av rättstillämpningen att de även prövas av Högsta domstolen. Något överklagande har, när denna artikel skrivs, inte inkommit men än har parterna några dagar på sig. Vi hoppas givetvis på att få en dom även från Högsta domstolen i detta mål!

Karin Söderberg är biträdande jurist och arbetar i Bird & Birds IP-grupp sedan 2013. Hon har under sina verksamma år arbetat brett med olika immaterialrättsliga frågor, bland annat inom varumärkesrätt, upphovsrätt och marknadsrätt.

Kajsa Zenk är biträdande jurist och arbetar i Bird & Birds IP-grupp. Hon tog examen vid Uppsala universitet hösten 2018 och är IP-gruppens senaste tillskott.

Gorrissen Federspiel

Tue Goldschmieding

1. Brug af konkurrents varemærke som Google AdWord var en overtrædelse af den danske varemærkelov og markedsføringslov

Den danske sø- og handelsret ('Sø- og Handelsretten') afsagde den 15. marts 2019 dom i sagen BS-8990/2018-SHR mellem ChefMe IVS og ChefMade ApS. Sagen drejede sig om, hvorvidt betegnelsen »ChefMade« krænkede ChefMe IVS' varemærke »ChefMe«, og hvorvidt ChefMade ApS havde overtrådt den danske varemærkelov ved at benytte »ChefMe« som Google AdWord.

Retten fastslog indledningsvist, at »ChefMe« og »ChefMade« ikke var forvekslelige. Retten lagde i den forbindelse vægt på, at ordene »Me« og »Made« var forskellige både visuelt, fonetisk og betydningsmæssigt, ligesom at der ikke var sammenfald mellem ydelserne, som de to firmaer leverede. Sø- og Handelsretten fandt derfor, at betegnelsen »ChefMade« ikke krænkede det registrerede varemærke.

Retten fandt det dog bevist, at ChefMade ApS havde benyttet ChefMe IVS' registrerede varemærke »ChefMe« som søgeord i forbindelse med deres markedsføring gennem Google AdWords. ChefMade ApS' brug af varemærket medførte, at søgninger på Google efter »ChefMe« producerede et søgeresultat, hvor en annonce for ChefMade ApS fremgik som det første sponsoreret søgeresultat og dermed øverst på resultatlisten.

Retten vurderede, at anvendelsen havde givet anledning til forveksling mellem ChefMade ApS' og ChefMe IVS' virksomhed, jf. den danske varemærkelovs § 4, stk. 2. På baggrund af dette pålagde retten ChefMade ApS at betale et vederlag for anvendelsen, jf. den danske varemærkelovs § 43, stk. 1, nr. 1. Retten fastsatte vederlaget skønsmæssigt til 5.000 kr.

Læs hele dommen her:
http://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-8990-2018.pdf

2. Brug af navnet Ørsted var ikke en krænkelse af den danske navnelov, varemærkelov eller selskabslov

Den 10. maj 2019 afsagde den danske sø- og handelsret ('Sø- og Han-

delsretten') dom i sagen BS-3803/2018-SHR m.fl. mellem efterkommere af den kendte videnskabsmand H.C. Ørsted og Ørsted A/S (tidligere DONG Energy A/S).

DONG Energy A/S skiftede i 2017 navn til Ørsted A/S. På baggrund af navneskiftet anlagde en række efterkommere af H.C. Ørsted sag ved Sø- og Handelsretten med påstand om forbud mod brug af navnet Ørsted. Hovedspørgsmålet i sagen var, om slægtsnavnet Ørsted var et beskyttet efternavn, og om det gav navnebærerne mulighed for at forbyde andres brug af navnet.

Sø- og Handelsretten fastslog indledningsvist, at personnavnet Ørsted var et beskyttet efternavn omfattet af lovbekendtgørelse nr. 1816 af 23. december 2015 ('den danske navnelov'), da navnet bæres af færre end 2.000 personer.

Herefter konstaterede Sø- og Handelsretten, at sagens spørgsmål ikke alene skulle afgøres efter navneloven. Spørgsmålet skulle således afgøres på grundlag af speciallove med inddragelse af navneloven i relevant omfang. Ifølge lov nr. 341 af 6. juni 1991 ('den danske varemærkelov') § 14, nr. 4. kan et varemærke, der indeholder et personnavn, til hvilket en anden har lovlig adkomst, udelukkes fra registrering, medmindre der henvises til en for længst afdød person.

Sø- og Handelsretten fandt, at Ørsted A/S' anvendelse af Ørsted er en henvisning til den for længst afdøde videnskabsmand. Varemærket »Ørsted« var således ikke udelukket fra registrering, jf. den danske varemærkelovs § 14, nr. 4.

Retten konkluderede, at Ørsted A/S' ret til at anvende Ørsted som varemærke også gav dem ret til at benytte varemærket som selskabsnavn, uanset navnet samtidig var et slægtsnavn, jf. lov nr. 470 af 12. juni 2009 ('den danske selskabslov') § 2, stk. 2.

Læs hele dommen her: http://domstol.fe1.tangora.com/media/-300011/files/Dom_i_BS-3803-2018-SHR__BS-3836-2018-SHR__BS-4.pdf

3. Brug af kendetegnene »Bar'bette« og »Bar'bette's« krænkede varemærket »Babette«

Den 12. april 2019 afsagde Sø- og Handelsretten dom i sagen BS-34707/2018-SHR mellem Restaurant Babette ApS ('Restaurant Babette') og Babette Guldsmeden ApS ('Babette Guldsmeden').

Sagen omhandlede spørgsmålet om, hvorvidt Babette Guldsmeden havde overtrådt et forbud mod at anvende ordet »Babette« ved salg af mad og drikke, og hvorvidt deres anvendelse af »Bar'bette« og »Bar'bette's« var en krænkelse af Restaurant Babettes varemærket til ordet »Babette«. Forinden sagen havde Babette Guldsmeden fået forbud mod at anvende ordet »Babette« i forbindelse med salg af mad og drikke ved dom fra Østre Landsret den 28. marts 2017.

Sø- og Handelsretten konkluderede, at Babette Guldsmedens enkeltående brug af ordet »Babette« på et A-skilt ikke var en forsætlig krænkelse af forbuddet, da A-skiltet var anvendt af en medarbejder ved en fejl, og da det var blevet fjernet straks efter henvendelse fra modpartens advokat.

I forhold til Babette Guldsmedens brug af ordene »Bar'bette« og »Bar'bette's« fastslog Sø- og Handelsretten, at ordene havde fonetisk og visuel lighed med »Babette«, hvorfor der var forvekslingsrisiko for forbrugerne, især da ordene blev brugt i forbindelse med restauranten på et hotel ved navn Babette.

Efter en helhedsvurdering konkluderede Sø- og Handelsretten derfor, at Guldsmeden Babette havde krænket Restaurant Babettes varemærke ved brugen af disse ord. Brugen af »bette« som en betegnelse for noget småt kunne ikke lede til et andet resultat, da det ikke kunne forventes, at forbrugerne ville opfatte det som en betegnelse for en lille bar som ellers anført af Babette Guldsmeden.

Læs hele dommen her: http://domstol.fe1.tangora.com/media/-300011/files/Dom34707.pdf

4. Det danske folketing vedtager lovforslag, der fritager digitale aviser for moms

Den 7. maj 2019 vedtog det danske folketing ('Folketinget') et nyt lovforslag om indførelse af nulmoms på elektronisk leverede aviser. Formålet med loven var at omlægge støtten til nyhedsmedier, således at den var ensartet for både trykte og internetbaserede nyhedsmedier. Loven trådte i kraft den 1. juli 2019.

Levering af varer og ydelser pålægges som udgangspunkt 25 pct. moms i Danmark dog undtaget levering af trykte aviser, jf. lov nr. 760 af 21. juni 2016 ('den danske momslov') § 34, stk. 1, nr. 18, og § 37, stk. 1, idet disse er omfattet af en såkaldt nulmoms. Virksomheder der udgiver eller importerer aviser, skal til gengæld betale lønsumsafgift, jf. lov nr. 237 af 7. marts 2017 ('den danske lønsumsafgiftslov') § 1, stk. 1. Lønsumsafgiften er 3,54 pct. af værdien af virksomhedens salg af aviser, jf. den danske lønsumsafgiftslovs § 5, stk. 4, og § 4, stk. 5.

Det har hidtil ikke været muligt at udvide nulmomsen til elektronisk leverede aviser i medfør af Europa-Parlamentets og Rådets direktiv 2006/112/EF af 28. november 2006 ('momsdirektivet'). Dette blev imidlertid ændret ved Europa-Parlamentets og Rådets direktiv 2018/1713/EU af 6. november 2018 om ændring af momsdirektivet, hvorefter det nu er muligt for de enkelte EU-lande at indføre den samme momsmæssige behandling

af elektroniske versioner, som der anvendes på levering af bøger, aviser og tidsskrifter.

Ændringen medfører, at internetbaserede nyhedsmedier, herunder elektronisk leverede aviser, i medfør af denne lov nr. 591 af 13. maj 2019 bliver omfattet af den gældende nulmoms for trykte aviser og samtidig pålægges lønsumsafgift. Herved vil trykte og elektronisk leverede aviser betale samme afgifter. De overordnede kriterier for, om der momsmæssigt foreligger en avis ændres ikke, og det er ikke et krav, at den elektronisk leverede avis kan modsvares af en trykt avis.

Læs hele lovændringen her: https://www.ft.dk/samling/20181/lovforslag/l222/index.htm

5. Den danske forbrugerombudsmand sætter øget fokus på brug af affiliate-netværk

Den danske forbrugerombudsmand ('Forbrugerombudsmanden') afsluttede i 2018 og 2019 en række sager, hvor flere virksomheder havde fremsendt e-mails via såkaldte affiliate-netværk til forbrugere. Efter Forbrugerombudsmandens opfattelse kunne virksomhederne ikke godtgøre, at forbrugerne havde givet samtykke til at modtage e-mails med markedsføring fra virksomhederne, hvorfor der var tale om spam jf. lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov') § 10, stk. 1.

Forbrugerombudsmanden udtalte, at det kunne konstateres, at annoncørerne ofte havde anvendt affiliate-netværk, når forbrugerne havde klaget over spam. Det er nu blevet indskærpet over for både virksomheder, der benytter affilitate-netværk, og operatørerne af affiliate-netværkene, at de kan gøres ansvarlige, såfremt der sendes markedsføring til forbrugere, der ikke har givet samtykke til at modtage e-mails.

Forbrugerombudsmanden har et skærpet fokus på spam, og Forbrugerombudsmanden forventer at behandle flere sager med henblik på at politianmelde overtrædelser af forbuddet mod uanmodet spam i den danske markedsføringslov.

Læs hele udtalelsen her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2019/forbrugerombudsmanden-skaerper-fokus-paa-spam-fra-affiliate-netvaerk/

6. Den danske forbrugerombudsmand udgiver vejledning om webshops, der sælger abonnementer

I år 2018 blev der sendt 307 klager til den danske forbrugerombudsmand ('Forbrugerombudsmanden') over webshops' salg af produkter, hvor det viste sig, at salget forudsatte tegning af et abonnement. Forbrugerombudsmanden politianmeldte tillige i 2018 fire virksomheder for at vildlede forbrugerne ved at benytte denne metode. Derfor har Forbrugerombudsmanden offentliggjort en vejledning om, hvordan virksomheder, der sælger abonnementer på nettet, ikke overtræder bestemmelserne i lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov') om vildledende markedsføring.

I vejledningen er det præciseret, at virksomheden først og fremmest tydeligt skal oplyse forbrugerne ved købet, at forbrugerne samtidigt tegner et abonnement. Derudover skal der af hjemmesiden fremgå oplysninger om indholdet af abonnementets pris, varighed, bindingsperiode og betingelser for opsigelse. Disse oplysninger skal fremgå både før, under og efter købet.

Vejledningen henvender sig primært til virksomheder, for at de kan overholde disse regler. Hvis virksomhederne ikke overholder reglerne, kan abonnementsaftalerne erklæres ugyldige i medfør af lov nr. 1457 af 17. december 2013 ('forbrugeraftaleloven') § 12, stk. 2. Derudover kan virksomheden straffes med bøde, jf. den danske markedsføringslov §§ 5 og 6 og § 37.

Læs hele vejledningen her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2019/forbrugerombudsmanden-offentliggoer-guide-til-webshops-der-saelger-abonnementer/

7. Den danske forbrugerombudsmand vurderer, at brugen af fiktive forlagspriser i markedsføring ikke er tilladt

Den danske forbrugerombudsmand ('Forbrugerombudsmanden') meddelte den 20. maj 2019, at brugen af udtrykket »forlagets pris« i markedsføring af bøger kan være en vildledende oplysning omfattet af lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov') § 5, stk. 1.

Meddelelsen kommer i forlængelse af boghandleren Saxo.com A/S' brug af udtrykket »forlagets pris« i sin sammenligning af bogpriser. I den pågældende sag sammenlignede Saxo.com A/S sine bogpriser med »forlagets pris«, selvom mange af bøgerne ikke kunne købes på forlagenes hjemmesider.

Forbrugerombudsmanden vurderede, at Saxo.com A/S' markedsføring gav forbrugerne det indtryk, at de kunne spare penge, hvis de valgte at købe bogen på Saxo.com A/S' hjemmeside i stedet for hos forlagene. Dog forudsætter sådan en sammenligning ifølge Forbrugerombudsmanden, at bøgerne reelt er til salg hos forlagene, hvilket ikke altid var tilfældet.

Derfor blev det ligeledes indskærpet, at udtrykkene »forlagets pris« og »vejledende pris« kun må bruges, hvis det reelt er markedsprisen. Det betyder, at selskabet skal kunne dokumentere, at produktet blev solgt til den oplyste pris hos et repræsentativt udsnit af sammenlignelige butikker.

Læs hele vurderingen her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2019/brug-af-fiktive-forlagspriser-i-markedsfoering-af-boeger-er-ikke-tilladt/

8. Domænet »advokat.dk« kunne ikke kræves overført

Det danske klagenævn for domænenavne ('Klagenævnet') traf den 26. april 2019 afgørelse i sagen j. nr. 2018-0724 mellem Advcrocatus ApS ('klager') og Advokatsamfundet ('indklagede'). Sagen angik, om klager kunne kræve domænenavnet »advokat.dk« overført.

Klager gjorde i sagen gældende, at de havde en stærk interesse i at anvende domænenavnet, eftersom selskabet drev en internetportal, der formidlede kontakten mellem danske forbrugere og advokater. Klager mente, at registreringen og opretholdelsen af domænenavnet var i strid med god domænenavnsskik, idet indklagede ikke havde anvendt domænenavnet aktivt i de seneste 21 år.

Klagenævnet fandt, at der måtte fortages en interesseafvejning, jf. lov nr. 164 af 26. februar 2014 ('den danske domænelov') § 25, stk. 1. Klagenævnet henviste til lovbekendtgørelse nr. 1284 af 14. november 2014 ('den danske retsplejelov') § 120, og de dertil knyttede væsentlige samfundsmæssige interesser i, at betegnelsen »advokat« kun benyttes af beskikkede advokater. Klagenævnet lagde til grund, at klager havde ikke en legitim interesse i domænet, da denne ikke drev advokatvirksomhed, ligesom klager ikke havde ansatte, der var beskikkede advokater. På baggrund heraf fandt klagenævnet, at brugen af en beskyttet titel som »advokat« som domænenavn for en uautoriseret portal ville kunne medvirke til at skabe uklarhed om kredsen af beskikkede advokater, hvorfor klager ikke kunne kræve domænet overført.

Læs hele afgørelsen her: https://www.domaeneklager.dk/sites/default/files/2019-05/2018-0724%20advokat.dk%20endelig.pdf

9. Domænet »vækstfonden.dk« kunne kræves overført

Det danske klagenævn for domænenavne ('Klagenævnet') traf den 26. april 2019 afgørelse i sagen j.nr. 2018-0761 mellem Vækstfonden ('klager') og W 5 Holding ApS ('indklagede'). Sagen angik, hvorvidt indklagede kunne tilpligtes at overføre domænenavnet »vækstfonden.dk« til klager. Klager var i juli 1992 blevet registreret under navnet Vækstfonden. Indklagede registrerede i marts 2005 domænenavnet »vækstfonden.dk«.

Klager gjorde gældende, at indklagedes registrering af domænenavnet var i strid med lov nr. 164 af 26. februar 2014 ('den danske domænelov') § 25, stk. 1 og stk. 2, om henholdsvis god domænenavnsskik og registrering med videresalg for øje.

Indklagede gjorde gældende, at en overdragelse skulle ske mod dækning af udgifter. Derudover bemærkede indklagede, at de havde været villige til at overdrage domænet uden betaling de sidste 14 år, men at klager ikke havde ønsket overtage domænenavnet i denne periode.

Klagenævnet lagde vægt på, at indklagede havde været villig til at overdrage domænet mod betaling, at domænet ikke havde været offentligt til salg, og at indklagede havde tilbudt at overdrage domænet uden betaling. Registreringen var derfor ikke var i strid med den danske domænelovs § 25, stk. 2.

Klagenævnet foretog en interesseafvejning ved vurdering af overtrædelsen af den danske domænelovs § 25, stk. 1. Klagenævnet fandt, at klageren havde væsentlig interesse i domænet, og at indklagede ikke tilstrækkeligt havde redegjort for formålet med registreringen. Klagenævnet fandt herefter, at indklagede skulle overføre domænenavnet »vækstfonden.dk« til klager.

Læs hele afgørelsen her: https://www.domaeneklager.dk/sites/default/files/2019-05/2018-0761%20vaekstfonden%20endelig.pdf

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

Dan Sørensen

IKT-Norge lanserer nye standardavtaler

Den nye porteføljen av standardavtaler fra IKT-Norge er bedre tilpasset dagens leveransemodeller, mer balanserte enn tidligere og har mange likheter med statens standardavtaler.

I tillegg til Den norske dataforening og Direktoratet for forvaltning og ikt (Difi) har også IKT-Norge en portefølje av standardavtaler for teknologileveranser. Denne porteføljen har ikke hatt noen større revisjoner siden 2010, og består nå av blant annet Avtale for ASP-tjenester, Ekomtjenester, IT-driftsytelser (outsourcing), Kjøp av utstyr og disposisjonsrett til standard programvare, Konsulentbistand, Rammeavtale, Software-as-a-Service, Systemutvikling og Vedlikehold og programservice.

IKT-Norges eksisterende standardavtaler benyttes først og fremst av leverandørene, og markedet har en generell oppfatning om at disse avtalene er noe ubalanserte i leverandørenes favør. På samme måte har tidligere versjoner av statens standardavtaler (SSA) fra Difi blitt oppfattet som ubalansert i kundenes favør.

Difi har gjennomført flere revisjoner de siste årene som har resultert i mer balanserte avtaler. Dette har nok ført til at leverandørene i større grad enn tidligere velger å benytte Difis standardavtaler fremfor IKT-Norges standardavtaler.

Det er grunn til å tro at IKT-Norge ønsker å gjøre standardavtalene mer balanserte, konsolidere og forenkle avtaletypene samt tilpasse avtalene til dagens leveransemodeller. I sitt utkast (juni 2019) til ny avtaleportefølje har IKT-Norge disse avtaletypene: Driftsavtalen, E-komavtalen, Kjøpsavtalen, Kjøpsbetingelser, Konsulentavtalen, Rammeavtalen, Tjenesteavtalen, Utviklingsavtalen og Vedlikeholdsavtalen. Med unntak av E-komavtalen og Kjøpsbetingelser, samsvarer utkastene til avtaletyper med Difis avtaletyper i SSA-porteføljen. Innholdsmessig minner reguleringene i utkastene fra IKT-Norge om reguleringene i SSAene og utkastene er mer balanserte enn eksisterende standardavtaler.

Videre er godkjenningsprosedyrene fortsatt enklere enn i SSAene, og kunden står noe svakere siden akseptansetesting/undersøkelsesperiodene er mindre omfattende eller fraværende. Ellers legger utkastene opp til endringsprosedyrer som gir kunden utvidede muligheter til å kreve endringer i leveransens omfang. Prosedyrene ligger nærmere endringsmekanismene i SSAene, men likevel i en forenklet drakt.

Et annet viktig område er reguleringen av ansvarsforhold når det gjelder standardiserte tredjepartsleveranser fra leverandørens underleverandører, som for eksempel standard programvare eller standard (sky)tjenester. I SSAene er reguleringen av disse ansvarsforholdene noe uklare og utilgjengelige for partene. I utkastene fra IKT-Norge er reguleringen tydelig, og slik at leverandøren har mer begrenset ansvar enn under SSAene.

For øvrig ser det ut til at utkastenes generelle ansvarsbegrensning også skal gjelde ved eventuelle erstatningskrav fra de registrerte i henhold til personopplysningslovens artikkel 82 – i motsetning til i SSAene hvor slike erstatningskrav er unntatt den ordinære ansvarsbegrensningen.

Det generelle inntrykket er at utkastene til nye standardavtaler fra IKT-Norge er inspirert av bestemmelsene i SSAene, men i forenklet form. Dette gjør at avtalene fremstår som mer brukervennlige, og kanskje flere vil foretrekke IKT-Norges nye standardavtaler fremfor de mer omfattende SSAene. Det blir interessant å se nærmere på innholdet i de endelige versjonene når disse blir lansert, og det er positivt at vi nå får en ny portefølje av reviderte standardavtaler.

Dan Sørensen er senioradvokat i avdelingen for HITEK i Advokatfirmaet Selmer, Oslo.

Gorrissen Federspiel

Tue Goldschmieding

1. Ikke erstatning for øgede omkostninger og tidsforbrug i forbindelse med it-projekt

Den danske byret i Glostrup ('Retten i Glostrup') afsagde den 14. maj 2019 dom i sagen BS 10C-590/2016 mellem Datacon A/S ('Datacon') og Flügger group A/S ('Flügger') vedrørende leverance af et ERP-system, som understøtter virksomheders forretningsprocesser inden for en række forretningsområder.

Datacon mente, at Flügger manglede at betale for dele af systemet, hvorfor der blev nedlagt påstand om betaling af 13.163.071,95 kr. Flügger mente, at Datacon havde sat sit timeforbrug for højt og krævet betaling for ydelser, der ifølge aftalen burde have været leveret vederlagsfrit. Flügger bestred betalingen 5.650.066,95 kr., og nedlagede selvstændig påstand om betaling af 15.000.000 kr. i erstatning for udgifter i forbindelse med leveringen af systemet.

Retten fandt, at ERP-systemet var mangelfuldt, idet det ikke havde været klar til at blive sat i drift på tidspunktet for den aftalte levering. Da der ikke havde været gennemført afprøvning af systemet som beskrevet i parternes aftale, var en række problemer og mindre fejl ikke identificeret og udbedret. Den manglende afprøvning var dermed den væsentligste årsag til de problemer, som opstod hos Flügger, efter at systemet blev sat i drift. Retten fandt ligeledes, at Datacon i mindre omfang havde faktureret for ydelser, som burde have været leveret vederlagsfrit.

Retten fandt endvidere, at Flügger var berettiget til erstatning for omkostningerne i forbindelse med udredning af manglerne i det omfang, Datacon ikke havde afhjulpet manglerne vederlagsfrit. Der kunne dog ikke ydes erstatning for eventuelle mangler vedrørende ERP-systemets infrastruktur, da Datacon ifølge parternes aftale ikke skulle levere infrastrukturen. Der fandtes heller ikke grundlag for at pålægge leverandøren særskilt ansvar for den rådgivning, leverandøren havde ydet i forbindelse med kundens etablering heraf.

Yderligere kunne der ikke ydes erstatning for øgede logistikomkostninger, konventionalbod til kunder og internt tidsforbrug, da disse poster måtte anses for at udgøre driftstab, følgeskader og andet indirekte tab, hvilket der i henhold til parternes aftale kun kunne ydes erstatning for, såfremt Datacon havde handlet groft uagtsomt. Dette fandt retten ikke var tilfældet.

Retten fastsatte skønsmæssigt Flüggers samlede erstatning til 8.000.000 kr., men fandt samtidig at dele af Datacons krav bestod.

Retten nedsatte Datacons krav til 5.163.071,95 kr. plus procesrente. Grundet sagens udfald fandt retten, at Flügger skulle betale sagsomkostninger til Datacon på i alt 3.150.000 kr. samt afholde udgifterne til syn og skøn.

Læs resumé af dommen her:
http://www.domstol.dk/glostrup/nyheder/domsresumeer/Pages/Ikkeerstatningfor%C3%B8gedeomkostningerogiinterntidsforbrugiforbindelsemedit-projekt.aspx

2. Den danske digitaliseringsstyrelse udgiver en statusrapport over den danske stats store it-projekter

Den danske digitaliseringsstyrelse udgav en statusrapport for den danske stats store it-projekter for 2. halvår af 2018. Det var den danske stats it-råd ('It-rådet'), der stod for udarbejdelsen af rapporten og vurderingen af projekternes tilstand. I alt var 37 projekter og ét program omfattet af statusrapporten.

It-rådet anvender »trafiklys« som parameter for vurdering af projekterne. Ved et rødt trafiklys forventes budgettet overskredet med mere end 10 pct., en forsinkelse på mere end tre måneder og en nettonutidsværdi på mindre end 90 pct. Ved gult trafiklys forventes budgettet overskredet med op til 10 pct., forsinket i op til tre måneder og en nettonutidsværdi på 90-95 pct. Ved grønt trafiklys forventes ingen overskridelser, højst én måneds forsinkelse og en nettonutidsværdi på mindst 95 pct.

I den pågældende periode tildelte It-rådet fem røde trafiklys, otte gule trafiklys og 24 grønne trafiklys. De tildelte gule og røde trafiklys skyldtes hovedsagligt forsinkelser i projekterne både i starten og i slutningen af forløbet.

It-rådets vurdering sker på baggrund af oplysninger om projekternes planlagte tidsplan samt forventede afvigelser herfra. Herudover sker vurderingen på baggrund af budget, forventede projektudgifter og gevinstrealisering.

Ved statusrapporteringen for 2. halvår af 2018 var kun ét projekt afsluttet. It-rådet forventer dog, at i alt 15 projekter vil blive afsluttet i 2019.

Læs hele rapporten her:
https://digst.dk/media/19303/statusrapport-2-halvaar-2018.pdf

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

KLIMANØYTRAL DISTRIBUSJON
Levert av Posten

NORGE P.P.
posten

Returadresse:
Lovdata
Postboks 2016 Vika
NO-0125 Oslo
Norge

Nytt fra

LOVDATA

NAV Rettskilder er en tjeneste utviklet i samarbeid mellom Stiftelsen Lovdata og NAV. Her finner du de mest sentrale lover, forskrifter, rundskriv m.m. som gjelder tjenester og ytelser i NAV, med lenker mellom de ulike kildene.

Du kan besøke den nye tjenesten på https://lovdata.no/nav/.