Lov & Data

Nr. 148
Desember 2021
Nr. 4/2021

Innhold

Lov&Data

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

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

Lovdata forbeholder seg rett til å bruke artikler og domsreferater i Lovdatas elektroniske systemer.

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

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

Abonnementspriser for 2022
Norge: nkr 385,- pr. år
Utland: nkr 468,- pr. år
Studenter, Norge: nkr 182,- pr år
Studenter, utland: nkr 244,- 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/*

Trykk og layout: 07 Media – 07.no

Leder

Denne høsten har det blitt enda større oppmerksomhet knyttet til sosiale medier og algoritmene som bestemmer hva plattformene viser oss i «feeden». I korthet kan man si at sosiale medier viser oss innhold basert på algoritmer som har et eneste formål: Maksimere den tid brukeren legger igjen på plattformen. Dette får mange uheldige utslag. Eksempelvis er det mindre relevant for algoritmene om det presenterte innholdet er destruktivt for brukerens mentale helse. I september publiserte Wall Street Journal en rapport med tittelen «Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show», og denne rapporten bør være pensum for alle foreldre.

Dette er imidlertid bare en av mange problemer knyttet til algoritmene. Det finnes undersøkelser som viser at omtrent halvparten av den voksne amerikanske befolkningen har Facebook som en kilde til nyheter. Det finnes ingen annen plattform som er i nærheten av dette. Hver eneste gang du klikker på et innhold som presenteres deg i «feeden», lærer Facebook litt mer om hva du (og andre som ligner deg) er villig til å bruke tid på. Dette handler altså ikke om hva du ønsker å bruke tid på, men hva som kan utløse et klikk.

Det er nemlig en forskjell på hva vi mennesker ønsker oss, og hva vi ønsker at vi ønsker oss. Algoritmene er kun opptatt av det første.

Dermed holdes brukeren i et univers hvor de mest primitive følelsene er avgjørende for innholdet du blir presentert. Det er gjerne dette man henviser til når man snakker om at algoritmene fører til en «Race to the bottom of the brainstem». I en verden hvor brukerne egentlig ønsker informasjon om klimaspørsmålet, er det saker om Meghan og Prince Harry som trender på sosiale medier.

Det er konstatert at mennesker oftere klikker på oppslag med en sint emoji enn oppslag med en glad emoji. Vi klikker også oftere på artikler med nyhetsoverskrifter som bekrefter de oppfatningene vi har fra før. For noen mennesker er dette enda mer tydelig enn andre, og algoritmene vet nøyaktig hvem dette er. De som tror på klimakrisen får dermed presentert nyhetsoverskrifter som går i den retningen,

mens den andre gruppen for presentert nyhetsoverskrifter om funn som peker i retningen av at menneskers påvirkning er mer begrenset. Slik splittes befolkningen.

Dersom du ber demokrater i USA om å estimere hvor stor andel av republikanerne tror rasisme fortsatt er et problem i USA, vil estimatet i snitt ligge på 40 %. Det riktige tallet er 75 %. Men algoritmene vet at sinte artikler med stoff som bekrefter mytene får flere klikk. Dermed får demokratene servert artikler om republikanere som benekter det åpenbare, og mytene lever videre. Når halvparten av den amerikanske befolkningen har Facebook som en viktig kilde til nyheter, er det lett å se at algoritmene skaper farlige ekkokamre.

Finnes det noen vei ut av dette? I Kina har myndighetene en slik kontroll over sosiale medier at brukernes oppmerksomhet kan styres. Vitenskapelige artikler dukker opp på sosiale medier selv om brukeren ikke tidligere har vist interesse for dette. Dersom brukeren viser interesse for vitenskapelige artikler innenfor et fagfelt, bombarderes vedkommende med mer stoff innen området. Om brukeren derimot viser interesse for stoff som kan føre til dårlig selvbilde, vil dette derimot ikke føre til gjentatte visninger.

Løsningen ligger selvfølgelig ikke i at myndighetene sensurerer sosiale medier. Men finnes det en middelvei, hvor man heller ikke overlater all makt til kommersielle krefter? Kanskje ligger det eneste håpet i å lære befolkningen om informasjonshygiene, trene folk til å ta bevisste valg om hvilken informasjon man vil oppsøke, slik at de i mindre grad baserer seg på informasjon som blir presentert av algoritmene til virksomheter som viser deg akkurat det som får deg til å klikke, og klikke og klikke.

Jarle Roar Sæbø

”Teknisk bearbetning eller teknisk lagring” – ett centralt rättsligt begrepp vid it-outsourcing

Av Christina Wikström

Den jurist som idag arbetar med it-juridik och digitalisering har utan tvekan stött på begreppet ”teknisk bearbetning eller teknisk lagring”. Begreppet förekommer på ett flertal ställen i den svenska lagstiftningen och har den senaste tiden uppmärksammats med anledning av It-driftsutredningens betänkanden. Men vilka konkreta tjänster omfattas egentligen av begreppet ”teknisk bearbetning eller teknisk lagring” och vilka gör det inte?

I denna artikel analyseras hur begreppet ”teknisk bearbetning eller teknisk lagring” har använts i lagtext, tolkats i rättspraxis samt uppfattats praktiken. Syftet med artikeln är att skapa förståelse för begreppet och klarlägga begreppets tillämpning vid myndigheters utkontraktering av olika typer av it-tjänster.

Begreppets förekomst

Begreppet teknisk bearbetning eller teknisk lagring introducerades i svensk rätt 1974 genom ändringar i

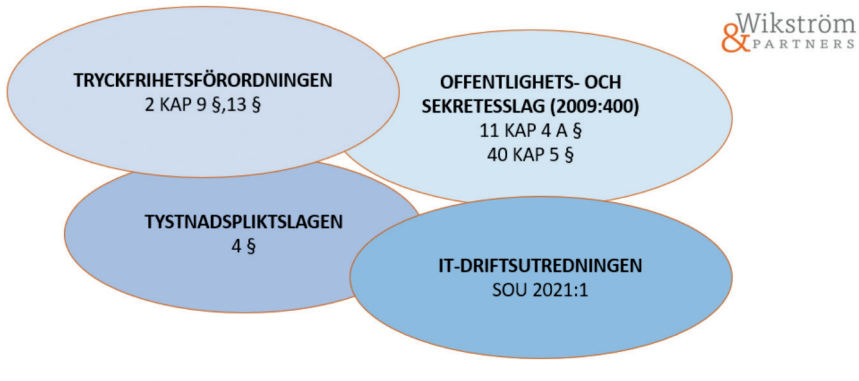
Christina Wikström

tryckfrihetsförordningen (TF). Sedan dess har begreppet återkommit i olika lagrum och förarbetsuttalanden (se bild).

Tryckfrihetsförordningen

Med handling avses enligt 2 kap 3 § TF en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas, avlyssnas eller uppfattas på annat sätt. Handlingar är allmänna om de förvaras hos en myndighet och är inkomna till eller upprättade hos en myndighet (2 kap 4 § TF). Vad gäller upptagningar anses de förvarade hos myndigheten om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller uppfattas på annat sätt enligt 2 kap 6 § TF. Av 2 kap 9 § första stycket TF framgår att en handling ska anses ha kommit in till en myndighet när den har anlänt till myndigheten eller kommit behörig befattningshavare till handa. Vad gäller upptagningar ska handlingen i stället anses ha kommit in till myndigheten när någon annan gjort den tillgänglig för myndigheten på det sätt som anges i 2 kap 6 § TF.

En åtgärd som vidtas endast som ett led i en teknisk bearbetning eller teknisk lagring av en handling som en myndighet har tillhandahållit ska däremot inte anses leda till att handlingen har kommit in till den myndigheten vilket framgår av (2 kap 9 § tredje stycket TF). Regleringen möjliggör att en myndighet anlitar en extern aktör för att endast tekniskt bearbeta eller tekniskt lagra



uppgifter, utan att upptagningen vid återkomsten till myndigheten i bearbetat skick blir att anse som en till myndigheten inkommen handling.

Av 2 kap 13 § första stycket TF framgår vidare att en handling som förvaras hos en myndighet endast som ett led i en teknisk bearbetning eller teknisk lagring för någon annans räkning inte är att anses som allmän handling hos den myndigheten.

Av propositionen framgår också ett antal exempel på teknisk bearbetning och teknisk lagring, men som är starkt kopplade till dåtidens teknik. Där nämns att datacentraler kunde utföra vissa åtgärder som föll inom begreppet så som överföring av ett maskinskrivet manuskript till magnetband. Även situationen att annan än datacentralen skulle utföra åtgärder så som tryckning eller kopiering av maskinskrivet manuskript, redigering av ljudupptagningar på magnetband, överföring av sådana upptagningar till grammofonskiva samt framkallning av fotografiskt material, bedömdes falla inom begreppet.[1] Trots att bestämmelserna i TF har ändrats ett antal gånger finns i de efterföljande förarbetena till TF inte några andra uttalanden om begreppets innebörd eller andra exempel på konkreta åtgärder som omfattas av begreppet.

Offentlighets- och sekretesslagen

I offentlighets- och sekretesslagen (2009:400) (OSL) återfinns bland annat regler om sekretess i offentlig verksamhet. Sekretess innebär ett förbud att röja uppgifter (3 kap 1 § OSL) och regelverket behöver beaktas när en myndighet utkontrakterar exempelvis drift av ett it-system.[2] Sekretessbestämmelserna i OSL gäller inte bara för uppgifter i allmänna handlingar utan även för uppgifter hos en myndighet som ännu inte blivit allmänna.

Om en myndighet i verksamhet för enbart teknisk bearbetning eller teknisk lagring för en annan myndighets räkning får en uppgift som hos den senare myndigheten är sekretessreglerad av hänsyn till ett allmänt intresse, blir sekretessbestämmelsen tillämplig även hos den mottagande myndigheten (11 kap 4 a § OSL). Sekretess gäller vidare i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning för uppgift om en enskilds personliga eller ekonomiska förhållanden (40 kap 5 § OSL).

Förarbetena till de aktuella sekretessbestämmelserna preciserar inte vilka konkreta tjänster som omfattas av begreppet teknisk bearbetning och teknisk lagring. I stället hänvisas till begreppets innebörd enligt TF.

Tystnadspliktslagen

I januari 2021 trädde lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (nedan tystnadspliktslagen) i kraft. I 4 w§ anges att den som på grund av anställning eller på något annat sätt deltar i eller har deltagit i en tjänsteleverantörs verksamhet att på uppdrag av en myndighet endast tekniskt bearbeta eller tekniskt lagra uppgifter inte obehörigen får röja eller utnyttja dessa uppgifter.

Trots förekomsten av begreppet teknisk bearbetning och lagring i ett flertal lagar finns det som sagt begränsat med konkreta exempel på vilka it-tjänster som idag skulle kunna klassificeras som teknisk bearbetning och lagring och en viss förvirring kring begreppets innebörd har förelegat, vilket kan utläsas av förarbetena till tystnadspliktslagen.[3] Den främsta ledningen för begreppets innebörd återfinns, förutom i propositionen till TF, i lagrådsremissen och propositionen till tystnadspliktslagen.

Av propositionen till tystnadspliktslagen framgår att innebörden av teknisk bearbetning eller teknisk lagring är densamma som i 2 kap 9 § tredje stycket TF, men att vilka slags åtgärder som kan omfattas av teknisk bearbetning eller teknisk lagring däremot behöver tolkas i förhållande till dagens digitala informationshantering och den fortgående tekniska utvecklingen. Det anges dock att ett uppdrag att endast tekniskt bearbeta och lagra uppgifter kan utföras inom ramen för en tjänsteleverantörs tillhandahållande av en it-driftstjänst, t.ex. en teknisk infrastruktur eller en teknisk plattform eller genom tillhandahållande av en it-baserad funktion, som en applikation eller en standardiserad eller anpassad digital tjänst. Det klargörs också att åtgärder under tjänstens livscykel exempelvis att införa, förvalta, utveckla och så småningom avveckla tjänsten, kan omfattas av begreppet. Ett antal exempel ges vidare på åtgärder som en tjänsteleverantör kan vidta för att upprätthålla tillgänglighet, funktionalitet och prestanda i tjänsten, vilka innefattar teknisk bearbetning eller lagring av uppgifter. Som exempel anges förändring och tillägg i en befintlig tjänsts funktionalitet, etablering av en tilläggstjänst, integration mot andra tjänster, konfiguration, test och utveckling samt tillhandahållande av supporttjänster. Utöver detta nämns säkerhetshöjande åtgärder som uppgradering, uppdatering, säkerhetskopiering, kryptering, anonymisering, pseudonymisering och incidenthantering, samt åtgärder så som migrering eller exportering av information vid avveckling av tjänster.[4]

1 Prop. 1975/76:160 s. 137

2 Se för en orientering i ämnet se eSam Outsourcing 2.0 - Vägledning om sekretess och dataskydd *www.esamverka.se*

3 SOU 2018:25 s. 74, 119, 279.

4 Prop. 2019/20:201 s. 22-23.

Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering (SOU 2021:1)

I januari 2021 överlämnades It-driftsutredningens betänkande *Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering* (SOU 2021:1). I delbetänkandet föreslås en ny sekretessbrytande bestämmelse som tar sikte på uppdrag att utföra teknisk bearbetning eller teknisk lagring.[5] I delbetänkandet framförs också ett synsätt på röjandebegreppet i OSL som skulle innebära att varje utkontraktering av it-drift är att betrakta som ett utlämnande av berörda uppgifter, oavsett om kryptering eller annan teknisk åtgärd har vidtagits för att begränsa eller minimera risken för att tjänsteleverantören tar del av uppgifterna.[6]

Den av utredningen föreslagna sekretessbrytande regeln har följande lydelse:

”Sekretess hindrar inte att en uppgift lämnas ut till ett företag eller en annan enskild eller till en annan myndighet som har i uppdrag att utföra endast teknisk bearbetning eller teknisk lagring av de uppgifter som lämnas ut för den utlämnande myndighetens räkning. En uppgift ska inte lämnas ut om det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut.”[7]

I SOU 2021:1 hänvisas till att begreppet teknisk bearbetning eller teknisk lagring förekommer i TF och OSL och därmed sedan länge är inarbetat. I delbetänkandet framhålls att även om uttrycket inte kan sägas vara alldeles entydigt framstår det som mer tydligt än uttrycket ”it-drift” och att man därför valt att avgränsa den sekretessbrytande bestämmelsen till att endast ta sikte på utkontraktering av teknisk bearbetning eller teknisk lagring av uppgifter. I SOU 2021:1 nämns också att uttrycket används i tystnadspliktslagen, vilken har ett nära samband med de frågor som behandlas i betänkandet.[8] I övrigt saknas i utredningen mer långtgående förtydliganden om begreppet endast teknisk bearbetning och teknisk lagring och dess betydelse i den föreslagna sekretessbrytande regeln.

Det kan framhållas att it-driftutredningen i skrivande stund arbetar med sitt slutbetänkande där förutsättningarna för samordnad statlig it-drift analyseras och redovisas. Utredningen har i uppdrag att presentera ett förslag på hur samordnad, säker och kostnadseffektiv it-drift kan tillgodoses. Även i detta sammanhang kommer begreppet endast teknisk bearbetning eller teknisk lagring få betydelse då myndigheter ska samverka inom de ramar för offentlighet och sekretess som TF och OSL skapar.

”Endast” eller ”enbart” teknisk bearbetning eller lagring

Begreppet teknisk bearbetning och teknisk lagring föregås av två olika ord i de ovan nämnda lagtexterna. I undantagsbestämmelserna i TF ska åtgärden *endast* ha vidtagits som ett led i en teknisk bearbetning eller lagring. För att bestämmelserna om sekretess i OSL ska aktualiseras handlar det i stället om att det är verksamheter för *enbart* teknisk bearbetning och lagring som ska behandla uppgifter. Ordet endast används i tystnadspliktslagen där tystnadsplikt gäller för en anställd eller någon som på annat sätt deltar eller har deltagit i en tjänsteleverantörs verksamhet att på uppdrag av en myndighet *endast* tekniskt bearbeta eller tekniskt lagra uppgifter. Samma formulering återfinns också i den föreslagna sekretessbrytande regeln i SOU 2021:1 – nämligen att sekretessen kan brytas vid ett utlämnande till företag, annan enskild eller annan myndighet som har i uppdrag att utföra *endast* teknisk bearbetning eller teknisk lagring av uppgifterna. I utredningen förtydligas också att avgränsningen innebär att tjänster som visserligen innefattar moment av teknisk bearbetning eller teknisk lagring, men som inte enbart avser sådan bearbetning eller lagring, inte ska omfattas av bestämmelsen.[9]

Förarbeten till lagbestämmelser som omfattar begreppet tekniska bearbetning eller teknisk lagring ger uttryck för att en samstämmighet ska råda i tolkning av begreppet. Vi kan inte finna stöd för att orden ”endast” och ”enbart” är tänkt att ha olika betydelse i detta sammanhang.

För annans räkning

En annan aspekt värd att notera är att de bestämmelser som finns gällande teknisk bearbetning eller teknisk lagring tar fasta på att åtgärderna ska ske för någon annans räkning. I SOU 2021:1 anges att det följer av den föreslagna bestämmelsens ordalydelse att sådan hantering av uppgifter som en privat tjänsteleverantör utför för ändamål kopplade till den egna verksamheten faller utanför den sekretessbrytande bestämmelsens tillämpning. Som exempel på detta nämns tjänsteleverantörens hantering av myndighetens uppgifter för utveckling av egna produkter och tjänster.[10] Betydelsen av detta rekvisit utvecklas närmare under avsnittet nedan om domstolspraxis.

Domstolspraxis som behandlar teknisk bearbetning och lagring

Begreppet teknisk bearbetning eller teknisk lagring har prövats i domstol vid några tillfällen. Främst handlar det om mål som rört rätten att ta del av allmän handling där undantagsregeln i 2 kap 13 § TF har aktualiserats.

I RÅ 1994 ref. 64 framhöll Regeringsrätten att Riksrevisionsverket (RRV) inte disponerade över redo-

5 SOU 2021:1 s. 33.
6 SOU 2021:1 s. 277.
7 SOU 2021:1 s. 33.
8 Se SOU 2021:1 s. 295.
9 SOU 2021:1 s. 295.
10 SOU 2021:1 s. 296.

visningsdata som behandlades i myndighetens ADB-stödda[11] ekonomi- eller redovisningssystem för andra myndigheters räkning mot ersättning. Uppgifterna ansågs vara förvarade endast som led i teknisk bearbetning eller teknisk lagring för annans räkning och därmed inte vara en allmän handling hos RRV. Liknande bedömningar har gjorts av Kammarrätten i Jönköpings mål nr 2692-10, 2010-11-15, Kammarrätten i Jönköpings mål nr 1929-12, 2012-08-21 och Kammarrätten i Göteborgs mål nr 428-17, 2017-05-09.

I Högsta förvaltningsdomstolens (HFD) avgöranden i HFD 2011 ref. 52 och i HFD 2018 ref 48 ansågs handlingar däremot inte vara förvarade hos myndigheterna endast som ett led i teknisk bearbetning eller lagring för annans räkning när befattningshavare kunnat ta del av uppgifterna i läsbart skick.

I HFD 2011 ref 52 hade handlingar i en databas gjorts tillgängliga för en mottagande myndighet då denna, utöver teknisk bearbetning och lagring även använde handlingarna för statistikframställning. Systemet i fråga var gemensamt för flera myndigheter och befattningshavare på den administrerande myndigheten kunde ta del av handlingarna i systemen för att inhämta underlag till statistik och rapporter.

I HFD 2018 ref. 48 bedömdes avvikelserapporter som införts i en kommuns verksamhetssystem av en privat hemtjänstutförare utgöra allmänna handlingar. För att en handling ska anses förvarad hos en myndighet ”endast” som led i teknisk bearbetning eller lagring krävs det enligt HFD att myndigheten såväl administrativt som tekniskt har begränsat den egna personalens tillgång till uppgifterna så att dessa inte är tillgängliga i läsbart skick. Så hade inte skett i det aktuella fallet där personalen på kommunen haft tillgång till rapporterna och även använt uppgifter i statistik som kommunen tog fram.

I en dom från Kammarrätten i Stockholm mål nr 7369–15, 2015-10-26, hade en journalist begärt ut handlingar från Arbetsförmedlingens CV-databas, lagrade på ett så kallat eget utrymme. Begäran nekades då Kammarrätten fann att handlingarna i databasen inte var något verksamhetssystem hos Arbetsförmedlingen, myndighetens handläggare saknade åtkomst till systemet och databasen inte heller användes för något statistikändamål eller likande. Detta talade enligt domstolen för att handlingarna förvarades hos Arbetsförmedlingen endast som ett led i teknisk bearbetning eller teknisk lagring för enskildas räkning. Att vissa anställda hade åtkomst till databasen för att administrera den ansågs däremot ligga i sakens natur och hindrade inte att undantagsbestämmelsen kunde vara tillämplig. I den mån handlingar från databasen skulle tas in i Arbetsförmedlingens handläggning av ärenden eller verksamhet kunde det däremot förutsättas att de skulle bli allmänna.

Doktrin och annan vägledning om begreppet

Inte heller i doktrin har det utvecklats någon stark eller etablerad uppfattning kring innebörden av begreppet teknisk bearbetning och lagring. Tvärtom understryks även där att det är oklart exakt vilka tjänster som omfattas av begreppet och att de tidigare uttalandena i förarbeten ska tolkas med hänsyn till dagens teknik.[12]

I anslutning till 40 kap 5 OSL, där det stadgas att sekretess gäller i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning för uppgift om en enskilds personliga eller ekonomiska förhållanden, har framhållits att tystnadsplikten kan gälla både i samband med tillhandahållande av digitala tjänster till enskilda och vid myndigheters utkontraktering av it-drift till en annan myndighet.[13] Mot den bakgrunden kan nämnas att en typ av teknisk bearbetning och lagring rönt särskild uppmärksamhet, nämligen det så kallade ”egna utrymmet”. Här åsyftas ett eget digitalt utrymme som en myndighet tillhandahåller till den enskilde för att förvara uppgifter till exempel ett utkast inför ingivande av en ansökan, där myndigheten enbart tekniskt bearbetar och lagrar uppgifterna för den enskildes räkning, utan egen tillgång till innehållet. Det egna utrymmets rättsliga status har varit föremål för olika uppfattning men förtydligats genom motiven till den nya förvaltningslagen. Av propositionen framgår att uppgifter som lagras på ett eget utrymme för den enskildes räkning omfattas av 2 kap 10 § första stycket TF, så vida inte uppgifterna görs tillgängliga för myndighetens handläggare före ingivandet av uppgifterna.[14]

Vad gäller frågan om eget utrymme har också eSam skrivit vägledningar, den senaste publicerad i mars år 2021.[15] För den som vill veta mer om bedömningar och innebörden av eget utrymme hänvisas till eSams webbsida där vägledningarna finns publicerade.[16]

Sammanfattande kommentar

Sammanställningen ovan visar att begreppet endast teknisk bearbetning och teknisk lagring kommit till användning i ett antal lagregleringar över åren. Mycket talar för att även framtida lagstiftning kommer att bygga på begreppet. Detta eftersom en strävan om likformighet och återhållsamhet tycks prägla lagstifta-

11 Automatisk databehandling

12 Magnusson m.fl., Rättsinformatik, s. 359

13 Lenberg, Tansjö, Geijer Offentlighets- och sekretesslagen En kommentar, avsnitt 40 kap 5 §.

14 Prop. 2016/17:180, s. 141 f.

15 eSam, Eget utrymme hos en myndighet - En vidareutveckling, mars 2021, s. 19–21.

16 www.esamverka.se

rens ambition att främja digitalisering av offentlig sektor.

Det hörs ofta röster som framhåller att begreppet är oklart och svårtolkat. Även som praktiserande advokat uppfattar jag att det finns rättsliga oklarheter kring begreppet ”endast teknisk bearbetning och lagring”. Men vi ser också att en samsyn har utvecklats om vilka it-tjänster som vid en utkontraktering kan anses utgöra teknisk bearbetning och lagring.

De traditionella infrastrukturtjänsterna där it-leverantören tillhandahåller drift, underhåll, lagring, säkerhetskopiering med tillhörande säkerhet- och övervakningstjänster ses allmänt som tjänster som kan omfattas av begreppet. Så uppfattar vi vara fallet oberoende om nämnda tjänster avser hårdvara, operativsystem, applikationer eller ett sammansatt system. Det kan framstå som självklart att de nödvändiga arbetsinsatser som krävs för att sätta upp, upprätthålla och avveckla infrastrukturtjänsten måste anses omfatta begreppet. Här bör särskilt nämnas tillhörande säkerhetstjänster av olika slag som ofta är en grundläggande förutsättning för att en myndighet ska kunna nyttja infrastrukturtjänsten.

Förekomsten av olika paketerade it-tjänster där leverantören tar ett helhetsansvar för att tillhandahålla systemfunktionalitet har successivt ökat de senaste decennierna. Vi uppfattar att även de paketerade infrastrukturtjänsterna kan omfattas av begreppet, under förutsättningen att de ingående beståndsdelarna inte går utöver de ovan nämnda separata infrastrukturtjänsterna. Till dessa paketerade tjänster hör systemleveranstjänsterna och it-baserade funktioner som också kan utgöra endast teknisk bearbetning och lagring, vilket också framgår av förarbeten till tystnadspliktslagen som redovisats ovan. Då lagstiftaren tydligt uttrycker att begreppet ska tillämpas teknikneutralt ser vi inte heller att bakomliggande teknik borde påverka synen på om begreppets tillämplighet. Till exempel borde molnbaserad teknik kunna användas för tillhandahållande av ovan nämna infrastrukturtjänster, men i sådant fall måste självfallet övriga rättsliga aspekter kring molntjänster beaktas för att en rättsenlig utkontraktering ska vara möjlig.

Däremot kommer vissa it-tjänster som saknar karaktär av ”enbart teknisk bearbetning eller teknisk lagring” falla utanför begreppet och därför inte omfattas av ovan nämnda lagregler. Som exempel kan nämnas tillhandahållande av it-arbetsplatstjänster där leverantören tillhandahåller funktionen it-arbetsplats, genom att leverera en sammansatt tjänst bestående av hårdvara, programvara och service/support. Även tillhandahållande av fristående it-supporttjänster till myndighetens användare via olika supportkanaler (telefon, webb, mejl etc.) avviker till sin karaktär på så sätt att den fristående it-supporttjänsten inte kan anses utgöra ”enbart teknisk bearbetning eller teknisk lagring”.

It-tjänstens grundläggande karaktär och förutsättningarna för dess tillhandahållande är således avgörande för om den kan anses omfattas av det aktuella begreppet. Men självfallet måste de övriga ovan redovisade rekvisiten kopplade till begreppet vara uppfyllda för att de redovisade rättsregler ska vara tillämpliga på it-tjänster som har karaktär av ”enbart teknisk bearbetning eller teknisk lagring”.

//Advokat Christina Wikström

Christina Wikström är advokat och Managing partner på Wikström & Partners Advokatbyrå. Christina är senior it-rättsexpert med mycket stor erfarenhet av digitalisering, innovation och dataskydd, från mångårig rådgivning inom privat och offentlig sektor, samt som medlem av eSam juridiska expertgrupp.

Källkodsdeposition under ständig förändring

Av Christina Wainikka og Tommy Svensson

Christina Wainikka

Tommy Svensson

Fungerande datorprogram är en nödvändighet i dagens samhälle. Hela den snabba digitaliseringen är beroende av datorprogram. Det leder ständigt till nya typer av frågor. Informationssäkerhet handlar inte bara om att skydda sig mot olika former av intrång utan också om att ha säker tillgång till data, att systemen fungerar med mera.

Ny programvara, även kallad mjukvara, utvecklas i rask takt. Befintlig programvara lever ett förändrligt liv. Den utvecklas och den anpassas för att samverka med annan programvara, ofta i avancerade IT-system. Fel upptäcks och sårbarheter måste åtgärdas. Sådana programmeringsinsatser kräver tillgång till programvarans källkoder

Trots att det finns immaterialrättsliga skydd finns det situationer där aktörer inte vill använda sig av öppen programvara. Det kan till exempel handla om en bedömning att hemlighållande i kombination med immaterialrättsliga skydd ger en bättre trygghet. Krav kan också ställas från investerare om att hemlighålla snarare än att släppa ut öppet.

Vi kommer här att belysa några rättsliga och praktiska frågor gällande programvara och källkoder.

Datorprogram i juridiken

Det finns flera olika perspektiv som kan läggas på datorprogram i juridiken. Det ena perspektivet är det rättsliga skydd som finns för programvara inom immaterialrätten. Det andra är vem som ska få ha tillgång till programvarans källkoder.

Frågan om, och i så fall hur, datorprogram ska få skydd i immaterialrätten har varit föremål för diskussion allt sedan programvara började användas i en större omfattning. De två rättigheter som särskilt stod i fokus var patenträtten och upphovsrätten.

Den väg som småningom valdes var huvudregeln att datorprogram ges skydd i upphovsrätten. Detta står också numera uttryckligen i 1 § upphovsrättslagen. På motsvarande sätt stadgas det uttryckligen i patentlagen att det inte går att få patent för det som utgör enbart ett datorprogram.

Här kan konstateras att diskussionen lever vidare. I amerikansk rätt har det patenterbara området för datorprogram ansetts vara mer omfattande. Företag som tar fram olika AI-lösningar kan exempelvis i mycket högre utsträckning få patent i amerikansk rätt än i europeisk rätt. I Europa förs diskussioner om det patenterbara området behöver utvidgas här, inte minst med tanke på den praxis som finns från Europeiska Patentorganisationen (EPO). I skrivande stund lär det vara så att de planerar en översyn av sina guidelines just när det gäller det patenterbara området i relation till datorprogram.

Vid sidan av de immaterialrättsliga aspekterna finns frågan om vem som ska ha tillgång till programvarans källkoder. När det gäller källkodsdeposition är detta något som inte lagstiftaren löst fullt ut. Vid sidan av de immaterialrättsliga ensamrätterna kan skydd även finnas för källkod som företagshemligheter. Det gör att hanteringen av källkoden är viktig att ha under säkra och kontrollerade former. Ett sätt att hantera det är källkodsdeposition.

Källkodsdeposition

Redan på 1970-talet blev det vanligt i USA att programvaruföretag deponerade källkoder (Source Code Escrow). Syftet var att säkerställa kundernas, licenstagarnas, verksamhet på lång sikt, oberoende av programvaruföretagets insatser. Risken

är annars att om något händer programvaruföretaget, exempelvis att det går i konkurs, kan kunderna riskera att inte få hjälp med anpassningar, nödvändigt underhåll m.m.

Nyligen kom en dom från EU-domstolen om rätten för en licenstagare att dekompilera programvara för att utöva sin lagstadgade rätt till ändring. Då kan tyckas att källkodsdeposition är överflödig, när licenstagaren ändå har rätt att tränga in i programvaran. En jämförelse kan vara att även om man har rätt att analysera sin favoritsås så är det lättare att använda receptet. Mänskligt begriplig källkod är för datorprogram vad receptet är för en maträtt.

Beroendet av verksamhetskritisk programvara i företag och förvaltning motiverar fortlöpande säkerhetsåtgärder av olika svårighetsgrad. Såväl stora som små programvaruföretag kan gå i konkurs eller av annan anledning försumma sina åtaganden gentemot kunderna enligt licensavtal och underhållsavtal. Programvaruföretag kan bli uppköpta och då kan underhåll av mjukvara upphöra p g a sammanslagningar av verksamheter och rationalisering av mindre lönsamma delar m.m. Nyckelpersoner kan lämna företag och äventyra en programvaras framtid. För kunderna eller licenstagarna är det i allmänhet mycket svårt och kostsamt eller i vissa fall nästan omöjligt att själva eller genom nya konsulter underhålla ett existerande datasystem utan tillgång till källkoden för den aktuella programvaran. Källkodsdeposition är en enkel åtgärd för att hantera den typen av risker. Enbart källkodsdepositionen medför dock ingen garanti för att det som deponeras är användbart för licenstagaren, mer om detta nedan.

Riskhantering handlar inte enbart om hotbilder utan även om affärsmöjligheter. En intressant utveckling är att programvaruföretag ser att depositioner ökar affärsmöjligheterna. Programvaruföretag ökar sin attraktionskraft hos kunder och investerare genom att självmant deponera källkoden. Den juridiska situationen blir fördelaktig för programvaruföretaget som då självt kan anvisa eller välja avtalsform och jurisdiktion. Till detta kommer att administrationen blir minimal vid uppdateringar, dessa kan göras på ett enda ställe oavsett var i världen kunderna befinner sig.

De upphovsrättsliga aspekterna finns också med bland motiven. Depositioner med tidsstämplar har ett visst bevisvärde om det uppstår en tvist mellan den rättighetsinnehavare som deponerat och någon tredje part som begår eller hävdar upphovsrättsintrång. Tidsstämplar kan alltså tjäna som bevisning om vem som hade gjort vad vid vilken tidpunkt, något som kan få stor betydelse för den som hävdar sig inneha det upphovsrättsliga skyddet.

Mer överraskande är de företag som regelbundet deponerar källkoder utan att det finns någon kund inblandad. Anledningen är att företaget löpande vill ”tanka ur” sina anställda utvecklare. En välkänd IT-profil beskrev en gång detta behov genom att konstatera att ”dokumentationen låg i bakfickan på ett par jeans som gått genom tvätten två gånger”.

För att få skydd av lagen om skydd för företagshemligheter krävs att rättighetsinnehavaren hanterar sina hemligheter med varsamhet och hög säkerhet internt. Depositioner hos en tredje part visar att källkoderna hanteras som en företagshemlighet. Om källkoderna i stället lämnades ut till alla avtalsmotparter hade kunnat ifrågasättas om hanteringen verkligen lever upp till hemlighetsrekvisitet, såsom det uttrycks både i nationell lagstiftning och i EU-direktivet på området.

I det följande fokuserar vi på ovanstående motiv. Dessa är många och varierande, vilket gör att frågor uppkommer hur man praktiskt och juridisk går till väga för att uppnå syftet med depositionen.

Avtalsparterna

Den som deponerar måste ha de *immateriella rättigheterna* eller ha ett medgivande från rättighetsinnehavaren. I och med att det ofta är många som samarbetar för att skapa mer komplex programvara krävs att det finns tydliga avtalsrelationer med dessa.

I dag är det vanligt att det som ska deponeras ingår i system med kopplingar till annan mjukvara, inte sällan med öppen källkod inblandad. Tekniska uppfinningar av produkter kan innehålla egenutvecklad kod blandad med licensierad kod och öppen källkod. I sådana sammanhang kan krävas en gedigen genomlysning (rättighetsklarering) före deponering.

Depositionen

Ett depositionsavtal är ofta kopplat till ett licensavtal som reglerar detaljer kring vad som ska deponeras. Där kan finnas angivna utlämnandegrunder och annat som depositionsavtalet kan hänvisa till. Generellt brukar i licensavtalen anges att leverantören är skyldig att deponera och uppdatera den källkod och den dokumentation som behövs för att en normalt skicklig person ska kunna fortsätta använda mjukvaran.

Tidpunkten för depositionen bör särskilt övervägas när det gäller utvecklingsprojekt. Vanligtvis får depositionen anstå till dess leverans sker men andra gånger sker depositionen löpande under projektets gång.

Källkodsdeponering handlar delvis om en trygg förvaringstjänst, såsom hårddiskar, CD-skivor och USB-minnen som deponeras i säkerhetsskåp och bankvalv. I dag är det allt vanligare att depositioner sker on-line.

Lika viktigt som en säker förvaring är att syftet med deponeringen blir säkerställt.

För att skapa den avsedda tryggheten för licenstagaren krävs att det som deponeras (källkod och erforderlig dokumentation) är använd-

bart och hålls uppdaterat. Detta kontrolleras genom verifieringstjänster. Licenstagarens kompetens och förmåga att själv kunna använda en till denne utlämnad deposition bör beaktas i god tid. Vissa verifieringstjänster medför att extern kompetens finns säkerställd om ett utlämnade skulle bli aktuellt.

Några praktiska erfarenheter från utlämnande av depositioner

Leverantören brukar förpliktigas att hålla sin deposition uppdaterad. Därför är det vanligt att parterna inledningsvis planerar för många uppdateringar. Vanligtvis utmynnar det ändå i ett fåtal uppdateringar per år, av det skälet att många uppdateringar inte är affärs- eller verksamhetskritiska. Intressant är att när det väl sker ett utlämnande hörs kommentarer om att ytterligare uppdateringar hade varit värdefulla.

Verifieringar kan begränsas till att bekräfta vad som deponerats. Verifieringar kan också säkerställa användbarheten genom avancerade kontroller och dokumentering för att snabbt kunna komma igång efter ett utlämnande. Det blir naturligtvis mer kostsamt inledningsvis, men när det väl sker ett utlämnande konstaterar licenstagaren ofta att det hade varit klokt att välja en mer avancerad verifiering.

Utlämnandegrunder

Den ena sidan av deponering är att källkoden lämnas för deponering. Den andra sidan är att någon begär ut det som har deponerats.

Grunderna för ett utlämnande av depositioner bör ha fokus på leverantörens oförmåga eller ovilja att uppfylla sina avtalade förpliktelser. Ofta när det talas om deposition av källkod nämns konkurssituationer. Att enbart ange konkurs som ett skäl för utlämnande är olyckligt eftersom avtalets sakrättsliga verkan mot ett konkursbo kan ifrågasättas. Det intressanta är huruvida leverantören fullgör sina underhållsåtaganden eller inte. Görs inte det kan licenstagaren begränsa sin skada genom tillgång till depositionen. Ett utlämnande av depositionen innebär inte att de immateriella rättigheterna övergår till licenstagaren men i konkurssituationer händer att licenstagaren köper loss de immateriella rättigheterna från konkursboet.

Leverantör och kund har möjlighet att komma överens om mindre vanliga grunder för utlämnade, exempelvis uteblivna uppdateringar. Viktigt är att utlämnandegrunderna är tydligt angivna från början. Depositionsföretaget (depositarien) bör inte acceptera utlämnandegrunder som inte är objektivt fastställbara.

Om det uppkommer tvist mellan leverantör och kund bör depositionsföretaget inte vara den som avgör tvisten. Rollen som oberoende tredje part är att verkställa det beslut som fattas av domstol eller skiljemän alternativt följer av annan utlämnandegrund, exempelvis en av kunden ställd bankgaranti.

En vanlig missuppfattning är att det brådskar med ett utlämnande. Visserligen fungerar depositionen också som en back-up (säkerhetskopia) men det är oftast inte huvudsyftet. Uteblivna prestationer från leverantörens sida innebär normalt att programvaran fungerar allt sämre över tid, inte att den plötsligt blir obrukbar. Det innebär att ett utlämnade kan anstå till dess att parternas tvist avgjorts av domstol eller skiljemän. De gånger ett snabbt utlämnande ändå är av affärskritisk betydelse kan problemet lösas genom att kunden/licenstagaren ställer en bankgaranti på ett belopp som parterna angivit i depositionsavtalet.

Slutord

En av juridikens viktigaste uppgifter är att komplettera det avtalsparter inte kan reglera sinsemellan. En annan är att stimulera utveckling genom att till exempel ge incitament för innovation. Ett av de tydligaste områdena där dansen mellan juridik och praktik blir tydlig är just datorprogram. Avtalsparter kan inte sinsemellan skapa immaterialrättsliga ensamrätter som är verksamma mot tredje man, det behöver lagstiftaren göra.

Lagstiftningen inom immaterialrättens område utgör en grund som ofta kompletteras med egna avtalsrättsliga lösningar. Källkodsdeposition är ett exempel där juridik och avtalshantering kompletterar varandra och tillsammans levererar lösningar som kan tillgodose marknadens efterfrågan.

Christina Wainikka, är policyexpert för immaterialrätt vid Svenskt Näringsliv. Hon är även docent i civilrätt vid Stockholms universitet.

Tommy Svensson är vd på Deposit AB – Escrow Europe Scandinavia. Han har varit ordförande i Svenska föreningen för it & juridik samt styrelseledamot i Institutet för rättsinformatik, IRI.

Nye avgjørelser fra Datatilsynet om tilgangsstyring og logging i helsesektoren

Av Fride Hedin og Emilie Sverdrup

Innledning

Aktører som yter eller administrerer helsehjelp, behandler sensitive personopplysninger om pasienter og brukere i betydelig omfang. Virksomhetenes behandling av særlige kategorier av personopplysninger er en forutsetning for at disse aktørene skal kunne tilby nødvendige helsetjenester. Samtidig stiller GDPR og særlovgivningen strenge krav til personopplysningssikkerheten når helseaktørene behandler slike personopplysninger.

Datatilsynet har hittil i år truffet flere vedtak om brudd på GDPR og særlovgivningen som følge av manglende tilgangsstyring og logging i helsesektoren. Vedtakene illustrerer viktigheten av å implementere tilfredsstillende sikkerhetstiltak slik at det kun er ansatte med tjenstlig behov som gis tilgang til personopplysninger. I denne artikkelen ser vi nærmere på hvilke sikkerhetsmessige krav som gjelder ved behandling av helseopplysninger, i lys av de siste sentrale vedtakene fra Datatilsynet.

GDPR stiller strenge krav til personopplysningssikkerheten

GDPR artikkel 5(1)(f) oppstiller et prinsipp om sikring av integritet og konfidensialitet ved behandling av personopplysninger. Etter bestemmelsen er den behandlingsansvarlige ansvarlig for og skal kunne påvise at personopplysninger behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, ved bruk av egnede tekniske eller organisatoriske tiltak.

Fride Hedin

Emilie Sverdrup

Hvilke konkrete sikkerhetstiltak den behandlingsansvarlige må iverksette er nærmere beskrevet i GDPR artikkel 32. Den behandlingsansvarlige skal, idet det tas hensyn til en rekke opplistede faktorer som blant annet den tekniske utviklingen og behandlingens art og omfang, gjennomføre tiltak for å oppnå et sikkerhetsnivå som er *egnet* med hensyn til risikoen. Ved vurderingen av egnet sikkerhetsnivå, skal det særlig tas hensyn til risikoene forbundet med behandlingen, blant annet som følge av ikke-autorisert utlevering av eller tilgang til personopplysninger som behandles.

Siden helseopplysninger er å anse som en særlig kategori av personopplysninger etter GDPR artikkel 9 nr. 1, stilles det strengere krav til sikkerheten ved behandling av slike opplysninger enn ved behandling av alminnelige personopplysninger. Kravene skjerpes ytterligere dersom opplysningene knytter seg til barn, som har et særskilt krav på vern etter personvernregelverket.

GDPR artikkel 24 fastsetter den behandlingsansvarliges særskilte plikt til å gjennomføre egnede tekniske og organisatoriske tiltak. Dette omfatter etablering av egnede retningslinjer for vern av personopplysninger, dersom det står i et rimelig forhold til behandlingsaktivitetene.

Særlige krav til behandling av helseopplysninger i pasientjournalloven

Pasientjournalloven inneholder særskilte krav for behandling av helseopplysninger som er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til enkeltpersoner, og supplerer de generelle kravene til behandling av personopplysninger i GDPR. Datatilsynet fører tilsyn med overholdelsen av loven og tilhørende forskrifter, jf. pasientjournalloven § 26.

Etter pasientjournalloven § 22 om informasjonssikkerhet, skal den behandlingsansvarlige og databehandleren gjennomføre tekniske og

organisatoriske tiltak, i tråd med GDPR artikkel 32, for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Dette omfatter blant annet å sørge for tilgangsstyring, logging og etterfølgende kontroll. Videre oppstiller lovens § 23 krav til internkontroll i tråd med GDPR artikkel 24, for å sikre og påvise at behandlingen utføres i samsvar med gjeldende personvernlovgivning. Etter bestemmelsen skal den behandlingsansvarlige dokumentere tiltakene, og gjøre dokumentasjonen tilgjengelig for medarbeiderne hos den behandlingsansvarlige, hos databehandleren og for tilsynsmyndighetene.

Nye vedtak fra Datatilsynet om brudd på kravene til tilgangsstyring og logging

Datatilsynet fattet nylig vedtak mot St. Olavs hospital (sak 20/01813-4) og Høylandet kommune (sak 20/01879-7) for brudd på kravene til sikkerhet ved behandling av blant annet helseopplysninger. I begge sakene var helseopplysninger blitt tilgjengeliggjort for ansatte som ikke hadde tjenstlig behov for slik tilgang. Vedtakene bidrar til bedre forståelse av hvilke konkrete tiltak som må iverksettes for å oppfylle kravene til tilgangsstyring og logging etter gjeldende personvernregelverk.

I vedtaket mot St. Olavs hospital uttaler Datatilsynet at selv om opplysningene var lagret på et område det kreves noe kunnskap å finne frem til, forelå det like fullt en risiko for brudd på opplysningenes konfidensialitet og integritet. Risikoen knytter seg her til at ansatte uten tjenstlig behov kunne fått tilgang til et omfattende antall helseopplysninger om pasienter ved sykehuset.

Datatilsynet legger videre vekt på manglende logging av aktivitetene på de aktuelle fil-/mappeområdene. Dette gjør det umulig å avdekke om ansatte uten tjenstlig behov faktisk har benyttet seg av tilgangene, og gjør det vanskelig å bedømme konsekvensene av avviket for de berørte. Ifølge Datatilsynet øker manglende logging risikoen for at man mister oversikt over hvor personopplysningene befinner seg. Motsetningsvis vil innføring av et loggsystem gjøre det enklere å oppdage eventuelle avvik på et tidlig tidspunkt og kontrollere tilgangene.

Tilsynet fremhever også viktigheten av å ha på plass tilfredsstillende personvernrutiner. I saken mot Høylandet kommune uttales det at behandlingsansvarlig må ha etablert rutiner som ivaretar kravene til personvern og informasjonssikkerhet, inkludert prinsipper for skjerming og tilgangsstyring. Det presiseres at det er et ledelsesansvar at rutiner er etablert og fungerer som forutsatt.

I den samlede vurderingen av avvikene legger Datatilsynet vekt på en rekke momenter, herunder varigheten av avvikene, antall registrerte som er berørt, antall ansatte som har hatt urettmessig tilgang til opplysningene, samt hvilke tiltak som er iverksatt for å rette avvikene.

Etter at avvikene ble oppdaget, hadde St. Olavs hospital iverksatt flere tiltak for å rette opp i avvikene som i) gjennomgang og kontroll av tilgangsstyringen, ii) etablering av ny passordrutine og begrensning av tillatt antall mislykkede påloggingsforsøk, iii) implementering av system for overvåking og logganalyse, og iv) utarbeidelse av behandlingsprotokoll i samsvar med GDPR artikkel 30. Datatilsynet ser positivt på dette, men det endrer likevel ikke konklusjonen om at sykehuset hadde brutt grunnleggende krav til personopplysningssikkerhet. Tiltakene som ble implementert av St. Olavs hospital er tiltak som enhver helseaktør burde sørge for å ha på plass.

Vurderingen av om overtredelsesgebyr skal ilegges og dets størrelse

Ved vurderingen av om overtredelsesgebyr skal ilegges, og ved utmålingen, ser Datatilsynet hen til flere av de samme momentene som nevnt ovenfor, herunder varigheten av avvikene og hvilke tiltak som er iverksatt. I tillegg legges det blant annet vekt på karakteren og alvorlighetsgraden av overtredelsen, samt hvilke kategorier av personopplysninger som er berørt.

Felles for begge de nevnte vedtakene er at de omhandler svært sensitive personopplysninger. Saken mot St. Olavs hospital omfattet også opplysninger knyttet til barne- og ungdomspsykiatrien. Ifølge Datatilsynet øker dette alvorlighetsgraden av lovbruddet.

Videre ble helseopplysninger om et stort eller ukjent antall personer berørt av avvikene, opplysningene hadde vært tilgjengelige for et stort eller ukjent antall ansatte uten tjenstlig behov, og avvikene hadde vedvart over lengre tid uten at det ble fanget opp gjennom interne rutiner.

Hvorvidt adekvate tiltak ble iverksatt for å forhindre videre lovbrudd etter at avvikene ble oppdaget, er også et moment som vektlegges i vurderingen av gebyret størrelse. I motsetning til St. Olavs hospital, iverksatte Høylandet kommune innledningsvis ingen slike tiltak, utover å oppfordre de ansatte til ikke å åpne de aktuelle filene. Ifølge Datatilsynets uttalelser er dette ikke tilstrekkelig, og tilsier at det har vært grunnleggende mangler ved rutinene for skjerming av helseopplysninger og håndtering av avvik.

Basert på en konkret helhetsvurdering, ble overtredelsesgebyrene satt til 400 000 kroner og 750 000 kroner i vedtakene mot henholdsvis Høylandet kommune og St. Olavs hospital. Det er i denne sammenheng verdt å merke seg at lovbruddene dels fant sted før personopplysningsloven av 2018 og GDPR trådte i kraft, noe Datatilsynet har sett hen til ved fastsettelsen av gebyrenes størrelse.

Fride Hedin er advokatfullmektig i Advokatfirmaet Wiersholm.

Emilie Sverdrup er advokatfullmektig i Advokatfirmaet Wiersholm.

Halvor Manshaus, *leder IP/Media-gruppen i Advokatfirmaet Schjødt AS, Oslo og fast spaltist i Lov&Data.*
Jenny O. Nondal, *advokatfullmektig/Associate i Advokatfirmaet Schjødt AS.*

Rogstad-saken:
Bruk av bilde uten samtykke

Borgarting lagmannsrett avsa 22. september 2021 dom i saken mellom advokatfirmaet Rogstad og VG vedrørende bruk av fotografier hentet fra to ulike nettsteder (LB-2020-164203). Det sentrale spørsmålet i saken var hvorvidt bruken av fotografiene i nyhetssakene hos VG utgjorde et urettmessig inngrep i åndsverkslovens bestemmelser om vern av bildene.

Lagmannsretten innleder avgjørelsen med en gjennomgang av sakens bakgrunn. Tidlig i 2020 hadde VG publisert flere kritiske nyhetssaker om advokatfirmaet Rogstad. For å illustrere reportasjene publiserte VG fotografier hentet fra Rogstads nettside og en Facebook-side der firmaets daglige leder poserte bak en Lamborghini. I april 2020 saksøkte Rogstad VG og en journalist og krevde erstatning for brudd på opphavsretten til de aktuelle fotografiene. Det ble også krevd forbud mot videre spredning av fotografiene.

VG og journalisten fikk medhold i Oslo tingrett og ble frikjent for kravet (TOSLO-2020-64392). Rogstad anket dommen videre til lagmannsretten der det ble en ny full hovedforhandling. Spørsmålet for lagmannsretten var om VG kunne offentliggjøre fotografiene uten samtykke fra rettighetshaver, og om dette i tilfelle utløste et krav på vederlag eller erstatning.

Offentlig gjengivelse av opphavsrettsbeskyttede verk og fotografier krever som hovedregel samtykke fra rettighetshaver som fastsatt i åndsverkloven § 3 og § 23.

Det er imidlertid oppstilt flere unntak fra hovedregelen om samtykke til offentliggjøring. Åndsverksloven § 1 slår i litra a) først fast at formålet med loven er å gi rettigheter til den som skaper, fremfører eller investerer i åndsverk eller nærstående rettigheter. Begrepet nærstående rettigheter er utdypet nærmere i lovens kapittel 2, og i § 23 oppstilles en enerett for fotografier uavhengig av om det foreligger verkshøyde. I § 1 litra b heter det det videre at et ytterligere formål med loven er å avgrense nettopp rettighetene beskrevet under litra a, slik at det oppstår en rimelig balanse mellom hensynet til rettighetshaveren og det som fremstår som en rimelig utnyttelse ut i fra samfunnsmessige hensyn. Et konkret angitt eksempel på interesser som kan avgrense åndsrettighetene er informasjons- og ytringsfriheten.

For å klargjøre grenseskillet mellom åndsrett og informasjons- og ytringsfriheten er det inntatt enkelte særbestemmelser i åndsverksloven. For denne saken er det relevant å vise til at Åndsverkloven § 29 åpner for sitater fra offentliggjorte verk og fotografier uten samtykke fra rettighetshaver og uten krav på kompensasjon. Videre tillater § 36 gjengivelse av offentlige verk og fotografier av media i forbindelse med rapportering av en *«dagshending»*, uten samtykke fra rettighetshaver, men slik at det i disse tilfelle normalt skal ytes vederlag.

Lagmannsretten måtte følgelig vurdere om § 29 eller § 36 skulle anvendes, altså om den aktuelle bruken utløste et krav på vederlag eller ikke.

Retten fant at fotografiene ikke hadde verkshøyde etter åndsverksloven § 2, men at disse nøt vern som fotografiske verk etter § 23. Både åndsverksloven § 29 og § 36 får anvendelse også på fotografiske verk. Det hadde altså ingen praktisk betydning i denne saken om fotografiene ble ansett å være åndsverk eller ikke. Kanskje dette forklarer hvorfor lagmannsretten bare kort konstaterer at portrettfotografier ikke har verkshøyde i et tilfelle der det er snakk om masseproduserte bilder til markedsføring. Det kan diskuteres om rettens drøftelse utgjør en fullverdig analyse opp mot terskel for verkshøyde, men spørsmålet var altså ikke avgjørende i denne saken. Selv om bildene hadde

blitt vurdert som åndsverk antas de å ha ville ligget i det nedre sjiktet målt opp mot verkshøydekravet.

Retten konkluderer i dommen med at VGs bruk av fotografiene var utenfor rammen av § 36, ettersom VGs nyhetssaker ikke knyttet seg til en *«dagshending»* . Retten uttalte at selv om rekkevidden av §§ 29 og 36 er overlappende, er bestemmelsene uavhengige av hverandre. Vederlagsregelen i § 36 begrenser derfor ikke anvendelsen av sitatretten i § 29. Retten fant at VGs bruk av fotografiene var tillatt etter § 29. Som omtalt ovenfor krever ikke § 29 at det ytes vederlag for bruken. Det forelå følgelig ikke noe grunnlag for å tilkjenne erstatning til Rogstad.

Det er flere sentrale punkter fra lagmannsrettens avgjørelse som er relevante for medienes rett til å publisere fotografier i nyhetssaker uten samtykke fra eller kompensasjon til rettighetshaver.

For det første slo lagmannsretten fast prinsippet om at opphavsrettslovgivningen ikke skal begrense den grunnleggende retten til ytringsfrihet etter Grunnloven § 100 og Den europeiske menneskerettskonvensjon (EMK) art. 10. Dette er også klart fastslått i forarbeidene til åndsverkloven av 2018, der det er forutsatt at rettsanvenderen må gjøre en konkret rettsstridsvurdering opp mot våre konvensjonsforpliktelser og EMK artikkel 10. Retten anvendte dette prinsippet ved tolkningen av unntaket, som er angitt i § 29, fra rettighetshavernes enerett til fotografiske verk i § 23. Lagmannsrettens avgjørelse innebærer at retten til å sitere et fotografisk verk eller fotografi etter § 29, og omfanget av andre unntak fra opphavsrettens eneretter, må fastlegges i tråd med ytrings- og informasjonsfriheten.

For det andre stadfestet dommen at retten til å sitere et fotografisk verk eller fotografi i henhold til § 29 kan omfatte hele fotografiet, ikke bare utsnitt fra dette. Hvor mye

som kan siteres vil måtte avgjøres etter en konkret vurdering i den enkelte sak.

For det tredje er § 29 om sitater av fotografiske verk eller fotografier, og § 36 for dagshendinger, uavhengige og selvstendige avgrensninger av rettighetshavernes enerett etter § 3 og § 23. Unntaket i § 36 er ikke en spesialbestemmelse til § 29 og begrenser derfor ikke rekkevidden av § 29. Dette innebærer at selv om § 36 ikke fikk anvendelse i denne saken var det anledning til å gå videre og vurdere den aktuelle bruken opp mot § 29.

For det fjerde drøftet lagmannsretten kravet til dagshending i § 36. Det kan reises spørsmål ved om lagmannsretten i denne saken vurderte innholdet i dagshendingsunntaket for strengt når bildebruken ble ansett å falle utenfor § 36. Lagmannsretten la tilsynelatende stor vekt på uttalelser fra forarbeidene knyttet til hvorvidt det er tid i en dagshendingssituasjon til å innhente et samtykke, og uttaler: *«I saken her er det neppe tale om en «dagshending». Det er tale om et relativt langvarig journalistisk arbeid, som pågikk over måneder før første publisering. Hensynet til å kunne bruke bildene selv om det ikke er tid til å innhente forhåndssamtykke har liten relevans i et slikt tidsperspektiv. Det som er beskrevet i reportasjene har etter lagmannsrettens syn en klar nyhetsverdi, og langt over det* «minstemål av generell nyhetsverdi» som Høyesterett *savnet i Rt-1995-1948. Dagsaktualiteten og det tidshensyn som begrunner bestemmelsen i § 36 er likevel ikke til stede.»*

I forarbeidene (lovproposisjonen til åndsverksloven Prop. 104 L 2016-17 punkt 5.11.5) drøftes vilkåret om dagshending. Det vises til at innholdet i begrepet er forankret i konvensjoner og direkte i opphavsrettsdirektivet. Det konkluderes i proposisjonen med at *«Vilkåret inne-*

bærer i henhold til norsk rettspraksis at det kreves et visst minstemål av generell nyhetsverdi, jf. Rt. 1995 s. 1948 (Diana Ross).» (vår utheving). Høyesterettsavgjørelsen det er vist til omhandlet spørsmål om nettopp dagshending, der kravet til aktualitet ikke fremstår som spesielt høyt. Spørsmålet målt opp mot EMK artikkel 10 er om det foreligger tilstrekkelig aktuell og allmenn interesse i den konkrete sak, og det er da relevant å trekke inn kilder fra andre rettsområder som berører aktualitetskravet.
I NOU 2019:10 «Åpenhet i grenseland» som gjelder bruk av bilder og opptak i ulike omsorgstjenester, diskuteres forholdet mellom ytringsfriheten og kravet til samtykke for bildepublisering etter åndsverksloven § 104 litra a under punkt 1.3.2.1 Publisering kan etter denne bestemmelsen skje uten samtykke fra avbildede der avbildningen har aktuell og allmenn interesse. I vurderingen opp mot EMK artikkel 10 viser NOU 2019:10 til det samme sitatet fra Diana Ross-saken Rt-1995 s. 1948, og fremhever deretter at det i rettspraksis er trukket opp flere faktorer som skal inngå i vurderingen:

«Den sentrale vurderingen er altså om de offentliggjorte personopplysningene har aktuell og allmenn interesse. Aktualitetskravet innebærer i henhold til norsk rettspraksis «at det kreves et visst minstemål av generell nyhetsverdi.» Det finnes heller ingen entydig definisjon av «allmenn interesse». En viss generell interesse må foreligge, men det er ingen klare avgrensninger i så måte. Det kan for eksempel være ulik vurdering dersom en sak har en geografisk avgrenset interesse, eller på samme måte innen et fagfelt eller kollegium. Vurderingen av om allmenn interesse foreligger, og ikke minst i hvilken grad en eventuell slik interesse kan trumfe en persons rett til å bestemme over eget bilde og/eller privatliv, bygger på en avveining av flere faktorer som er stilt opp i norsk og internasjonal rettspraksis.

Utgangspunktet for avveiningen er at noe informasjon kan være viktig for at samfunnet skal være løpende informert om saker av relevans og interesse, og sånn sett bidra til et velfungerende demokrati. Slik informasjonsflyt har tradisjonelt vært et sentralt medieoppdrag.*»*

I den videre gjennomgang pekes det på flere relevante faktorer, slik som pressens særlige rolle som formidler av informasjon, graden av allmenn interesse, subjektive forhold, grad av aktsomhet osv. Lagmannsretten drøftet flere av disse faktorene i forbindelse med andre spørsmål i saken, men trakk ikke dette inn i vurderingen av spørsmålet om det foreligger en dagshending på samme måte som i forarbeidene. Vår innvending er at lovens system krever en *relativisert vurdering*, der de ulike faktorene veies opp mot hverandre. Et helt sentralt element i denne vurderingen vil være graden av allmenn interesse. Der det foreligger sterk allmenn interesse står man i kjernen av informasjons- og ytringsfriheten, og det må kreves mer av andre faktorer som taler for å begrense denne friheten. Det er da naturlig at domstolen må vurdere hvordan tidselementet skal inngå i denne vurderingen, og om det er rimelig å forvente at media skal vente med å publisere saken i påvente av klarering av bruk av de aktuelle bildene. Slik saken lå an var dette et underordnet spørsmål, all den tid sitatretten uansett ga grunnlag for bruk av bildene uten vederlag. Hadde dette ikke vært tilfelle ville det vært av større betydning hvordan lagmannsretten så på spørsmålet om dagshending. Lagmannsrettens betraktning om at oppslagenes nyhetsverdi langt overskredet minstemålet er det uansett enkelt å tiltre.

Avgjørelsen er ikke rettskraftig og er påanket. Saken vil kunne ha betydning for ulike former for publisering av bildemateriale uten samtykke der det foreligger offentlig interesse, slik som her hvor det dreide seg om gravejournalistikk og undersøkende journalistikk. Anvendelse av sitatretten i § 29 krever altså at saken har tilstrekkelig grad av offentlig interesse, og ellers at det siteres i samsvar med god skikk og bare så langt formålet tilsier det.

Det informeres for ordens skyld om at artikkelforfatterne jobber i Advokatfirmaet Schjødt og at vår kollega advokat Halvard Helle førte saken for VG i tingretten og lagmannsretten.

Litteratur

«Selvbetjent rettshjelp – En undersøkelse av digitale, selvbetjente rettshjelpsløsninger».

Sunniva Slotten og Dag Wiese Schartum.

Oslo: Universitetet i Oslo, Juridisk fakultet 2021, 3/2021. ISSN 2703-8777 Complex

https://www.jus.uio.no/ifp/forskning/om/publikasjoner/complex/2021/2021-03.html

«Rettslige begrensninger for forvaltningens bruk av data til trening av maskinlæringsalgoritmer – Spesielt om personvernrettslige og forvaltningsrettslige rammer».

Julie Lossius Husum.

Oslo: Universitetet i Oslo, Juridisk fakultet 2021, 4/2021. ISSN 2703-8777 Complex

https://www.jus.uio.no/ifp/forskning/om/publikasjoner/complex/2021/2021-04.html

«Det er på tide å pensjonere gjeldsbrevloven»

Olav Torvund.

i Lov og Rett07 / 2021 (Volum 60), artikkel 5 av 7.
https://www.idunn.no/lor/2021/07/det_er_paa_tide_aa_pensjonere_gjeldsbrevloven

«Journalisters rett til å bruke bilder og videoer hentet fra internett En analyse av dagshendingsreglene og sitatretten i åndsverkloven»

Ellen Lexerød Hovlid.
i Lov og Rett07 / 2021 (Volum 60), artikkel 4 av 7.

Sammendrag: Bilder og video er sentrale virkemidler i journalistikken. Internett og sosiale medier har gitt journalister vesentlig større tilgang på bilder og videoer enn de hadde tidligere. Denne artikkelen tar for seg de opphavsrettslige reglene for når journalister kan bruke bilder og videoer de finner på nettet. Utgangspunktet er at journalister må inngå avtale med den som har rettighetene til bildet eller videoen. Noen ganger kan imidlertid journalister bruke materialet uten å spørre om lov. Det er særlig dagshendingsreglene og sitatretten som regulerer dette, og i artikkelen drøftes disse reglene. Konklusjonen er at journalister har en nokså vid rett til å benytte andres bilder og videoer som ledd i nyhetsdekning. I de fleste tilfeller har imidlertid rettighetshaveren krav på vederlag for bruken.

https://www.idunn.no/lor/2021/07/journalisters_rett_til_aa_bruke_bilder_og_videoer_hentet_fra

Gorrissen Federspiel

Tue Goldschmieding

Ny lov om beskyttelse af whistleblowere

Folketinget vedtog den 24. juni 2021 lov nr. 1436 af 29. juni 2021. Loven træder i kraft den 17. december 2021. Formålet med loven er at garantere en bedre beskyttelse af whistleblowere. Dette er gjort ved at sikre kanaler til at indberette lovovertrædelser i den offentlige samt private sektor. Loven implementerer Europa-Parlamentets og Rådets direktiv (EU) 2019/1937 af 23. oktober 2019 om beskyttelse af personer, der indberetter overtrædelser af EU-retten.

Loven pålægger alle virksomheder i den offentlige og private sektor med 50 eller flere ansatte at fastsætte en intern whistleblowerordning, der skal muliggøre en skriftlig eller mundtlig indberetning. Private arbejdsgivere med 250 eller flere ansatte og hele den offentlige sektor skal etablere en offentlig whistleblowerordning senest samtidig med lovens ikrafttræden den 17. december 2021. Private arbejdsgivere, der har mellem 50 og 249 ansatte, skal først realisere kravet senest den 17. december 2023. Efter den nye lov om beskyttelse af whistleblowere § 9, stk. 3, er der mulighed for at etablere en koncernfælles whistleblowerordning.

Loven finder anvendelse på indberetninger om overtrædelse af en række specifikke områder inden for EU-retten samt alvorlige lovovertrædelser eller øvrige alvorlige forhold. Med dette menes, at loven også finder anvendelse på alvorlige overtrædelser i dansk ret, der går videre end direktivet. Loven gør det obligatorisk for offentlige og private arbejdsgivere med mere end 50 ansatte at etablere en whistleblowerordning. Den nye lov indeholder et forbud mod enhver form for repressalier over for whistlebloweren.

Læs loven her:
https://www.retsinformation.dk/eli/lta/2021/1436

Datatilsynet udtalte alvorlig kritik af forsikringsselskabs behandling af personoplysninger i forbindelse med overvågning borger

Det danske Datatilsyn traf den 6. september 2021 afgørelse i en sag med journalnummer 2020-31-3586 vedrørende et forsikringsselskabs behandling af personoplysninger. Datatilsynet udtalte alvorlig kritik af, at et forsikringsselskabs behandling af personoplysninger ikke var sket i overensstemmelse med reglerne i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»databeskyttelsesforordningen«) artikel 15, jf. lov nr. 502 af 23. maj 2018 (»den danske databeskyttelseslov«) § 22.

Et advokatselskab havde, på vegne af en borger, anmodet om indsigt i oplysninger, som et forsikringsselskab havde indsamlet om den pågældende i forbindelse med en overvågning af borgeren, efter at denne havde søgt erstatning for erhvervsevnetab efter at have været involveret i en trafikulykke. Forsikringsselskabet anmeldte borgeren til politiet på baggrund af overvågningen.

Datatilsynet fandt, at forsikringsselskabet ikke havde påvist hensyn af en sådan afgørende karakter, at borgerens ret til indsigt burde vige herfor. Personoplysningerne, der var indsamlet under overvågningen, kunne ikke medføre nærliggende fare for, at private interesser ville lide skade af væsentlig betydning. Endvidere vurderede Datatilsynet, at oplysningerne i den konkrete sag ikke udgjorde et så afgørende hensyn til forsikringsselskabets interesser, at oplysningerne kunne undtages fra retten til indsigt. Dette var tilfældet, selvom borgeren kunne benytte overvågningsmaterialet til skade for forsikringsselskabet i forbindelse med en eventuel retssag. Herudover fandt Datatilsynet, at forsikringsselskabet ikke kunne nægte udlevering af overvågningsmaterialet under henvisning til hensyn til offentlige interesser, herunder politiets efterforskning. Datatilsynet lagde vægt på, at politianmeldelse allerede var indgivet, og at borgeren kendte til efterforskningen.

Datatilsynet udtalte på baggrund af ovenstående, alvorlig kritik af, at forsikringsselskabets håndtering af klagers anmodning ikke var sket i overensstemmelse med databeskyttelsesforordningens artikel 15, jf. den danske databeskyttelseslov § 22. Datatilsynet noterede sig, at forsikringsselskabet efterfølgende udleverede overvågningsmaterialet.

Læs afgørelsen her:
https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/sep/afgoerelse-vedroerende-forsikringsselskabets-behandling-af-personoplysninger

Datatilsynet udtalte alvorlig kritik af Rigspolitiets behandling af teledataoplysninger

Det danske Datatilsyn traf den 19. juli 2021 afgørelse i en sag med journalnummer 2019-819-0003 vedrørende Rigspolitiets behandling af teleoplysninger. Datatilsynet udtalte alvorlig kritik af, at Rigspolitiets behandling af personoplysninger ikke var sket i overensstemmelse med lov nr. 410 af 27. april 2017 (»den danske retshåndhævelseslov«), og meddelte desuden Rigspolitiet påbud om at slette personoplysninger, der ikke opfyldte Rigspolitiets telecenters egne retningslinjer.

Datatilsynet fik på baggrund af presseomtale kendskab til, at Rigspolitiets IT-system ikke til enhver tid viste retvisende resultater af fysiske personers geografiske placering. Fejlene var begrundet i konverteringsfejl i rådata, mangelfuld rådata om kommunikation ved nyere tjenester og fejl i konvertering af mastekoordinater. Fejlene medførte, at ufuldstændig og ikke-opdateret data blev videresendt.

Datatilsynet vurderede, at Rigspolitiets behandling af personoplysninger vedrørte retten til retfærdig og offentlig rettergang efter Den Europæiske Menneskerettighedskonventions artikel 6, stk. 1, hvor det er afgørende, at der kan stoles på de oplysninger, som politiet behandler og videregiver til fremlæggelse som bevismateriale i retten. I denne forbindelse måtte der tillige stilles høje krav til databeskyttelse. Det havde Rigspolitiet ikke efterlevet, idet der ikke var truffet passende sikkerhedsforanstaltninger, særligt henset til at fejlene havde stået på over en længere årrække og vedrørte et større antal sager. På baggrund af en samlet vurdering udtalte Datatilsynet derfor alvorlig kritik over, at behandlingen af personoplysninger ikke var sket i overensstemmelse med den danske retshåndhævelseslov § 27, § 4, stk. 4-6 og § 4, stk. 8, jf. stk. 7.

Læs afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/jul/afgoerelse-vedroerende-rigspolitiets-behandling-af-teledata-oplysninger

Alvorlig kritik af Helsingør Kommune i Chromebook-sag

Det danske Datatilsyn traf den 10. september 2021 afgørelse i sag med journalnummer 2020-431-0061 og udtalte alvorlig kritik af Helsingør Kommune for at bryde personsikkerheden i forbindelse med skoleelevers adgang til G-Suite (nu Google Workspace), som er en pakke af værktøjer til cloudcomputing, produktivitet og samarbejde.Cloudcomputing er levering af forskellige tjenester til mange brugere via internettet,

Helsingør Kommune anmeldte den 29. januar 2020 et brud på persondatasikkerheden til Datatilsynet. Det fremgik af anmeldelsen, at Kommunen i overensstemmelse med sin myndighed havde udleveret Chromebooks til skoleelever. I denne forbindelse blev der oprettet en adgang til Google G-Suite, hvor der skulle oprettes en Google-konto til hver elev. Denne Google-konto blev oprettet med elevernes fulde navn, der, i forbindelse med en ændring i brugerbetingelserne, havde været tilgængeligt for andre Google-produkter, herunder Youtube. Såfremt eleverne anvendte YouTube på deres Chromebook, fik de således automatisk adgang med deres skolekonto, hvor deres fulde navn, skole og klasse blev vist. Dette var Kommunen ikke vidende om.

Skolekontoen kunne oprettes manuelt, men kunne også oprettes gennem skolernes administrative system således, at for- og efternavn, skole og klassetrin blev overført. Elever med beskyttede navne- og adresseoplysninger kunne oprettes med et alias og dermed blive anonymiseret. Der var dog i indeværende sag tilfælde, hvor elevers fulde navn var anført i stedet for et alias. Datatilsynet vurderede på denne baggrund, at Kommunen havde overtrådt Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»databeskyttelsesforordningen«) artikel 4, nr. 12 om brud på persondatasikkerheden.

Det blev oplyst i sagen, at Kommunen ikke foretog en risikovurdering af brugen af tillægsprogrammerne, herunder YouTube, da det ikke var meningen, at eleverne skulle anvende programmerne. Kommunen overtrådte dermed databeskyttelsesforordningens artikel 5, stk. 1, litra c. Kommunen har senere lukket for adgangen til YouTube. Idet Kommunen endvidere ikke havde foretaget en konsekvensanalyse af, hvad ændringen i Googles brugerbetingelser kunne betyde for eleverne, havde Kommunen tillige overtrådt databeskyttelsesforordningens artikel 35 om konsekvensanalyse.

Datatilsynet fandt, at Helsingør Kommune ikke kunne påvise overholdelsen af databeskyttelsesforordningens artikel 5, stk. 1, litra f om personoplysninger. Datatilsynet lagde vægt på, at Kommunen ikke kunne påvise, hvilken konfiguration der skete og dermed påvise, at der var tilstrækkelig sikkerhed med behandling af oplysningerne.

På baggrund af ovenstående samt det, at Kommunen ikke havde foretaget tilstrækkelig sikring mod uautoriseret brug af computerne, vurderede Datatilsynet, at Kommunen ikke har truffet passende organisatoriske og tekniske foranstaltninger der passede til det sikkerhedsniveau, der var ved Kommunens behandling af personoplysninger jf. databeskyttelsesforordningens artikel 32, stk. 1.

Endvidere fandt Datatilsynet, at Kommunen ikke levede op til kravene i databeskyttelsesforordningens artikel 33, stk. 1, idet Kommunen ikke anmeldte bruddet på persondatasikkerheden til Datatilsynet.

Datatilsynet meddelte Kommunen et påbud om at bringe brugen

af Chromebooks i overensstemmelse med forordningen jf. artikel 58, stk. 2, litra d: Kommunen skal inden den 1. november 2021 foretage en risikovurdering og evt. en konsekvensanalyse. Hvis risikovurderingen viser en høj risiko, vil Datatilsynet meddele Kommunen en midlertidig begrænsning i behandlingerne således, at Kommunen ikke må foretage behandlinger, der indebærer en høj risiko, før risikoen er nedbragt. Endvidere meddelte Datatilsynet en advarsel om brugen af tillægsprogrammer, og udtalte til sidst alvorlig kritik af Helsingør Kommunes behandling af personoplysningerne.

Læs afgørelsen her:
https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/sep/afgoerelse-vedroerende-brud-paa-persondatasikkerheden

Region Midtjylland indstillet til bøde

Det danske Datatilsyn oplyste i en pressemeddelelse af 8. september 2021, at Datatilsynet havde politianmeldt Region Midtjylland, da Datatilsynet fandt, at Region Midtjylland ikke havde etableret tilstrækkelig adgangsbegrænsning til et arkiv med patientjournaler.

Datatilsynet modtog den 12. juni 2020 en anmeldelse fra Region Midtjylland om brud på persondatasikkerheden i et livstilscenter, der har fokus på behandling af folk med livstilssygdomme som diabetes og overvægt. Det fremgik af anmeldelsen, at alle patienter og medarbejdere på livstilscenteret ved anvendelse af et adgangskort havde haft adgang til et arkiv med op mod 100.000 fysiske patientjournaler. Forbipasserende havde også kunnet kigge ind på omslagene af journalerne gennem et vindue til arkivet, hvor bl.a. patienters CPR-numre og navne var synlige. Under behandlingen af sagen oplyste Region Midtjylland, at patienter og medarbejdere havde haft adgang til arkivet siden 2016, og at der ikke havde været periodevis kontrol af, hvem der havde adgang til arkivet.

Datatilsynet fandt, at Region Midtjylland ikke havde etableret de fornødne sikkerhedsforanstaltninger. Endvidere fandt Datatilsynet, at bruddet havde været af en sådan størrelse, at der i overensstemmelse med Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 83, stk. 2 om administrative bøder, skulle pålægges Region Midtjylland en bøde på 400.000 kr., hvorefter Datatilsynet anmeldte regionen til politiet.

Læs pressemeddelelsen her:
https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/sep/region-midtjylland-indstillet-til-boede

Medicals Nordic I/S indstillet til bøde

Det danske Datatilsyn oplyste i en pressemeddelelse den 9. juli 2021, at Datatilsynet har politianmeldt Charlottenlund Lægehus Medicals Nordic I/S (»Medicals Nordic«) for i forbindelse med COVID-19-tests at have behandlet fortrolige oplysninger og helbredsoplysninger om borgere, uden at Medicals Nordic havde etableret den fornødne sikkerhed omkring behandlingen af oplysningerne.

Virksomheden brugte applikationen WhatsApp, som er en kommunikationstjeneste, til transmission af borgernes fortrolige oplysninger, og det foregik via medarbejdernes privattelefoner. Hvert af Medicals Nordics fire testcentre oprettede en WhatsApp-gruppe, hvor alle medarbejdere i det pågældende telt blev tilføjet. Hver medarbejder modtog alle de beskeder, som teltets andre medarbejdere transmitterede. Det var Datatilsynets vurdering, at medarbejdere, der ikke havde et arbejdsbetinget behov for at behandle oplysninger, alligevel modtog borgernes oplysninger. Yderligere blev medarbejdere, der ikke længere var ansat, ikke fjernet fra grupperne, og modtog derfor stadig oplysningerne. Datatilsynet fandt også, at overtrædelserne i flere tilfælde var sket forsætligt.

På den baggrund indstillede Datatilsynet Medicals Nordic til en bøde på 600.000 kr.

Læs pressemeddelelsen her:
https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/jul/medicals-nordic-is-indstillet-til-boede

Datatilsynets tilsyn med informationssikkerheden hos 30 organisationer

Det danske Datatilsyn iværksatte i løbet af sommeren 2021 en række tilsyn hos henholdsvis 9 hoteller, 10 forsikringsselskaber og 11 kommuner hvortil der blev udsendt identiske spørgeskemaer, som organisationerne skulle tage stilling til. Der var svarfrist den 10. september 2021. De udsendte spørgsmål omhandlede hovedsageligt, hvilke tiltag organisationerne havde foretaget for at sikre informationssikkerheden. Datatilsynets forventning med spørgeskemaundersøgelsen var, at besvarelserne ville afspejle det databeskyttelsesniveau, som de forskellige organisationer havde vurderet passende til at imødegå de risici, som organisationernes behandling af data udgjorde for de registrerede. Der blev således stillet spørgsmål til den overordnede organisering, herunder medarbejdernes adgang til oplysninger, interne politikker, netværkssikkerhed, backup og håndteringen af brud på persondatasikkerheden.

Tilsynet skal give Datatilsynet mulighed for at foretage en individuel vurdering af en organisations modenhed på databeskyttelsesområdet. Datatilsynet skal desuden vurdere, om de enkelte tilsyn blot kan afsluttes, eller om der skal varsles egentlige tilsynsbesøg. Datatilsynet vil sammenholde besvarelserne inden for samme branche og på tværs af brancherne for at vurdere det generelle niveau af datasikkerhed.

Læs spørgsmålene her:
https://www.datatilsynet.dk/Media/637655638046113311/Bilag%202%20-%20Sp%C3%B8rgsm%C3%A5l%20med%20hj%C3%A6lpetekster.pdf

Læs vejledningen til besvarelse af spørgeskemaundersøgelsen her:
https://www.datatilsynet.dk/Media/637650628087681525/Bilag%201%20Vejledning%20til%20besvarelse%20af%20sp%C3%B8rgeskemaunders%C3%B8gelse.pdf

EU-kommissionen anerkender Storbritannien som sikkert tredjeland

EU-Kommissionen anerkendte den 28. juni 2021 ved en tilstrækkelighedsafgørelse Storbritannien som et sikkert tredjeland i relation til Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»databeskyttelsesforordningen«).

Afgørelsen betyder, at personoplysninger nu frit kan overføres til Storbritannien uden et overførselsgrundlag. Det skyldes, at personoplysningerne er underlagt et i det væsentlige tilsvarende beskyttelsesniveau i Storbritannien som garanteret under EU-retten, da Storbritanniens behandling af personoplysninger er baseret på de samme regler og principper som gjaldt i Storbritannien, før de forlod EU. Storbritannien skal stadig overholde Databeskyttelsesforordningens bestemmelser. Andre lande, der også er godkendt, er blandt andre Argentina, Israel, Japan, New Zealand og Uruguay. Af stor praktisk betydning er hverken USA, Kina eller Indien godkendt.

Som noget nyt indeholdte denne tilstrækkelighedsafgørelse en solnedgangsklausul, der betyder, at afgørelsen automatisk udløber efter 4 år og kun kan blive fornyet, hvis Storbritannien fortsat opretholder det fornødne databeskyttelsesniveau. Klausulen blev indsat i tilfælde af fremtidige uoverensstemmelser.

EU-Kommissionen udstedte samtidig en tilstrækkelighedsafgørelse om Storbritannien og direktiv 2016/680/EU af 27. april 2016 (»retshåndhævelsesdirektivet«).

Læs nyheden her:
https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183

Ny vejledning med retningslinjer for stemmestyrede assistenter

Det Europæiske Databeskyttelsesråd (»EDPB«) vedtog den 7. juli en vejledning med retningslinjer for stemmestyrede assistenter.

Stemmestyrede assistenter (virtual voice assistants) er den funktionalitet, hvor stemmekommandoer bruges til at betjene forbrugerelektronik. De senere år har stemmestyrede assistenter fundet vej til flere og flere elektroniske produkter (smartphones, smart TV's osv.).

Der knytter sig væsentlige databeskyttelsesretlige overvejelser til denne teknologi. Dette er blandt andet i forhold til opbevaring af data, de registreredes rettigheder, brugen af kunstig intelligens og behandlingsgrundlag.

Vejledningen retter sig især mod professionelle aktører og er en god, teknisk gennemgang af de databeskyttelsesretlige regler og teknologierne. Den vejleder blandt andet om, hvordan de dataansvarlige stadig skal oplyse brugerne i henhold til Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»databeskyttelsesforordningen«). Her foreslår vejledningen, at udbyderne af stemmestyrede assistenter udvikler et stemmebaseret interface, der giver den påkrævede information til brugeren.

Derudover giver vejledningen retningslinjer om, hvordan udbyderne bør forholde sig til antallet af registrerede til deres tjenesteydelser. På nuværende tidspunkt kræver alle stemmestyrede assistenter, at mindst én bruger registreres i tjenesteydelsen. Her bør udbyderne overveje nødvendigheden af at have en registreret bruger for hver af ydelsens funktioner. Yderligere bør den dataansvarlige træffe kontrolforanstaltninger, der sikrer integritet, fortrolighed og tilgængelighed for de forskellige brugere.

I vejledningen angiver EDPB, at udbyderne bør afholde sig fra at tilkoble e-mail eller videostreaming til deres tjenesteydelse, da disse involverer en lang og kompleks datapolitik, der ikke overholder databeskyttelsesforordningens gennemsigtighedsprincip.

Vejledningen anfører, at i de tilfælde, hvor data bliver behandlet for at kunne udføre en brugers anmodning, der er den dataansvarlige undtaget fra kravet om at have brugerens forudgående samtykke efter Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor artikel 5(3).

Den dataansvarlige skal slette data, der ikke længere er nødvendigt for det formål, som personoplysningerne bliver behandlet for. Derudover skal der slettes data, der ikke er nødvendig for tjenesteydelsens brug. Dette kan eksempelvis være andre personers stemmer i baggrunden, når en person bruger den stemmestyrede assistent. Den dataansvarlige bør derfor, når det er muligt, bruge teknologi, der filtrerer unødvendig data fra, således at kun brugerens stemme optages.

Ifølge vejledningen vil både produktudvikling og brug af de pågældende teknologier ofte udløse en pligt for den dataansvarlige til at lave en konsekvensanalyse.

Læs et kort resumé af vejledningen her:
https://www.datatilsynet.dk/internationalt/internationalt-nyt/2021/jul/retningslinjer-for-stemmestyrede-assistenter

Læs vejledningen her:
https://edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf

Ny vejledning om dataansvarlige og databehandlere

Det Europæiske Databeskyttelsesråd vedtog den 7. juli 2021 en vejledning om dataansvarlige og databehandlere baseret på definitionerne i artikel 4 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»databeskyttelsesforordningen«).

Hovedformålet med vejledningen er at tydeliggøre betydningen af begreberne og at tydeliggøre de forskellige roller og ansvarsfordelingen. Det følger af vejledningen, at det er vigtigt, at have beskrevet den præcise betydning af begreberne, idet disse spiller en afgørende rolle i anvendelsen af databeskyttelsesforordningen. I del 1 af vejledningen diskuteres retningslinjerne for definitionerne af de forskellige begreber. I del 2 gives der vejledning på de konsekvenser, der er knyttet til de forskellige roller.

Til illustration fremfår det – allerede kendte - af vejledningen, at en dataansvarlig bestemmer formålet med behandlingen, det vil sige hvorfor og hvordan behandlingen foregår. Vejledningen præciserer herefter, at der ikke er nogen begrænsning af, hvilken person (fysisk eller juridisk), der påtager sig rollen som dataansvarlig. Det er i praksis virksomheden som helhed og ikke en individuel person i virksomheden, som eksempelvis den administrerende direktør eller en medarbejder. Endvidere fremgår det af vejledningen, at det ikke er nødvendigt for en dataansvarlig at have adgang til de omhandlede data for at blive udnævnt som ansvarlig.

En databehandler er en fysisk eller juridisk person, offentlig myndighed, styrelse eller et andet organ, der behandler personoplysninger på vegne af den dataansvarlige. Vejledningen opstiller to krav til databehandleren. Det første krav er, at databehandleren er en særskilt enhed i forhold til den dataansvarlige. Det andet krav er, at personoplysningerne behandles på vegne af den dataansvarlige. Vejledningen præciserer, at en databehandler har et vist skøn til at træffe beslutninger om, hvordan den dataansvarliges anvisninger følges på bedste vis. Det er dog en overtrædelse af databeskyttelsesforordningen, hvis databehandleren bestemmer egne formål med behandlingen.

Yderligere fremgår det af vejledningen, at der skal indgås en behandlingsaftale mellem den dataansvarlige og databehandleren, hvilket er specificeret i databeskyttelsesforordningen. Denne aftale skal dog ikke blot gentage bestemmelserne i databeskyttelsesforordningen, derimod bør aftalen indeholde specifikke oplysninger om, hvordan kravene vil blive opfyldt, og hvilket sikkerhedsniveau, der kræves for behandlingen af den data, der er omfattet af aftalen.

Læs et kort resumé af vejledningen her:
https://www.datatilsynet.dk/internationalt/internationalt-nyt/2021/jul/ny-europaeisk-vejledning-om-dataansvarlige-og-databehandlere

Læs vejledningen her:
https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

Retningslinjer 1/2020 om behandling af personoplysninger i forbindelse med opkoblede køretøjer og mobilitetsrelaterede anvendelser

Det Europæiske Databeskyttelsesråd (»EDPB«) vedtog den 9. marts 2021 Retningslinjer 1/2020 om behandling af personoplysninger i forbindelse med opkoblede køretøjer og mobilitetsrelaterede anvendelser. Retningslinjerne har til formål at fremme overholdelsen i forbindelse med behandling af personoplysninger inden for ikke-erhvervsmæssig brug af opkoblede køretøjer. Retningslinjerne finder anvendelse på personoplysninger, der (1) behandles i køretøjet, (2) udveksles mellem køretøjet og de personlige enheder, der er tilsluttet eller (3) indsamles lokalt i køretøjet og eksporteres til eksterne enheder, hvor de behandles.

Opkoblede køretøjer indsamler data om fysiske personer, der kan identificeres og indsamler dermed personoplysninger. Opkoblede køretøjer giver anledning til bekymringer vedrørende beskyttelse af data og privatlivets fred i forbindelse med behandling af lokaliseringsdata. EDPB ønskede at lægge vægt på at styrke interessenternes bevidsthed om, at lokaliseringsteknologier kræver, at der gennemføres sikkerhedsforanstaltninger, der forhindrer overvågning og misbrug af disse data.

EDPB vurderede, at køretøjsførere og -passagerer ikke altid informeres tilstrækkeligt om den behandling af data, der foretages i et opkoblet køretøj. Databehandlere skal derfor være opmærksomme på at indhente samtykke, der ikke er sammenknyttet købskontrakten, fra alle deltagere f.eks. ejer, fører, biludlejer mm. I mange tilfælde er brugeren ikke klar over, at der foretages databehandling i vedkommendes køretøj, og det er dermed svært at påvise at gyldigt samtykke i henhold til Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»databeskyttelsesforordningen«).

EDPB opstillede i retningslinjerne tre kategorier af personoplysninger, som kræver særlig opmærksomhed fra køretøjs- og udstyrsfabrikanters, tjenesteudbyderes og andre dataansvarliges side. Dette er lokaliseringsdata, biometriske data samt data, der kan afsløre lovovertrædelser eller trafikforseelser. Disse oplysninger må behandles i forbindelse med blandt andet førersikkerheden, forsikring, effektiv transport, underholdning eller informationstjenester. Den dataansvarlige skal dog sikre, at formålet med behandlingen er »specifikt, udtrykkeligt og legitimt« samt at der er

et gyldigt retsgrundlag i artikel 5 i databeskyttelsesforordningen. EDPB anbefaler, at den dataansvarlige jævnligt indhenter samtykke.

EDPB oplyste, at dataansvarlige så vidt muligt skal undgå at anvende processer, der involverer personoplysninger eller overførsel af personoplysninger uden for køretøjet. Såfremt det overvejes at overføre oplysninger uden for køretøjet, mener EDPB, at det skal overvejes at anonymisere oplysningerne.

EDPB kommenterede også på den registreredes rettigheder. Det anbefales, at de dataansvarlige fremmer de registreredes kontrol i hele behandlingsperioden ved at give dem værktøjer til effektivt at udøve deres rettigheder såsom ret til indsigt, berigtigelse og sletning mm. EDPB anbefaler derfor et profilstyringssystem, hvor føreren kan stoppe indsamling af data midlertidigt eller permanent.

EDPB understregede, at retningslinjerne ikke er udtømmende og fremlagde endvidere en række caseeksempler på problemstillinger inden for behandling af personoplysninger med køretøjer og mobilitetsrelaterede anvendelser.

Læs retningslinjerne her: https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_da.pdf

TikTok har fået en bøde for krænkelse ved behandling af børns persondata

Den hollandske databeskyttelsesmyndighed (»AP«) offentliggjorde den 22. juli 2021 en pressemeddelelse om, at AP har pålagt TikTok en bøde på € 750.000 for krænkelse af børns privatliv.

TikTok er en videoapp, der gør det muligt for brugerne at skabe videoer, som de kan dele med resten af TikTok's brugere.

TikTok havde udarbejdet en engelsk erklæring om, hvordan app'en indhentede, behandlede og brugte personoplysninger. Ved ikke at tilbyde erklæringen på hollandsk fandt AP, at TikTok ikke kunne give sine hollandske brugere en tilstrækkelig forklaring på, hvordan app'en opererede for dens hollandske brugere. De primære brugere af TikTok er børn, som er en særlig udsat kategori af borgere i henhold til den hollandske databeskyttelseslovgivning, hvorfor der gælder særlige beskyttelseshensyn ved behandling af børns persondata.

TikTok krænkede derfor hollandsk lovgivning om databeskyttelse, som er baseret på et princip om, at personer altid skal kunne gennemskue, hvad der sker med deres personoplysninger.

AP har, modsat det danske Datatilsyn, mulighed for at udstede administrative bøder, hvilket de valgte at gøre i den pågældende sag. TikTok har gjort indsigelse mod bøden.

Læs nyheden her: https://edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en

Amazon pålægges rekordbøde for overtrædelse af databeskyttelsesforordningen på 746 mio. euro

Den 16. juli 2021 pålagde Luxembourgs myndighed for databeskyttelse (»CNPD«) onlinegiganten Amazon (nærmere bestemt Amazon Europe Core S.à r.l.) en bøde på 746 mio. euro for overtrædelse af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'). Det offentliggjorde Amazon den 29. juli 2021 i forbindelse med indgivelsen af sin kvartalsrapport til US Securities and Exchange Commission (SEC). Heri kaldte Amazon CNPD's beslutning for »without merit«, og Amazon har givet udtryk for at ville appellere afgørelsen.

Afgørelsen og nærmere oplysninger om, hvordan Amazon har overtrådt databeskyttelsesforordningen, er ikke blevet offentliggjort. En lov i Luxembourg forhindrer offentliggørelse indtil appelprocessen er afsluttet.

Bøden er resultatet af en undersøgelse, der startede med en klage i 2018 fra en fransk gruppe, La Quadrature du Net, der søger at fremme borgeres digitale rettigheder og friheder. I klagen anførte La Quadrature du Net, at Amazons system for målrettede reklamer ikke var samtykkebaseret.

Ifølge flere medier er bøden den hidtil største bøde givet for overtrædelse af databeskyttelsesforordningen og den første af den kaliber. Den tidligere rekord var en fransk bøde til Google på 50 mio. euro.

Læs Amazons rapport for 2. kvartal 2021 her (bøden fremgår af side 13): https://s2.q4cdn.com/299287126/files/doc_financials/2021/q2/cbae1abf-eddb-4451-9186-6753b02cc4eb.pdf

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


Peter Nordbeck og Malin Svensson

Nyheter från integritetsskyddsmyndigheten

I denna notis kommer tre utvalda nyheter från den svenska tillsynsmyndigheten Integritetsskyddsmyndigheten (”IMY”) presenteras. Två av nyheterna avser inledda granskningar och den tredje nyheten berör det nya samarbetet mellan IMY och AI Sweden.

IMY granskar SKR:s väntetidsdatabas

Sveriges Kommuner och Regioner (”SKR”) använder en nationell väntetidsdatabas i syfte att ta fram statistik avseende väntetider i vården. Uppgifterna i databasen är insamlade från patientjournaler i regionerna som sedan överförs till SKR.

Dataskyddsförordningen (”GDPR”) uppställer krav på rättslig grund när en myndighet eller en organisation behandlar personuppgifter. Känsliga personuppgifter, så som uppgifter om hälsa, är som huvudregel förbjudet att behandla. För att få behandla känsliga personuppgifter måste det utöver rättslig grund även finnas ett tillämpligt undantag i GDPR som är tillämpligt på behandlingen.

IMY meddelade på sin hemsida den 9 november 2021 att de ställer frågor till SKR om vilken rättslig grund, samt vilket undantag från förbudet mot behandling av känsliga personuppgifter, som SKR:s behandling stödjer sig på. Knäckfrågan, som även är av principiell betydelse, är vilka möjligheter en privat organisation, som inte är en vårdgivare, har att behandla personuppgifter på det sätt som sker i väntetidsdatabasen.

IMY inleder granskning efter anmälan från DO

Diskrimineringsombudsmannen (”DO”) har i en anmälan till IMY pekat ut ett webbformulär som en personuppgiftsincident. Webbformuläret används för att lämna in tips och klagomål. DO menar att det analysverktyg som används för att förbättra användarvänligheten i vissa fall kan inhämta och lagra personuppgifter.

Den 12 oktober 2021 meddelade IMY på sin hemsida att de beslutat att inleda en granskning av det som skett. IMY påpekar att en personuppgiftsansvarig har ett stort ansvar för att löpande kontrollera sina IT-system och säkerheten kring dem. Det gäller inte minst när det avser ett webbformulär som kan innehålla känsliga uppgifter.

Samarbete mellan IMY och AI Sweden avseende frågor om AI och dataskydd

De som arbetar med AI får många gånger brottas med svåra rättsliga frågor om dataskydd och integritet. För att sådana frågor inte ska stå i vägen för innovation och samhällsutveckling har IMY och AI Sweden inlett ett samarbete. Arbetet sker i linje med det uppdrag som IMY fått av regeringen; att höja den allmänna kunskapsnivån om integritets- och dataskyddsfrågor bland innovationsaktörer. IMY påpekar att samarbetet med AI Sweden är ett viktigt steg i det arbetet.

AI Sweden arbetar tillsammans med sina partners för att utveckla lösningar på rättsliga frågeställningar om datahantering som uppstår i samband med utveckling av AI. Ett exempel på en utmaning i GDPR som lyfts fram särskilt är innebörden av anonymisering. AI Sweden ser fram emot att tillsammans med IMY skapa möjligheter för att öka användningen av AI i Sverige.

Samarbetet pågår fram till den 31 mars 2023. Genom gemensamma insatser kommer IMY och AI Sweden att ge stöd och vägledning avseende de rättsliga frågeställningar som identifieras.

Peter Nordbeck er advokat i *Advokatfirman Delphi, Stockholm.*

Malin Svensson er Associate Trainee i *Advokatfirman Delphi, Stockholm.*

Bird & Bird

Gunnar Hjalt

100 kr i ersättning för konstaterat upphovsrättsintrång, mål nr PMFT 4168-20.

Patent- och marknadsöverdomstolen (PMÖD) har bedömt att en artikel som gjorts tillgänglig på en blogg och vilken funnits tillgänglig där under nästan två år innebar ett intrång i upphovsrätten till artikeln. Därutöver konstaterade domstolen att upphovsmannen inte namngivits på korrekt sätt. Den enstaka exemplarframställning som Patent- och marknadsdomstolen (PMD) tidigare funnit vara ursäktlig med hänsyn till rättsvårdande intressen – det hade gjorts en polisanmälan med anledning av artikeln – bedömdes istället av PMÖD vara en exemplarframställning för privat bruk. Rättighetshavaren tilldömdes 100 kr i skälig ersättning för tillgängliggörandet men ingen ersättning för utebliven namngivning. Domstolen ansåg inte att upphovsmannen hade kunnat redogöra för vilken skada den yrkade ersättningen skulle täcka.

Se avgörandet här: *https://www.domstol.se/globalassets/filer/domstol/patentochmarknadsoverdomstolen/avgoranden/2021/pmft-4168-20.pdf*

Brott mot avkodningslagen och intrång i signalrätten gav fängelse i 2 år. Mål nr B 5557-21

Patent- och marknadsöverdomstolen (PMÖD) har funnit två personer skyldiga till brott mot både avkodningslagen och för intrång i signalrätten enligt upphovsrättslagen. I det ena fallet – brott mot förbudet beträffande viss avkodningsutrustning – gällde målet en s.k. cardsharing-verksamhet vilken involverade upp till 6617 unika användare per augusti 2016. Denna verksamhet fasades senare ut till förmån för en iptv-verksamhet som involverade upp till 1766 aktiva användaridentiteter per september 2018.

Huvudmannen hade tidigare dömts för liknande brott och dömdes nu till 2 års fängelse och näringsförbud i fem år. En annan gärningsman fick påföljden fängelse i 1 år och 6 månader. En tredje gärningsman befanns skyldig till intrång enbart i signalrätten och dömdes till villkorlig dom och dagsböter.

Samtliga gärningspersoner ålades att solidariskt betala skälig ersättning för utnyttjandet av tv-utsändningarna, till flera målsägandebolag. Totalt 82 600 000 kr avseende brott mot förbudet beträffande avkodningsutrustning samt 10 973 000 kr avseende brott mot upphovsrättslagen.

Se avgörandet här: *https://www.domstol.se/globalassets/filer/domstol/patentochmarknadsoverdomstolen/avgoranden/2021/b-5557-21.pdf*

Full ersättning för rättegångskostnad i såväl Patent- och marknadsdomstolen som i Patent- och marknadsöverdomstolen trots att överklagande i den materiella frågan återkallats, mål nr PMT 873-19.

Målet vid Patent- och marknadsöverdomstolen (PMÖD) gällde intrång i den svenska delen av europeiskt patent 09727929.3 (EP 2257260) avseende ett tyngdtäcke. Patenthavaren stämde en svensk förmodad intrångsgörare för patentintrång varvid denne försökte förklara patentet ogiltigt vid samma domstol dvs Patent- och marknadsdomstolen (PMD). Patentet upprätthölls härvid men i begränsad avfattning. PMDs beslut överklagades av båda parter, initialt både i intrångsdelen och i ogiltighetsdelen.

Under tiden som tvisten i Sverige pågick var stridspatentet föremål för en invändning från svarandens sida vid Europeiska patentmyndigheten (EPO). Utgången vid EPO blev att stridspatentet förklarades ogiltigt. Patenthavaren överklagade beslutet till Board of Appeal vilken fastställde att patentet var ogiltigt. Parterna återkallade därefter sin respektive talan vid PMÖD, frånsett frågan om fördelning av rättegångskostnaderna. PMÖD kom fram till att den aktuella situationen i rättegångskostnadshänseende måste likställas med den att svaranden vunnit full framgång med sitt överklagande i sakfrågan. Därmed kunde domstolen komma fram till att patenthavaren skulle ersätta svaranden för dess rättegångskostnad i båda instanserna.

Se avgörandet här: *https://www.domstol.se/globalassets/filer/domstol/patentochmarknadsoverdomstolen/avgoranden/2021/pmt-873-19.pdf*

Legalroom inte förväxlingsbart med LegalZoom för identisk verksamhet, mål nr PMÖÄ 11204-20

I en invändning från innehavaren av varumärket LegalZoom mot svensk varumärkesregistrering 600 290 Legalroom kom Patent- och registreringsverket (PRV) fram till att det var fråga om identiska tjänster, likartade märken såväl fonetiskt som visuellt men att märkena gav upphov till olika associationer.

Sökandens märke avsåg juridiska tjänster i klass 45 och invändarens märke avsåg även det (bland annat) juridiska tjänster i klass 45.

Patent- och marknadsdomstolen (PMD) kom också fram till att de konceptuella skillnaderna mellan märkena gjorde att det inte förelåg någon förväxlingsrisk, även med beaktande av att det var fråga om tjänsteslagsidentitet.

Patent- och marknadsdomstolen (PMÖD) delade de lägre instansernas uppfattning att det var fråga om tjänsteslagsidentitet samt att märkena var visuellt och fonetiskt lika. PMÖD gjorde bedömningen att båda märkena saknade klar och bestämd innebörd och måste ses som fantasiord som vart och ett gav upphov till olika associationer. Domstolen påpekade också att innehavaren hade valt att skriva märket som LegalZoom, alltså med versaler för bokstäverna L och Z och i övrigt med gemena, vilket ytterligare talade för att märket skulle delas upp i förledet LEGAL och suffixet ZOOM.

Se avgörandet här:
https://www.domstol.se/globalassets/filer/domstol/patentochmarknadsoverdomstolen/avgoranden/2021/pmoa-11204-20.pdf

Gunnar Hjalt, Senior Counsel, Bird & Bird Advokat.

Gorrissen Federspiel

Tue Goldschmieding

Domænenavnet »guerciotti.dk« skulle overdrages til klageren

Det danske Klagenævn for Domænenavne traf den 8. juli 2021 afgørelse i sag 2021-0027 mellem Summit Distributions ApS (»klager«) og indklagede, som drev virksomhed under navnet Guerciotti Cykler fra 1981 til 2008 og var indehaver af en varemærkeregistrering af ordmærket GUERCIOTTI fra 1985 til 1996. Sagen drejede sig om, hvorvidt domænenavnet »guerciotti.dk« skulle overdrages til klager.

Klager argumenterede blandt andet for, at klager havde en række binavne tilknyttet sit selskab, herunder Guerciotti ApS, der var registreret den 26. januar 2021. På tidspunktet for klagen benyttede klager domænenavnet »guerciotti.nu« i forbindelse med sin virksomhed. Klager havde en aftale med den italienske virksomhed Guerciotti Export srl om, at klager skulle distribuere og opbygge det danske marked med Guerciotti, som er et italiensk cykelbrand. Guerciotti Export srl har et registreret EU-varemærke, hvori betegnelsen »Guerciotti« indgår. Klager mente, at det var hæmmende for virksomheden ikke at kunne distribuere Guerciotti-cykler i Danmark uden anvendelse af domænet »guerciotti.dk«.

Frem til 2008 blev domænet »guerciotti.dk« brugt til indklagedes tidligere virksomhed med salg af cykler. På tidspunktet for klagen blev det brugt til e-mailkorrespondance, og der kunne ikke foretages køb på hjemmesiden. Derudover havde indklagede af nostalgiske årsager bibeholdt domænet.

Efter en interesseafvejning i medfør af lov nr. 164 af 26. februar 2014 (»den danske domænelov«) § § 25, stk. 1 om god domænenavnsskik kom Klagenævnet for Domænenavne frem til, at klagers kommercielle interesse vejede tungere end indklagede interesse i forsat at kunne bruge sin e-mailadresse. Klagenævnet for Domænenavne lagde bl.a. vægt på, at domænenavnet bestod betegnelsen »Guerciotti«, som indgik i varemærket tilhørende klagers samarbejdspartner.

Klagenævnet for Domænenavne fandt derfor, at domænenavnet »guerciotti.dk.dk« skulle overføres til klager.

Læs afgørelsen her:
https://www.domaeneklager.dk/sites/default/files/2021-07/2021-0027%2C%20guerciotti.dk_.pdf

Domænenavnet »naturpartiet.dk« skulle ikke overdrages til klageren

Det danske Klagenævn for Domænenavne traf den 8. juli 2021 afgørelse i sag 2021-0121. Klagenævnet for Domænenavne fandt frem til, at domænenavnet »naturpartiet.dk« ikke skulle overdrages til klageren.

Klager gjorde gældende, at denne havde oprettet et internetprojekt ved navn »Naturpartiet«, der med tiden skulle blive til et rigtigt parti, formentlig til kommunalvalget 2021. Klageren havde på daværende tidspunkt registreret og anvendt domænenavnet »naturparti.dk«. Klageren mente, at dennes domænenavn helst skulle svare til partinavnet, før der kunne fremstilles merchandise med partinavnet. Desuden fremførte klager, at der ikke fandtes en hjemmeside, der var tilknyttet domænenavnet, ligesom at domænenavnet ikke var anvendt til noget. Klager var i april 2021 i kontakt med indklagede, der var villig til at overdrage domænenavnet for penge. Klager mente på denne baggrund, at domænenavnet skulle overdrages til klager.

Indklagede gjorde gældende, at domænenavnet blev anvendt som et samlingssted for netværket »Naturpartiet«, som indklagede stiftede efter landsindsamlingen »Danmark planter træer«. Indklagede gjorde desuden gældende, at domænenavnet var aktivt i brug i forbindelse med indklagedes politiske netværk. Indklagede statuerede desuden, at denne ikke ønskede at sælge domænenavnet, da indklagede gentagne gange havde afvist salg. Indklagede mente, at klager fremkom med urigtige oplysninger i sin klage, da naturparti.dk skrev på deres hjemmeside, at der var tale om »et fiktivt inspirations- og internetprojekt«. Indklagede mente på denne baggrund ikke, at domænenavnet skulle overdrages til klager.

Klagenævnet for Domænenavne lagde først til grund, at indklagede ikke havde registreret domænenavnet »Naturpartiet.dk« med henblik på videresalg eller udlejning. Klagenævnet for Domænenavne fandt, at klagerens interesse i domænenavnet ikke oversteg indklagedes interesse heri. Derfor indebar indklagedes fastholdelse af registreringen af domænenavnet ikke en overtrædelse af lov nr. 164 af 26. februar 2014 (»den danske domænelov«) § 25 om god domænenavnsskik.

Klagenævnet for Domænenavne kunne derfor ikke overdrage domænenavnet »Naturpartiet.dk« til klager.

Læs afgørelsen her:
https://www.domaeneklager.dk/sites/default/files/2021-07/2021-0121%2C%20naturpartiet.dk%20-%20anonymiseret.pdf

Sag om midlertidigt forbud mod markedsføring af sutter

Sø- og Handelsretten afsagde den 20. august 2021 dom i sagen BS-17072/2021-SHR mellem AH License ApS (»AH«) og Bibs Danmark ApS (»Bibs«) som sagsøgere og FB Trading ApS (»FB«), Frigg Production ApS (»Frigg«) og Sundesutter.dk ApS (»Sundesutter«) som sagsøgte. Sagen angik, hvorvidt tre af de sagsøgtes suttemodeller var nærgående efterligninger af sagsøgernes suttemodeller.

Indledningsvis fandt Sø- og Handelsretten, at sagsøgernes modeller »Bibs Colour« og »Bibs De Lux«, under henvisning til bl.a. deres nøje udvalgte farver, udtrykselementer og formgivning, havde et kommercielt særpræg. Suttemodellerne nød derfor beskyttelse mod meget nærgående eller slaviske produktefterligninger, jf. § 3, stk. 1 i lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov'). Sø- og Handelsretten tog herefter stilling til, om de sagsøgtes modeller »Frigg Classic«, »Frigg Color Blocks« og »Frigg Daisy« krænkede sagsøgernes beskyttede modeller. Sø- og Handelsretten fandt, at »Frigg Classic« og »Frigg Color Blocks« ud fra et helhedsindtryk fremstod forvekslelige med sagsøgernes modeller under henvisning til sutternes formgivning og farvevalg. Sø- og Handelsretten fandt ikke, at »Frigg Daisy« var kommercielt identiske med sagsøgers produkter, hvorfor der ikke forelå forvekslingsrisiko.

På baggrund heraf kom Sø- og Handelsretten frem til, at sagsøgerne havde sandsynliggjort, at der forelå en krænkelse af sagsøgernes ret, jf. § 413, stk. 1 i lovbekendtgørelse nr. 1835 af 15. september 2021 ('den danske retsplejelov'). Da sagsøgerne alene havde sandsynliggjort, at der forelå en krænkelse, betingede Sø- og Handelsretten nedlæggelse af et forbud af, at sagsøgerne senest den 3. september 2021 stillede sikkerhed for DKK 10.000.000. Retten fandt ikke, at der var grundlag for, at der skulle ske beslaglæggelse af sagsøgtes produkter eller forme til fremstilling af produkterne.

Læs et kort resumé af dommen her:

https://www.domstol.dk/soeoghandelsretten/aktuelt/2021/8/baby-sutter/

Læs hele dommen her:

https://domstol.fe1.tangora.com/media/-300011/files/BS-17072-2021-SHR_Kendelse.pdf

Varemærkerne »PANZERGLASS« og »PANSERGLAS« m.fl. nød beskyttelse mod andres brug af betegnelser som »panserglas«

Den 30. august 2021 afsagde Sø- og Handelsretten dom i sagerne BS-9582/2017-SHR og BS-26278/2020-SHR mellem sagsøger Panzerglass A/S, som udvikler og sælger beskyttelsesprodukter til bl.a. mobiltelefoner, og de sagsøgte TechAmmo ApS og Selek Danmark ApS, som begge bl.a. sælger skærmbeskyttelse til mobiler.

Spørgsmålet var, om de sagsøgte ved at sælge skærmbeskyttelse under forskellige afarter af betegnelsen »panserglas« krænkede Panzerglass A/S' varemærkerettigheder efter Europa-Parlamentets og Rådets forordning (EU) 2017/1001 af 14. juni 2017 om EU-varemærker (»varemærkeforordningen«), lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) og/eller lov nr. 426 af 3. maj 2017 (»den danske markedsføringslov«). Panzerglass A/S påberåbte sig i den forbindelse to danske og fire EU-varemærker, herunder »PANZER GLASS« og »PANSERGLAS«, registreret for bl.a. beskyttelsescovers til mobiltelefoner. Retten skulle også tage stilling til, om det danske varemærke »PANSERGLAS« var ugyldigt, og om Panzerglass A/S' varemærkerettigheder var ophørt ved degeneration.

Først fandt Retten efter en samlet vurdering af bevisførelsen, at Panzerglass A/S' EU-varemærke »PANZER GLASS« nød beskyttelse som et velkendt varemærke. EUIPO's appelinstans havde tidligere truffet en afgørelse om varemærkets gyldighed, som var bindende for parterne.

Derefter fandt Retten under henvisning til grunde EUIPO havde anført og til bevisførelsen for Retten selv, at der ikke var grundlag for at tilsidesætte det danske varemærke »PANSERGLAS« som ugyldigt. Retten bemærkede, at det ville gøre beskyttelsen af EU-varemærket »PANZER GLASS« illusorisk, hvis »PANSERGLAS« blev ophævet, og fandt det ikke godtgjort, at »PANSERGLAS« manglede oprindeligt særpræg, eller at nogen af Panzerglass A/S' varemærker havde mistet deres varemærkestatus ved degenerering.

Ved sin stillingtagen til krænkelsesspørgsmålet fandt Retten, at de sagsøgtes anvendelse af forskellige afarter af betegnelsen »panserglas« skabte en risiko for forveksling med, og dermed krænkede, Panzerglass A/S' varemærkerettigheder grundet fonetiske, konceptuelle og visuelle ligheder. Retten bemærkede, at det ikke havde betydning for forvekslingsrisikoen, om der indgik glas i de omtvistede beskyttelsescovers. Det sidste var ellers et væsentligt tvistepunkt for parterne. Retten fandt ikke grundlag for at dømme for overtrædelse af den danske markedsføringslov.

Som resultat nedlagde Retten forbud mod, at de sagsøgte gør erhvervsmæssig brug af bl.a. betegnelsen »panserglas« for beskyttelsescovers og beskyttelsesfilm til bl.a. laptops, mobiltelefoner og tablets, samt at begge sagsøgte skulle betale vederlag, erstatning og delvise sagsomkostninger til Panzerglass A/S for krænkelse af dennes varemærkerettigheder.

Læs et kort resumé af dommen her:

https://www.domstol.dk/soeoghandelsretten/aktuelt/2021/8/om-varemaerket-panzer-glass/

Læs hele dommen her:

https://domstol.fe1.tangora.com/media/-300011/files/BS-9582-2017-SHR_og_BS-26278-2020-SHR_-_Dom_(sambehandling).pdf

Ordmærkerne »VVS-Eksperten.dk« og »VVS-Eksperten« var ikke indarbejdet som varemærker

I dommen i sag BS-4052/2021-SHR afsagt den 8. september 2021 fandt Sø- og Handelsretten det ikke godtgjort, at navnene »VVS-Eksperten.

dk« eller »VVS-Eksperten« ved indarbejdelse var blevet varemærker.

Sagen vedrørte, om sagsøgeren VVS-Eksperten A/S havde stiftet varemærket til ordmærkerne »VVS-Eksperten« og »VVS-Eksperten.dk«, og om sagsøgte Kliplev VVS og Sydventilation A/S (»Kliplev«) havde krænket sagsøgers varemærkerettigheder ved anvendelse af navnet »VVS-Eksperten« og »VVS-Eksperten.com«.

Retten fandt, at betegnelserne måtte anses for beskrivende for detailhandel med VVS-artikler og VVS-værktøj, hvorfor mærket ikke havde særpræg. Mærkerne kunne derfor alene stiftes som varemærker ved indarbejdelse, jf. lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) § 3, stk. 3, 2. pkt. Retten lagde ved vurderingen vægt på, at sagsøger ikke kunne bevise, at brugere specifikt søgte efter sagsøgers virksomhed, når der på Google blev søgt på »vvs eksperten« og at markedsføringsomkostninger ikke i sig selv beviste, at »VVS-Eksperten.dk« havde ændret karakter fra artsbetegnelse til forretningskendetegn. På denne baggrund blev Kliplev frifundet.

Retten fandt dog, at Kliplevs brug af udsagnet »Vi er eksperter, vores autorisation er din sikkerhed. For at slå det helt fast, så har vi intet at gøre med VVS-Eksperten A/S eller andre uautoriserede virksomheder at gøre« var vildledende og misrekommanderende og udgjorde en overtrædelse af lov nr. 426 af 3. maj 2017 (»den danske markedsføringslov«) § 3 og § 20.

Læs et kort resumé af dommen her:

https://www.domstol.dk/soeoghandelsretten/aktuelt/2021/9/varemaerke-ikke-indarbejdet/

Læs hele dommen her:

https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-4052-2021-SHR.pdf?rev1

Parkeringsselskab betaler penge tilbage til forbrugere

Den danske Forbrugerombudsmand udsendte den 2. september 2021 en pressemeddelelse om, at Forbrugerombudsmanden havde vurderet, at parkeringsselskabet Apcoa benyttede en urimelig betalingsmetode på nogle af selskabets parkeringspladser. Metoden medførte, at forbrugerne betalte et højere beløb end timetaksten for den tildelte parkering.

Ved parkering på de omhandlede parkeringspladser kunne forbrugerne vælge at betale et beløb ved at trykke på værdiknapper f.eks. 2 kroner, 5 kroner eller 10 kroner på betalingsautomaten. Hvis beløbet oversteg timetaksterne for et helt antal af timer, ville Apcoa trække det valgte beløb fra forbrugerens betalingskort, men samtidig kun give forbrugeren en ret til at parkere i det hele antal af timer. Et valgt overskydende beløb udløste således ikke ekstra minutter af parkeringstid.

Forbrugerombudsmanden vurderede, at betalingsmetoden udgjorde en urimelig aftale efter § 36, stk. 1 og § 38 c, stk. 1 i lovbekendtgørelse nr. 193 af 2. marts 2016 (»den danske aftalelov«). Forbrugerombudsmanden bemærkede, at det ved et betalingskort var muligt at trække et præcist beløb, der svarede til en fastsat parkeringstid, og at forbrugerne ikke burde betale for parkeringstid, som de ikke fik tildelt. Det fremgik af Forbrugerombudsmandens pressemeddelelse, at forbrugerne derfor havde krav på, at få refunderet det for meget betalte beløb.

Læs pressemeddelelsen her:

https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2021/parkeringsselskab-betaler-penge-tilbage-til-forbrugere/

Easy Park politianmeldes for at vildlede forbrugere ved bl.a. ikke at oplyse tydeligt om et gebyr

Den danske Forbrugerombudsmand oplyste i en pressemeddelelse den 26. august 2021, at Forbrugerombudsmanden har politianmeldt Easy Park for at overtræde forbuddet mod vildledning i lov nr. 426 af 3. maj 2017 (»den danske markedsføringslov«).

Forbrugerombudsmanden vurderede, at Easy Park overtrådte vildledningsforbuddet ved at skjule, at det beløb, der bliver vist i Easy Parks parkeringsapp, når brugerne skal betale for parkering, omfatter et gebyr på 15 % af parkeringstaksten. Derfor politianmeldte Forbrugerombudsmanden Easy Park for dels ikke at have oplyst tydeligt om gebyret på 15 % på sin danske hjemmeside, i app'en eller når brugerne downloader og tilmelder sig app'en, og dels slet ikke at have oplyst om gebyret på 15 % på skilte på Easy Parks parkeringspladser.

Derudover politianmeldte Forbrugerombudsmanden også Easy Park for ikke tydeligt at have oplyst app'ens brugere om, at lokalitetsfunktionen i app'en afhænger af telefonens GPS-funktionalitet, som kan være upræcis, og at brugerne selv har ansvaret for, at deres bil er placeret i det rigtige parkeringsområde.

Forbrugerombudsmanden vurderede, at Easy Park var forpligtet til at refundere det opkrævede gebyr på 15 % til de kunder, der havde benyttet sig af såkaldt fastprisparkering (betaling af et på forhånd fastsat beløb for parkering i et bestemt antal timer). Ifølge Forbrugerombudsmanden var det i strid med den danske markedsføringslovs vildledningsforbud og § 9, stk. 3 i lov nr. 1457 af 17. december 2013 (»den danske forbrugeraftalelov«), at kunderne i disse tilfælde blev vist en pris, som ikke inkluderede gebyret på 15 %, og i strid med § 82, stk. 1 i lov nr. 652 af 8. juni 2017 ('den danske betalingslov') at Easy Park trods dette hævede betalingen af den oplyste parkeringspris med tillæg af gebyret uden forbrugernes samtykke.

Easy Park har oplyst, at de tilbagebetaler gebyret på 15 % til privatkunder, der har benyttet fastprisparkering uden at få gebyret oplyst de sidste tre år, og at app'en er ændret, så gebyret har været inkluderet i den oplyste pris ved fastprisparkering siden april 2020.

Læs pressemeddelelsen her:

https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2021/forbrugerombudsmanden-politianmelder-easy-park/

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


simonsen vogtwiig

Hedda Baumann Heier og
Emile Schjønsby-Nolet

Oslo tingrett: vederlagsberegning for offentlig fremføring av musikkverk

TONO SA («Tono») var ikke med på Oslo-Filharmonien («Filharmonien») sine toner i en ny sak fra Oslo tingrett publisert 3. september 2021. Tono er en forvaltningsorganisasjon som representerer komponister, tekstforfattere og musikkforlag. Filharmonien er en av de såkalt «fire store» symfoniorkestrene i Norge. Saken gjaldt størrelsen på det vederlag Filharmonien skal betale Tono for den fremføring av musikkverk som skjer på Filharmoniens fysiske konserter.

Bakgrunnen for saken er at Tono og de «fire store» avtalte på 80-tallet at orkestrene skulle betale et årlig vederlag til Tono basert på en prosentsats av det enkelte orkesterets årlige samlede inntekter, inkludert blant annet statstilskudd. I 1996 inngikk de fire orkestrene hver sin avtale med Tono hvor vederlaget ble regulert til et fast beløp, basert på de tidligere nevnte prosentvise andelene av hva de totale inntektene utgjorde i 1996. Dette beløpet ble så indeksregulert hvert år.

Denne vederlagsmodellen skiller seg fra den som Tono anvender overfor andre orkestre og aktører som fremfører musikk offentlig på fysiske konserter. Andre betaler i henhold til den såkalte «konserttariffen» hvor arrangøren betaler vederlag basert på en prosentvis andel av billettinntektene med en særregel for gratiskonserter.

I 2014 sa Tono opp avtalen med Filharmonien og partene startet forhandlinger. Forhandlingene førte ikke frem og Tono tok til slutt tok ut forliksklage i desember 2018. Mens partene forhandlet har Filharmonien betalt i henhold til konserttariffen, noe som i praksis har medført en tilnærmet halvering i årlig vederlag sammenliknet med hva som ellers skulle ha blitt betalt under den tidligere avtalen.

Spørsmålet i saken for Oslo tingrett var om konserttariffen utgjorde et «rimelig vederlag» for fremføring av verk, jf. åndsverksloven § 69 og lov om kollektiv forvaltning av opphavsrett § 28. Retten valgte å dele drøftelsen inn i tre hovedbolker: 1) betydningen av verdien av retten som overføres, 2) om det stilles krav til sammenheng mellom bruk og vederlag og hva det eventuelt innebærer, og 3) betydningen av vanlig praksis.

Når det gjelder betydningen av verdien av retten som overføres, uttaler retten at det antagelig ikke er kommersielt grunnlag i Norge for å ha et så stort orkester med en slik kvalitet som Filharmonien uten offentlig støtte. Retten mener likevel at billettprisene for Filharmoniens ulike konserter fastsettes dynamisk i et fritt marked styrt av alminnelige prinsipper om tilbud og etterspørsel, og at statsstøtten ikke er noen form for billettsubsidiering. Selv om statsstøtten er en forutsetning for driften, har den etter rettens syn ingen sammenheng med den økonomiske verdien av fremføringen av vernede musikkverk. Etter rettens syn utgjorde billettinntektene det beste uttrykket for orkesterfremføringenes økonomiske verdi. Dette fordi billettinntektene reflekterer hvilke inntekter orkesteret har klart å skape knyttet til de konkrete verk som fremføres på de aktuelle konsertene.

Retten viser videre til at det er klart at det ved fastsettelsen av rimelig vederlag må stilles krav om sammenheng mellom vederlaget som betales og bruken av vernede verk. Dette tilsier etter rettens syn at modellen også må ta hensyn til andelen vernede verk. I denne konkrete saken var det slik at en ikke ubetydelig andel av de musikkverk som ble benyttet var falt i det fri. Retten fant det bevist at andelen vernede verk for perioden 2010-2019 lå på mellom 42,5% og 20 % per år.

Til sist kan det også fremheves at retten ikke var enig i Tonos anførsel om at det gamle avtaleverket for de «fire store» gav uttrykk for hva som var vanlig på området. Tvert imot kunne retten ikke se noen grunn til å forskjellsbehandle de fire store symfoniorkestrene sammenliknet med andre orkestre eller øvrige konsertarrangører.

Basert på ovenstående kom retten til at rimelig vederlag for Filharmoniens bruk av musikk vil være konserttariffen, korrigert for andelen vernede verk. Filharmonien vant således frem med sitt krav.

Les saken med saksnr. TOSL-2021-52095 i Lovdatas database. I skrivende stund vites det ikke om saken er anket.

Oslo tingrett: nyhetsretten ved bruk av klipp fra sportssendinger

Den 17. september avsa Oslo tingrett avgjørelse i en tvist mellom Via-

sat AS og Nordic Entertainment Group UK Limited (heretter samlet «NENT») på den ene siden og Verdens Gang AS og VGTV AS (heretter samlet «VG») på den andre siden.

Tvisten gjaldt VGs bruk av klipp fra sportsbegivenheter som NENT hadde eksklusive senderettigheter til. I perioden frem til november 2019 hadde VG en avtale med NENT som ga rett til å sende slike klipp mot et vederlag på MNOK 1 per år. Etter utløpet av avtalen fortsatte VG samme bruk av klipp uten avtale. VG anførte at bruken var lovlig som følge av åndsverkloven § 22 fjerde ledd som gir rett til å sende korte utdrag fra sportsbegivenheter av stor interesse for allmennheten (den såkalte «nyhetsretten»). Spørsmålet i saken var altså om nyhetsretten kom til anvendelse for de aktuelle klippene.

Det rettslige utgangspunktet etter åndsverkloven § 22 første ledd er at kringkastingsselskaper – her NENT – har enerett til å råde over sine egne sendinger. Nyhetsretten utgjør et unntak fra eneretten i de tilfellene det er tale om «*begivenheter av stor interesse for allmenheten*». Regelen springer ut av direktiv 2010/13/EU («AMT-direktivet») og er begrunnet i ønsket om «mangfoldig og variert nyhetsformidling, samt å sikre ytrings- og informasjonsfrihet», jf. fortalens avsnitt 48.

Med henvisning til Rt 2010 s. 366, valgte tingretten å avvise VGs anførsel om at hva som er av stor interesse for allmenheten er en redaksjonell vurdering som retten skal være forsiktig med å overprøve. Etter rettens syn var det ikke begrenset prøvingsadgang i saken.

Etter en gjennomgang av ulike rettskilder som tilsynelatende trekker i litt ulik retning, kom retten til at et egnet avgrensningskriterium vil være om en begivenhet har nyhetsverdi for en «*en større kreds af personer, og samtidig er af interesse for andre end dem, der normalt følger med i begivenheder af lignende karakter*», jf. de danske lovforarbeidene til den tilsvarende danske bestemmelsen LFF 2009-10-07 nr. 25 punkt 4.5.3.1. Videre gis det også samme sted en pekepinn på at nasjonal toppseriefotball ikke i seg selv er tilstrekkelig. Dette mener retten også må gjelde for norske forhold, men legger likevel til at slike fotballkamper etter omstendighetene unntaksvis *kan* være begivenheter av stor interesse for allmennheten likevel. Som eksempel trekkes det frem seriefinaler i nasjonal toppseriefotball.

Retten tar deretter stilling til spørsmålet om hvorvidt en sportsbegivenhet har stor allmenn interesse må vurderes i forkant av begivenheten eller om det også kan vurderes underveis i lys av det som skjer underveis i begivenheten. Retten kommer til at det sistnevnte må være tilfelle, men tilføyer hvis det da i utgangspunktet må skje noe helt ekstraordinært underveis i begivenheten. Som eksempel vises det til at Bundesliga-kamper normalt ikke vil falle inn under nyhetsretten, men kampen der Erling Braut Haaland fikk sin debut for Bundesligaklubben Borussia Dortmund fikk likevel slik karakter da Haaland scoret tre mål etter å ha blitt byttet inn i kampens annen omgang.

I siste del av avgjørelsen går retten konkret til verks og vurderer om sportsklippene i saken gjaldt begivenheter av stor interesse for allmennheten. Retten kom da til at nyhetsretten ikke kom til anvendelse for klippene fra hverken fra Bundesligakamper, UFC-kamper eller Formel 1-løp. Ettersom VG dermed hadde handlet i strid med åndsverkloven § 22 første ledd, konstaterte retten at det forelå plikt til å svare vederlag og erstatning for tap av reklameinntekter knyttet til strømmetjenesten Viafree. Utmålingen var ikke en del av saken.

Les hele avgjørelsen med saksnummer TOSL-2020-180651 i Lovdatas database. Avgjørelsen er anket og saken er således ikke rettskraftig avgjort.

Bidragene er skrevet av senioradvokat Hedda Baumann Heier og advokatfullmektig Emile Schønsby-Nolet ved Simonsen Vogt Wiigs avdeling for Teknologi og Medier i Oslo.

KLIMANØYTRAL DISTRIBUSJON
Levert av Posten

NORGE P. P.
posten

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

Nytt fra

LOVDATA

Lovdata Pro gratis ut året for nye kunder

LOVDATA PRO

Produksjon: 07 Media AS