Lov & Data

Nr. 138
Juni 2019
Nr. 2/2019

Innhold

Lov&Data

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

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

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

Abonnementspriser for 2019
Norge: nkr 370,- pr. år
Utland: nkr 450,- pr. år
Studenter, Norge: nkr 175,- pr år
Studenter, utland: nkr 235,- pr. år
Alle fritt tilsendt.

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

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

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

MILJØMERKET TRYKKERI 07 MEDIA – 2041 0379

Rätten

Stora datamängder uppfattas i allt fler sammanhang som en värdefull resurs. Sådana datamängder genereras genom att allt flera saker, t.ex. smarta telefoner och självkörande fordon, innehåller sensorer som är anslutna till internet. En annan viktig källa är ”klickbeteende” vid användning av onlinetjänster. Den som har tillgång till stora datamängder kan t. ex. med hjälp av maskininlärningsteknik utveckla effektiva algoritmer och identifiera korrelationer mellan olika företeelser.

Mot denna bakgrund har diskussionen om ”rätten till data” intensifierats. Den handlar dels om vilket rättsligt skydd som rättsordningen erbjuder – eller bör erbjuda – för dessa datamängder, dels om avtalsutformningen i relationer där det förekommer värdefulla datamängder. Frågorna är givetvis inte nya, men har delvis kommit i ett nytt ljus genom den senaste tidens tekniska utveckling.

Själva uttrycket ”rätten till data” är dock problematiskt, bl.a. eftersom det är så vagt. Vilken typ av objekt och vilken typ av rättighet avses?

Det immaterialrättsliga skyddet för datamängder av det här diskuterade slaget är ofta – men inte alltid – svagt. Upphovsrättsrättsligt skydd kräver ett originellt urval eller en originell sammanställning av data, något som sällan är uppfyllt här. Sui generis-rätten enligt EU:s databasdirektiv kan erbjuda ett skydd för vissa datamängder, men då förutsätts att det gjorts väsentliga investeringar i anskaffning, granskning eller presentation. Automatgenererade datamängder omfattas normalt inte av detta skydd. Skyddet för företagshemligheter förutsätter hemlighållande och skada i konkurrenshänseende, krav som inte heller så ofta är uppfyllda när det gäller denna typ av datamängder.

EU-kommissionen har i ett meddelande diskuterat möjligheten att införa en ny rätt till data, men förslaget har fått ett svagt mottagande. Andra har istället föreslagit nya incitament och direkta skyldigheter att dela värdefulla datamängder i syfte att främja AI-utvecklingen.

I sammanhanget bör det noteras att stora datamängder ofta innehåller personuppgifter. Därmed har den registrerade en form av rätt till dessa uppgifter enligt dataskyddslagstiftningen, t.ex. är rätt att få tillgång till sina personuppgifter.

I avtalsrelationer – t.ex. i molntjänstavtal – talas det ofta uttryckligen om att en av parterna ska ha

till data

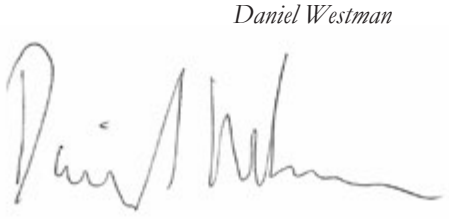
”rätten till data”. I praktiken blir en sådan reglering överlappande med och ibland motsägelsefull i förhållande till andra klausuler i avtalet, t. ex. sådana som rör immaterialrättigheter, konfidentialitet, dataskydd och skyldigheter att överlämna material till kunden i samband att avtalsrelationen avslutas (”exit”).

En vanlig svaghet är att det inte tillräckligt tydligt har analyserats vad parten ska ha rätt till. För fysiska saker tillhandahåller lagstiftningen färdiga paket av rättigheter kopplade till vissa rättsföljder. Den som äger ett visst föremål får t.ex. rättsordningens stöd både när det gäller att hindra andra från att utnyttja detta föremål och för att få tillbaka föremålet från någon som orättmätigt har det i sin besittning. Men en vagt beskriven ”rätt till data” enligt ett avtal, i kombination med en osäkerhet kring underliggande (immateriella) rättigheter, gör det mer osäkert vad som gäller i en verkställighetssituation.

Det finns därför ofta ett behov att vara mer tydlig med vilka rättigheter som avses. Det kan t.ex. handla om en rätt att hindra andra motparten från att använda vissa datamängder eller om en skyldighet för ena parten att lämna ut vissa datamängder i samband med att avtalet avslutas. Skapandet av sådana regler kräver i sin tur en noggrann analys av såväl de aktuella datamängderna som respektive parts behov.

Det är ingen tvekan om att utvecklingen inom big data och maskininlärning gör frågan om ”rätten till data” allt mer aktuell. Bakom det till synes enkla uttrycket döljer sig emellertid en rad olika rätts- och policyfrågor, som måste analyseras var för sig. Det gäller såväl vid framtagandet av nya regelverk, som vid tillämpningen av det befintliga, t.ex. i avtalsrelationer.

Daniel Westman



Forbudet mot automatiserte avgjørelser – Paraplyen full av hull

Av Hermon M. Melles

Hermon Melles

Personvernforordningen er et ambisiøst forsøk på å ta igjen en tiltagende teknologisk utvikling, og søker å gi borgere tilbake kontrollen over egne personopplysninger. Politiske ambisjoner og retorikk lar seg imidlertid ikke alltid omsette i faktisk og juridisk realitet. Inntoget av automatiserte beslutningsprosesser, roboter og kunstig intelligens har laget hull i den paraplyen forordningen søker å være.

I norsk lovgivning har det eksistert en rett til informasjon om automatiserte avgjørelser siden personopplysningsloven av 2000 (§ 22). Den generelle personvernforordningen (GDPR) av 2016 har videreført, utvidet og skjerpet informasjonsplikten. Reguleringen inneholder imidlertid vesentlige svakheter. Spørsmålet er om denne reguleringen beskytter mot den teknologien som er i faktisk bruk i dag – automatiserte beslutningsverktøy.

1 Innledning

Begrepet «automatiserte avgjørelser» har et varierende meningsinnhold, og brukes generelt om avgjørelser tatt av autonome systemer/programmer som fungerer uten menneskelig innblanding. Personvernforordningen opererer imidlertid med en utvidet definisjon av automatiserte avgjørelser. Forordningens artikkel 22 nr. 1 definerer automatiserte avgjørelser som en «avgjørelse som utelukkende er basert på automatisert behandling». Avgjørelsen må videre ha «rettsvirkning» eller på «tilsvarende måte i betydelig grad» påvirke den registrerte.[1]

At avgjørelsen anses som automatisert er en forutsetning for at de registrerte kan påberope seg en rekke rettigheter overfor den behandlingsansvarlige. Disse rettighetene inkluderer blant annet rett på informasjon etter artikkel 13 nr. 2 (f) og 14 nr. 2 (g), rett til innsyn etter artikkel 15 nr. 1 (h) og den behandlingsansvarliges plikt til å gjennomføre egnede tiltak etter artikkel 22 nr. 3 ved automatiserte avgjørelser.[2] Grensedragningen mellom automatiserte og ikke-automatiserte avgjørelser er med andre ord av sentral betydning for flere informasjonsgivende rettigheter. Oppfyllelsen av disse rettighetene er videre i kjernen av prinsippet om den registrertes rett til en åpen og rettferdig behandling etter artikkel 5 nr. 1 (a).

> Inntoget av automatiserte beslutningsprosesser, roboter og kunstig intelligens har laget hull i den paraplyen forordningen søker å være

Det at avgjørelsen må basere seg «utelukkende» på automatisert behandling må forstås som at avgjørelsen må være tatt uten menneskelig

1 Etter bestemmelsen har den registrerte en «rett» til ikke å bli utsatt for denne typen automatiserte avgjørelser. EUs tidligere rådgivende organ i personvernspørsmål – Artikkel 29-gruppen – har imidlertid uttalt at bestemmelsen skal forstås som et forbud mot å fatte avgjørelser om fysiske personer som utelukkende baserer seg på automatisert behandling. Enkelte har i teorien stilt seg kritisk til dette standpunktet, sist i en artikkel av Dag Wiese Schartum i Lov & Data, hefte 2/2018m s. 4–7. Undertegnede vil imidlertid ikke gå nærmere inn på denne diskusjonen, og legger til grunn at bestemmelsen må forstås som et forbud, med bakgrunn i uttalelsen fra Artikkel 29-gruppen.

2 Den behandlingsansvarliges plikt til å gjennomføre egnede tiltak etter artikkel 22 nr. 3, forutsetter at den automatiserte avgjørelsen har sitt grunnlag i at behandlingen er «nødvendig for å inngå eller oppfylle en avtale mellom den registrerte og en behandlingsansvarlig», eller «er basert på den registrertes uttrykkelige samtykke», jf. GDPR artikkel 22 nr. 3.

involvering.[3] Artikkel 29-gruppen har i deres veileder om automatiserte avgjørelser poengtert at det ikke er adgang til å omgå bestemmelsens forbud ved at en ansatt rutinemessig ser over anbefalinger fra et automatisert system, uten at den ansattes rolle eller kontrollfunksjon er meningsfull.[4] Uttalelsen utvider dermed bestemmelsens virkeområde utover det som følger direkte av ordlyden, i den forstand at regelen også omfatter perifer menneskelig behandling i tiden forut for da den automatiserte avgjørelsen tas.

Artikkel 29-gruppen går ett steg lenger i veilederen ved å uttale at «[t]o qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analyses, they should consider all the relevant data".[5] Artikkel 29-gruppen snur tilsynelatende på utgangspunktet, slik at vurderingstema blir om den behandlingsansvarlige har en meningsfull rolle, og til dette ligger det en vurdering av om vedkommende innehar en reell adgang til å påvirke resultatet.

En forutsetning for at påvirkningsadgangen er reell virker å være at «beslutningstakeren» har tilgang til alle relevante opplysninger. Uttalelsen samsvarer med det som er lagt til grunn i forarbeidene til den tidligere personopplysningsloven:

> Dette innebærer at registrerte ikke har rett til informasjon om avgjørelser i tilfeller hvor det benyttes et automatisert beslutningsverktøy for å tilrettelegge grunnlaget for en avgjørelse tatt av et menneske med en reell påvirkningsadgang

«Dersom ett eller flere mennesker tar del i beslutningsprosessen, f.eks. ved å tolke resultatet av datamaskinbehandlingen, eller ved å kvalitetskontrollere dette, gjelder ikke bestemmelsen. Den manuelle delen av behandlingen må imidlertid være reell».[6] Det er nok legitimt å slutte ut fra dette at Artikkel 29-gruppens tolkning bygger på en konsekvensorientert tankegang, da forbudet mot automatiserte avgjørelser raskt vil kunne uthules dersom en plasserer mennesker til å utføre rutineoppgaver som i realiteten innebærer en omgåelse av regelen.

I teorien har enkelte stilt seg kritisk til de standpunktene som Artikkel 29-gruppen forfekter.[7] Det har blitt anført at uttalelsene til Artikkel 29-gruppen ikke kan tillegges stor betydning. Dette med bakgrunn i at de ikke er juridisk bindende, og at gruppen ble erstattet av Personvernrådet ved ikrafttredelsen av forordningen. Undertegnede er uenig i mye av denne kritikken. Når Personvernrådet har gitt sin tilslutning til samtlige av Artikkel 29-gruppens veiledere og har anledning til å utstede retningslinjer eller såkalt «best practices» tilsier dette at uttalelsene til gruppen er av stor faktisk betydning.[8] Uttalelsene gir i vesentlig grad uttrykk for hvordan datatilsynene i de ulike medlemslandene vil håndheve forordningen og gir en indikasjon på hvordan forordningen vil kunne tolkes av EU-domstolen i fremtidige avgjørelser.

2 Automatiserte beslutningsverktøy – systemene vi faktisk benytter

Automatiserte beslutningsverktøy er programmer/systemer som tilrettelegger grunnlaget for en avgjørelse tatt av et menneske. Med bakgrunn i økonomiske, tekniske, sosiale og en rekke andre faktorer, er de aller fleste virksomheter i dag på et stadium der de benytter automatiserte beslutningsverktøy – i motsetning til helautomatiserte beslutningssystemer.

Kravet om reell påvirkning innebærer at avgjørelser fattet ved hjelp av automatiserte beslutningsverktøy bare anses som «automatisert» etter forordningen dersom individet som tar den endelige avgjørelsen, *ikke* har en reell overprøvelsesadgang. Dette innebærer at registrerte ikke har rett til informasjon om avgjørelser i tilfeller hvor det benyttes et automatisert beslutningsverktøy for å tilrettelegge grunnlaget for en avgjørelse tatt av et menneske med en reell påvirkningsadgang.[9]

3 Se Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251) på s. 20.

4 Se Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251) på s. 21.

5 Se Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251) på s. 21.

6 Ot.prp. nr. 92 (1998 – 1999) 16, kapittel III Informasjon om behandling av personopplysninger, til § 22 rett til informasjon om automatiserte avgjørelser.

7 Se blant annet artikkel av Dag Wiese Schartum i Lov & Data, hefte 2/2018 på s. 4–7.

8 *«During its first plenary meeting the European Data Protection Board endorsed the GDPR related WP29 Guidelines».* Sitat hentet fra European Data Protection Board (EDPB) sin hjemmeside. (2018). Se også GDPR artikkel 70 nr. 1 (f) om Personvernrådets adgang til å utstede retningslinjer med hensyn til artikkel 22 og automatiserte avgjørelser.

9 Se Mendoza, Isak og Lee A. Bygrave, «The Right Not to Be Subject to Automated Decisions Based on Profiling», University of Oslo Faculty of Law Research Paper (No. 20), 2017, på s. 11.

Utgangspunktet om at en saksbehandler må ha en reell adgang til å påvirke resultatet av den automatiserte avgjørelsen, reiser imidlertid flere spørsmål enn det besvarer: Når må den menneskelige involveringen anses som så perifer at overprøvelsesadgangen ikke lenger er reell? Er for eksempel saksbehandlerens rolle fremdeles reell dersom den nærmest aldri benyttes?

Det er et stort behov for diskusjon rundt disse spørsmålene, ettersom sondringen er avgjørende for hvorvidt den registrerte får innsyn i en beslutningsprosess som er teknisk, lite gjennomsiktig og til tider av stor betydning. Artikkel 29-gruppen og deres etterfølger, Personvernrådet, har imidlertid gitt svært lite veiledning knyttet til disse spørsmålene.

3 Hvorfor er det viktig at definisjonen omfatter automatiserte beslutningsverktøy?

Det er flere betenkeligheter ved en definisjon av "automatiserte avgjørelser" der automatiserte beslutningsverktøy som et utgangspunkt faller utenfor. En kan her dra en parallell til bestemmelsene om habilitet i forvaltningslovens kapittel 2.[10] Etter forvaltningsloven § 6 første ledd er en offentlig tjenestemann inhabil til å "*tilrettelegge grunnlaget for en avgjørelse eller til å treffe avgjørelse*", dersom en eller flere inhabilitetsgrunner foreligger.

Alternativet "*tilrettelegge*" innebærer at også saksbehandlere som utelukkende deltar ved saksforberedelse og ikke har noen beslutningsmyndighet, vil kunne anses inhabile. I forvaltningslovens forarbeider er det henvist til en uttalelse av komiteen om dette: "Det er klart at tilretteleggelse av saken ofte kan øve en betydningsfull innvirkning på avgjørelsen. Allerede opplegget for det materiale som skal innhentes – eller ikke innhentes – kan i mange saker være utslagsgivende. Likedan kan den nærmere fremgangsmåte ved innsamlingen av saksmateriale ha vesentlig betydning; ikke minst rollen den spiller i forbindelse med kontroll og granskning. Det forberedende arbeidet vil ofte munne ut i forslag til vedtak i saken, og i mange tilfelle vil sjefens eller det kollegiale organs avgjørelse bare være en ren formsak".[11]

> "Dersom et automatisert system kontinuerlig innfrir, vil dette kunne resultere i at det bygges opp en sterk tillit til systemet

Overført til temaet automatiserte beslutningsverktøy, må mange av de samme hensynene kunne sies å gjøre seg gjeldende. Et særlig poeng er at avgjørelsen vil ha karakter av å være en formsak, noe som er fremtredende der en benytter seg av automatiserte beslutningsverktøy. Vi har større tillit til tilrettelegging foretatt av et automatisert system enn til tilrettelegging foretatt av et menneske.[12] Dersom et automatisert system kontinuerlig innfrir, vil dette kunne resultere i at det bygges opp en sterk tillit til systemet. Dette vil igjen kunne resultere i at avgjørelsene som fattes er identiske med systemets anbefalinger, og at det dermed *de facto* er tale om en "automatisert avgjørelse".[13]

Det er mulig at EU-domstolen i fremtiden vil foreta en avklaring vedrørende virkeområdet til artikkel 22 og de tilfeller der et menneske med overprøvelsesadgang tar de endelige avgjørelsene. Rettstilstanden per i dag må imidlertid være at bruk av automatiserte beslutningsverktøy faller utenfor artikkel 22 sitt primære nedslagsfelt.

4 Om adgangen til å oppstille en rett til informasjon/forklaring basert på forordningens prinsipper

Hensynet til en rettferdig og åpen behandling tilsier at det bør gjelde en rett til forklaring av avgjørelser der det benyttes automatiserte beslutningsverktøy i beslutningsprosessen. Dersom en slik rett ikke gjelder, vil de registrerte risikere å stå uten en *reell* mulighet til å utfordre den konkrete avgjørelsen.

Fraværet av en forklaringsrett i slike tilfeller vil innebære en krenkelse av det grunnleggende prinsippet om gjennomsiktighet i forordningen som er hjemlet i forordningens artikkel 5 nr. 1 bokstav a. Datatilsynet skriver om dette i sin rapport fra 2018, der de viser til at: "Selv om det ikke finnes en rett til forklaring når avgjørelsen ikke er automatisert, tilsier prinsippet om gjennomsiktighet at den behandlingsansvarlige bør gi en tilsvarende forklaring som ved automatiserte avgjørelser".[14] Denne uttalelsen er imidlertid ikke begrunnet, og ordlyden "bør" kan tolkes som et uttrykk for usikkerhet knyttet til

10 Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) 16. juni 2017 nr. 63.

11 Se Ot.prp.nr. 38 (1964 – 1965), Om lov om behandling av forvaltningssaker (forvaltningsloven), s. 44.

12 Se Kamarinou, Dimitira, Christopher Millard og Jatinder Singh, «The age of intelligent machines», *Data Protection and Privacy*, Vol. 10, ss. 89 –112, 2017, på s. 97.

13 Se Veale, Michael og Lilian Edwards, «Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling», *Computer Law & Security Review* Vol. 34 (No. 2), ss. 398 – 404, 2018, på s. 400.

14 Rapport fra Datatilsynet (2018), «Kunstig intelligens og personvern», januar 2018, på s. 21.

grunnlaget for å oppstille en slik regel fra datatilsynets side eller som uttrykk for en ren anbefaling uten et konkret rettslig innhold.

En slik rett til forklaring eksisterer i offentlig sektor. Det følger av forvaltningsloven – som den offentlige sektor er underlagt – at enkeltvedtak skal begrunnes. Etter forvaltningsloven §§ 24 og 25 skal den vedtaket retter seg mot få informasjon om hvilke regler og faktiske forhold vedtaket bygger på. I tillegg skal det gis informasjon om hvilke hovedhensyn som har vært avgjørende ved utøving av forvaltningsskjønn. Det skilles med andre ord ikke mellom tilfeller der det benyttes automatiserte beslutningsverktøy og der det er tale om en automatisert avgjørelse. Plikten til å begrunne vedtaket har som hensikt å gjøre det lettere for den vedtaket gjelder å forsone seg med utfallet, samt bedømme muligheten for omgjøring, enten ved klage eller på annen måte.[15]

Det foreligger ingen lovfestet klagerett i privat sektor. En kan likevel si at tilsvarende hensyn til forsoning med avgjørelsens utfall, innsikt i avgjørelsens riktighet, og informasjon om mulighetene for positivt utfall ved ny behandling er relevante også i privat sektor, om enn i noe mindre grad. Overføringsverdien av de nevnte hensyn tilsier at en tilsvarende rett bør foreligge der det treffes en avgjørelse ved bruk av automatiserte beslutningsverktøy.

Det er imidlertid uklart om man kan strekke de nevnte hensyn og prinsipper såpass langt at det på selvstendig grunnlag kan oppstilles en rett på forklaring av avgjørelser. Når henholdsvis lovgiver, Artikkel 29-gruppen og Personvernrådet ikke gir uttrykk for at en slik regel kan oppstilles, eller at det er adgang til å strekke definisjonen av automatiserte avgjørelser lenger enn det som allerede er lagt til grunn, har det formodningen mot seg at Datatilsynets standpunkt kan opprettholdes.

Undertegnede er her av den oppfatning at Datatilsynets anbefaling neppe er et uttrykk for gjeldende rett. Derfor mener jeg at rettstilstanden er at den registrerte ikke har rett på en forklaring der personopplysningene er behandlet ved bruk av automatiserte beslutningsverktøy og at individet som tar avgjørelsen har en reell rolle. Etter mitt syn bør det foreligge en sterkere rettskildemessig forankring enn det gjennomsiktighetsprinsippet alene konstituerer, for å foreta en slik utvidende tolkning av ordlyden til artikkel 22, eventuelt for å oppstille et selvstendig grunnlag for en slik regel. Det foreligger følgelig et "vakuum" i forordningen på dette punkt, der denne rettstilstanden innebærer et vesentlig innhugg i gjennomsiktighetsprinsippet i et samfunn hvor de fleste aktører per i dag hovedsakelig benytter automatiserte beslutningsverktøy. Dette innebærer at registrerte blir stående uten en rett til forklaring av disse avgjørelsene, da de anses som alminnelige ikke-automatiserte avgjørelser.

Uavhengig, vil de registrerte fremdeles ha en alminnelig rett til informasjon og innsyn i behold etter artikkel 13, 14 og 15. De nevnte bestemmelser gir imidlertid ikke den registrerte en rett på informasjon om den underliggende logikken til mennesket som har tatt avgjørelsen. Det antas at en slik rett ville hatt begrenset verdi, da det som (tidligere) skissert kan argumenteres med at avgjørelsen i realiteten fattes av det automatiserte beslutningssystemet.

5 Avslutning

En kan håpe at det ikke tar lang tid før man får en autorativ avklaring av spørsmålet om når menneskets rolle slutter å være reell i relasjon til artikkel 22 sin definisjon av automatiserte avgjørelser. Det er imidlertid klart at det vil være utfordrende å gi en slik avklaring, ettersom menneskets rolle blir mindre og mindre etterhvert som den teknologiske utviklingen tiltar. Man risikerer med andre ord at avklaringen går ut på dato kort tid etter at den blir gitt. Dag Wiese Schartum skriver i LoD (2018) at «[a]utomatiseringsgraden i norsk og mange andre lands forvaltning er høy og økende».[16]

> "Plikten til å begrunne vedtaket har som hensikt å gjøre det lettere for den vedtaket gjelder å forsone seg med utfallet, samt bedømme muligheten for omgjøring, enten ved klage eller på annen måte

Det er ingen overdrivelse å si at denne utviklingen holder et tilsvarende eller høyere tempo i privat sektor. Fremfor å forsøke å gi en avklaring på enkelte av disse spørsmålene – som raskt vil bli utdatert – mener jeg at løsningen bør være at den behandlingsansvarliges bruk av automatiserte beslutningsverktøy gir registrerte en rett på forklaring av det automatiserte beslutningsverktøysystemets underliggende logikk. En slik løsning vil forhindre en eventuell grensedragningsproblematikk, sikre forutberegnelighet for både behandlingsansvarlige og registrerte, samt lappe igjen enkelte av hullene i den paraplyen forordningen søker å være.

Hermon M. Melles er advokatfullmektig hos Advokatfirmaet Bing Hodneland, tilknyttet firmaets IT & media-avdeling. Artikkelen er en bearbeidet versjon av kapittel 5.4 i avhandlingen «Har vi rett til å få vite hva roboter tenker?».

15 Eckhoff, Torstein og Eivind Smith, «*Forvaltningsrett*», 11. Utgave, Oslo, 2018, på s. 287.

16 Se blant annet artikkel av Dag Wiese Schartum i Lov & Data, hefte 2/2018 s. 4 – 7.

När omfattas manuell hantering av personuppgifter av dataskyddsförordningen?

Av Martin Brinnen

Inledning

Dataskyddsregleringen omfattar behandling av personuppgifter som sker helt eller delvis automatiskt samt i vissa fall även manuellt om det sker i ett ”register”. Begreppen som används för att avgränsa tillämpningsområdet – ”personuppgift”, ”behandling” och ”register” – är emellertid mycket vaga. Många gånger framstår det som omöjligt att utifrån en tolkning av dessa begrepp och med någon form av bestämdhet kunna fastställa regleringens yttre gränser.

Det är en brist i regelverket men till viss del en avsedd sådan. Liksom så många gånger annars vid tillämpningen av dataskyddsförordningen är avsikten att en bedömning måste göras med hänsyn till syftet med regleringen och omständigheterna i det enskilda fallet samt med beaktande av att regelverket är avsett att skydda fysiska personers grundläggande rättigheter och frihet, särskilt deras rätt till skydd för personuppgifter. Att fastställa tillämpningsområdet av dataskyddsförordningen handlar således inte enbart om en text- och begreppsanalys utan lika mycket en tolkning av syftet och bedömning av omständigheterna i det enskilda fallet.

Detta förhållande leder ofta till stora praktiska problem för organisationer som sitter med omfattande samlingar av information som kan innehålla personuppgifter, särskilt när det handlar om äldre arkiv i pappersform.

Trots att dataskyddsregleringens tillämpning på manuell behandling har diskuterats under en längre tid är rättsläget oklart. Av den anledningen väcktes förhoppningar om att EU-domstolen skulle klargöra tillämpningsområde i denna del när domstolen i juli 2018 uttalade sig om bl.a. pappersbaserad insamling av personuppgifter i samband med predikoarbete i sin dom C-25/17 Jehovan todistajat (Jehovas vittnen).[1]

Martin Brinnen

I denna artikel analyseras vad EU-domstolens dom innebär för rättsläget när det gäller dataskyddsförordningens[2] tillämpning på manuell behandling av personuppgifter. Därutöver redovisas ett förslag om hur man bör resonera kring tillämpningen av dataskyddsförordningen på manuell behandling av personuppgifter.

Sammanfattningsvis är bedömningen att EU-domstolen har breddat tillämpningsområdet av dataskyddsregleringen jämfört med vad som ansetts gälla tidigare enligt svensk rätt. Med anledning av domen, men även av praktiska skäl, finns det därför anledning att ta ett mer generellt grepp på all behandling av personuppgifter inom en organisation oavsett om den utförs automatiskt eller manuellt i ett kartotek, filsystem, i en anteckningsbok eller muntligt.

Aktuella bestämmelser i dataskyddsregleringen

Dataskyddsförordningen ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register (art. 2.1). Med register avses en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden (art. 4.6).

EU-domstolens dom avsåg bedömning enligt dataskyddsdirektivet. Bestämmelsen om manuell behandling av personuppgifter i dataskyddsdirektivet (art. 3.2 andra strecksatsen) samt definitionen av begreppet register med personuppgifter (art. 2 c) överensstämmer i huvudsak med motsvarande bestämmelser i dataskyddsförordningen. För förståelsen av domen är det även väsentligt vad som anges i skälen 15 och 27 i dataskyddsdirektivet.

Som framgår av skäl 27 medgav dataskyddsdirektivet en viss frihet för medlemsstaterna att närmare de-

1 Dom av den 10 juli 2018, Jehovan todistajat, C-25/17, ECLI:EU:C:2018:551.

2 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). Härefter ”dataskyddsförordningen”.

finiera tillämpningsområdet på manuell behandling. Den numera upphävda personuppgiftslagen var emellertid avsedd att ha samma tillämpningsområde som dataskyddsdirektivet även om begreppet register inte användes i lagtexten.[3] I stället infogades dataskyddsdirektivets definition av register i lagtexten som således gällde ”strukturerad samling” (5 § andra stycket). Lagtexten utformades dock med vissa till synes mindre avvikelser från formuleringen i dataskyddsdirektivet. Avvikelserna har dock betydelse för förståelsen av EU-domstolens dom och kan till viss del medfört att personuppgiftslagen har fått ett något mer inskränkt tillämpningsområde jämfört med hur dataskyddsdirektivet har tolkats i andra EU-länder. Jag återkommer till denna fråga nedan.

Dessvärre har den från dataskyddsdirektivet avvikande formuleringen i personuppgiftslagen av någon okänd anledning överförts till den svenska versionen av dataskyddsförordningen. Den svenska versionen innehåller således en översättning som inte fullt ut överensstämmer med den engelska versionen av dataskyddsförordningen.

Definitionen av begreppet register i de engelska versionerna av dataskyddsdirektivet respektive dataskyddsförordningen är däremot identiska. Mot den bakgrunden bör EU-domstolens uttalanden i domen om manuell behandling kunna läggas till grund för en tolkning av dataskyddsförordningen. Det bör dock noteras att skälen i dataskyddsförordningen som gäller tillämpningen av dataskyddsförordningen på manuell behandling av personuppgifter är mer kortfattade.

Tidigare tolkning av personuppgiftslagen

Från tiden med personuppgiftslagen finns det ett antal avgöranden och uttalanden i förarbeten som inte gav något entydigt svar på när lagen skulle tillämpas på manuell behandling av personuppgifter.[4]

> Sammanfattningsvis är bedömningen att EU-domstolen har breddat tillämpningsområdet av dataskyddsregleringen jämfört med vad som ansetts gälla tidigare enligt svensk rätt

Att samlingen ska vara tillgänglig enligt ”*särskilda kriterier*” (pluralis) har med stöd av ett uttalande av Datalagskommittén (SOU 1997:39 s. 340) tolkats som att samlingen ska vara sökbar på minst två kriterier. Till det kommer att Regeringsrätten (numera Högsta förvaltningsdomstolen) i RÅ 2001 ref. 35, förvisso utan uttrycklig hänvisning till tvåkriterieregeln, har bedömt att ett antal betygshandlingar sorterade först utifrån efternamn och därefter utifrån betygsgenomsnitt, dvs. endast en sökväg vid varje tillfälle, inte utgör ett register. Regeringsrätten ansåg bl.a. ”att en sortering av ett antal dokument i en viss ordning inte utan ytterligare åtgärder kan anses uppfylla det i lagtexten angivna kravet.”

Som jag återkommer till nedan innebär EU-domstolens dom att dessa uttalanden inte ensamt kan läggas till grund för tolkningen av dataskyddsdirektivet och dataskyddsförordningen.

EU-domstolens uttalande om manuell behandling

Bakgrunden till EU-domstolens dom var den uppsökande verksamhet som medlemmar i Jehovas vittnen i Finland ägnade sig åt genom att besöka personer i sina hem (dörrknackning). I samband med sådana besök förde medlemmarna minnesanteckningar om bl.a. namn, adress, sammanfattningar av samtal med de besökta personerna, samt deras religiösa övertygelse och familjeförhållanden. Anteckningarna som fördes på papper var avsedda att kunna användas för förberedelser inför senare besök och att administrera en förteckning (”förbudslistan”) över personer som inte önskar bli besökta av Jehovas vittnen.

Högsta förvaltningsdomstolen i Finland begärde förhandsavgörande från EU-domstolen och ställde bl.a. frågan om begreppet ”register” i artikel 2 c dataskyddsdirektivet ska tolkas så att det omfattar en samling av personuppgifter som samlats in inom ramen för predikoarbete genom dörrknackning, som innefattar namn, adress och ytterligare information om de besökta personerna, när dessa uppgifter i praktiken kan erhållas med lätthet för senare användning, eller om denna samling, för att omfattas av detta begrepp måste bestå av register, särskilda förteckningar eller andra arrangemang för sökning. Högsta förvaltningsdomstolen angav att samfundet Jehovas vittnen hade gett anvisningar till medlemmar om hur anteckningarna ska göras, att samfundet och dess församlingar organiserade och samordnade sina medlemmars predikoarbete genom dörrknackning. Samfundets församlingar administrerade dessutom en förteckning över personer som inte vill bli besökta av predikande medlemmar i den s.k. förbudslistan.

EU-domstolen konstaterar inledningsvis att dataskyddsdirektivet var är avsett att vara teknikneutralt för att undvika risken för att skyddet enligt direktivet kringgås (p. 53) och att begreppet ”register” måste ges en vid definition, särskilt eftersom det anges att den omfattar ”varje” strukturerad samling av personupp-

3 Prop. 1997/98:44 s. 40.

4 För en utförlig redovisning av rättsläget enligt personuppgiftslagen hänvisas till Personuppgiftslagen – En kommentar, Öman och Lindblom, Zeteo, publicerad 2018-02-16, kommentar till 5 §.

gifter (p. 56). Det bör noteras att den svenska versionen av dataskyddsförordningen i denna del (art. 4.6) anger ”*en* strukturerad samling” (min kursivering). Som nämnts ovan är det en formulering som även återfinnas i 5 § andra stycket personuppgiftslagen. Av personuppgiftslagen och den svenska versionen av dataskyddsförordningen kan man således felaktigt få uppfattningen att begreppet register ska tolkas mer begränsat.

När det gäller de ”särskilda kriterier” som ska ligga till grund för strukturering av en samling av personuppgifter enligt definitionen av register enligt artikel 2 c dataskyddsdirektivet (jfr art. 2.1 dataskyddsförordningen) konstaterar domstolen att bestämmelsen är oklar. Med hänvisning till att det framgår av skäl 27 i dataskyddsdirektivet att dessa kriterier måste ”[avse] enskilda personer”, fann domstolen att kravet på att samlingen av personuppgifter måste vara strukturerad efter bestämda kriterier ”endast syftar till att göra uppgifter om en person lätt tillgängliga” (p. 57). Exakt vilka kriterier eller vilken form – särskilda kartotek, förteckningar eller någon annan form av sökbart system – är betydelselöst så länge som informationen i praktiken kan erhållas med lätthet, tillade domstolen (p. 61).

Domstolen konstaterade också att de personuppgifter som är samlats in av Jehovas vittnen var strukturerade enligt kriterier som var knutna till syftet med insamlingen av uppgifterna, dvs. att förbereda senare besök och att administrera förteckningen över personer som inte önskar bli besökta, den s.k. förbudslistan. Kriterierna, bl.a. namn, adress, övertygelser har enligt domstolen valts ut på ett sådant sätt att informationen som en bestämd person kan erhållas med lätthet (p. 60).

Med dessa skäl ansåg EU-domstolen att frågan från den finska Högsta förvaltningsdomstolen skulle bevaras med att begreppet register i dataskyddsdirektivet ska tolkas så att det omfattar en samling av personuppgifter ”när dessa uppgifter i praktiken kan erhållas med lätthet för senare användning”. Domstolen tillägger att ”[d]enna samling behöver […] inte innehålla register, särskilda förteckningar eller andra arrangemang för sökning.”

Analys av domen

EU-domstolen gör en vid tolkning av begreppet register

EU-domstolens bedömning, i skälen och domslutet, innebär sammanfattningsvis att dataskyddsdirektivet är tillämplig på manuell behandling av personuppgifter om det är lätt att ta fram personuppgifterna efter en sökning på just personuppgifter och att det därvid saknar betydelse hur samlingen av personuppgifter har utformats (register, förteckning etc.) och vilka personuppgifter som har gjorts sökbara.

EU-domstolen gör en vid tolkning begreppet register och det materiella tillämpningsområdet för manuell behandling av personuppgifter. Den innebär i princip att även enkla pärmregister och liknande sammanställningar av personuppgifter kan komma att omfattas av dataskyddsförordningen. Det finns inget i domen som anger att det krävs någon mer avancerad sökfunktion eller att det skulle krävas att personuppgifterna är sökbara på flera än ett sökkriterium, t.ex. att handlingar sorterade på namn i bokstavsordning. Det tycks över huvud taget inte vara nödvändigt med någon sökfunktion t.ex. ett index (se sista meningen i domslutet ”För att omfattas av detta begrepp behöver denna samling inte innehålla register, särskilda förteckningar eller *andra arrangemang för sökning*.” min kursivering).

Man skulle kunna uttrycka det så att EU-domstolen gör en ändamålsinriktad tolkning som utgår från funktionen, dvs. att det ska vara lätt att återfinna personuppgifterna. Det har således mindre betydelse hur en viss samling av personuppgifter är organiserad t.ex. om det finns en eller flera sökkriterier eller liknande. Någon form av organisation får dock antas vara nödvändig för att uppfylla domstolens krav på att ”uppgifter i praktiken kan erhållas med lätthet för senare användning”. Personuppgifter som förekommer utan någon särskild organisation i löpande text bör t.ex. inte omfattas.

Syftet med bestämmelsen kan ge viss vägledning

EU-domstolen svarar inte på *hur enkelt* det måste vara att söka fram personuppgifter för att en samling av personuppgifter ska omfattas av dataskyddsdirektivet. Det måste emellertid finnas någon form av kvalificering för att en samling av personuppgifter ska omfattas.

Det övergripande syftet med dataskyddsregleringen är visserligen att skydda enskildas friheter och rättigheter vid behandling av deras personuppgifter. Men det centrala tillämpningsområdet är avgränsat till automatiserad behandling. Skälet till denna avgränsning kan antas vara de särskilda integritetsrisker som uppkommer till en följd av datorteknikens förmåga att snabbt, enkelt och billigt söka och sammanställa stora mängder personuppgifter.

Vad avser manuell behandling av personuppgifter är tillämpningsområdet avgränsat till strukturerade samlingar av personuppgifter. Skälen till dataskyddsdirektivet ger ingen entydig bild av vad syftet är med denna avgränsning (se bl.a. skäl 27). Syftet kan vara att undvika kringgående och att för detta syfte har regleringen utformats teknikneutralt. En mer trolig tolkning är dock att avsikten är *dels* att undvika kringgående av bestämmelserna, *dels* att skapa ett teknikneutralt skydd för enskildas personuppgifter. Det betyder att tillämpningen på manuell behandling inte är begränsad till de fall då det finns en tydlig avsikt

> Domen kan läsas som att domstolen går längre än vad som är nödvändigt för ett sådant syfte och att därmed skapar ett mer generellt integritetsskydd för manuell behandling av personuppgifter än vad som kan motiveras av dataskyddsregleringen

att kringgå regleringen. EU-domstolen tycks i vart fall utgå från den senare tolkningen. Å andra sidan är skyddet inte avsett att vara så teknikneutralt att det omfattar all manuell behandling av personuppgifter utan gäller endast behandling i strukturerade samlingar av personuppgifter. Mot den bakgrunden ligger det nära till hands att anta att syftet är att dataskyddsregleringen ska omfatta sådan manuell behandling som medför liknande integritetsrisker som typiskt sett uppkommer vid automatiserad behandling.[5]

Det kan emellertid diskuteras om ett sådant syfte har varit vägledande för EU-domstolens vida tolkning av begreppet register. Domen kan läsas som att domstolen går längre än vad som är nödvändigt för ett sådant syfte och att därmed skapar ett mer generellt integritetsskydd för manuell behandling av personuppgifter än vad som kan motiveras av dataskyddsregleringen.

Dataskyddsförordningen innehåller bestämmelser om tillämpningsområdet som i stort sett överensstämmer med dataskyddsdirektivet. I skälen till dataskyddsförordningen har dock vissa förändringar gjorts som kan tyda på att man vill betona att kringgåendesyftet är avgörande för tillämpningen på manuell behandling (jfr skäl 27 i dataskyddsdirektivet med skäl 15 i dataskyddsförordningen). Men det är oklart om dessa förändringar är avsedda att medföra en saklig förändring.

Syftet med sammanställningen kan ha betydelse

EU-domstolen noterar att de insamlade personuppgifterna i målet är strukturerade enligt kriterier som är knutna till syftet insamlingen. (p. 60). Domstolen tycks mena att om syftet är att det ska gå lätt att återfinna personuppgifter är det en faktor som talar för att samlingen omfattas av dataskyddsdirektivet.

Finska Högsta förvaltningsdomstolen uttryckte det möjligen tydligare när den meddelade sin dom i målet (HFD 2018:171).

> *Även om metoderna för antecknande och ordnande av personuppgifter som enskilda Jehovas vittnen följde kunde variera, hade det till vissa delar inte överhuvudtaget varit meningsfullt att föra anteckningar om de inte med det samma hade ordnats på så sätt att det med lätthet var möjligt att erhålla uppgifter gällande en särskild person och dennes adress.*

Vad som gäller om det inte finns ett syfte att söka fram personuppgifter ur en samling av personuppgifter men det ändå är möjligt, ger inte EU-domstolens dom svar på.

Riskerna med och ändamål för den aktuella behandlingen saknar betydelse

Bestämmelserna om tillämpningsområdet i dataskyddsförordningen ger inte intryck av att ändamålet med en viss behandling eller vilka personuppgifter som behandlas har betydelse för tolkningen av tillämpningsområdet vid manuell behandling. Avgörande är endast hur de har strukturerats. Det bör således sakna betydelse om det t.ex. handlar om känsliga personuppgifter, en omfattande kartläggning av en person eller anteckningar som ett stort antal personer, så länge uppgifterna inte är strukturerade på ett sådant sätt att de är ”tillgängliga enligt särskilda kriterier”.

Av EU-domstolens slutsats i domen kan man dock få en annan uppfattning. Domstolen anger att begreppet register omfattar en samling av personuppgifter ”som samlats in inom ramen för predikoarbete genom dörrknackning, som innefattar namn, adress och ytterligare information om de besökta personerna”. Det är en formulering som ingår i finska Högsta förvaltningsdomstolens fråga till EU-domstolen och som brukligt formulerar EU-domstolen svaret så nära fråga som möjligt. Det bör inte tas till grund för att EU-domstolen har vägt in dessa faktorer i bedömning av vilken manuell behandling som omfattas av dataskyddsdirektivet.

Med det sagt kan man inte bortse ifrån att dataskyddsregleringen ska tolkas utifrån ändamålen med regleringen och särskilt syftet att den utgör en skyddsreglering för den enskilde. Det finns därför anledning att anta att en mer riskfylld behandling av personuppgifter oftare anses omfattas av tillämpningsområdet än en behandling som knappast innebär några integritetsrisker alls. Detta går dock inte att utläsa av bestämmelserna men kan bli resultatet av EU-domstolens ändamålstolkning.[6]

Praktiska konsekvenser av domen

Ett bredare tillämpningsområde

Den vida tolkning som EU-domstolen som gör av begreppet register går till viss del emot den utveckling som har skett i svensk rätt enligt vilken det har ställts högre krav på

5 Jfr prop. 1997/98:44 s. 40. Se även Se även Peter Seipels yttrande såsom det refereras i RÅ 2001 ref. 35 och Artikel 29-gruppens yttrande 4/2007 om begreppet personuppgifter (WP136) s. 5.

6 Jfr t.ex. Google Spain-domen (C-131/12) p. 58.

strukturering för att manuell behandling skulle omfattas av personuppgiftslagen. Konsekvensen av domen är således att flera manuella behandlingar omfattas än vad som tidigare ansett gälla enligt personuppgiftslagen. Vilka manuella behandlingar av personuppgifter som omfattas av dataskyddsregleringen är fortfarande oklart men domen innebär att organisationer som har omfattande manuella arkiv bör genomföra en förnyad genomgång i syftet att identifiera manuella behandlingar som tidigare inte ansågs omfattas av personuppgiftslagen men som nu kan omfattas av dataskyddsförordningen.

Domen innebär inte att tidigare tolkningar enligt personuppgiftslagen har förlorat sin betydelse. Men till dessa tolkningar bör läggas den funktionellt inriktade tolkning som EU-domstolen gjorde. Sammanfattningsvis talar följande förhållanden för att personuppgifter ”i praktiken kan erhållas med lätthet för senare användning” och därmed omfattas av dataskyddsförordningen.

- Det är möjligt att söka fram personuppgifter med *minst två sökkriterier* omfattas normalt, t.ex. ett pärmregister sorterat på efternamn och som kompletteras med ett index som gör det möjligt att även söka på personnummer.
- Det finns en avsikt med samlingen att enkelt kunna söka fram personuppgifter.
- Det finns ett syfte att kringgå reglerna i dataskyddsförordningen.
- Sökmöjligheterna är sådana att de påminner om de som finns vid automatiserad behandling.

Med EU-domstolens funktionellt inriktade tolkning bör den hjälpregeln – ”the temp test” – som tillsynsmyndigheten i Storbritannien, Information Commissioner’s Office (ICO), tidigare använt sig av vara ett lämpligt sätt att åtminstone preliminärt avgörande om den manuella behandlingen omfattas av dataskyddsförordningen. ”The temp test” innebär att man utför en hypotetisk test. Testet innebär att en samling av personuppgifter omfattas av dataskyddsregleringen om en tillfälligt anställd administrativ assistent kan ta fram personuppgifter från en samling av personuppgifter utan någon särskild kunskap om verksamheten eller de dokument som verksamheten hanterar. Testet förutsätter att assistenten har en rimlig kompetensnivå och endast får en kort introduktion eller beskrivning till det aktuella filsystemet e.d.

Generell riskbedömning för all behandling av personuppgifter

I förhållande till tillsynsmyndigheten och vid en eventuell tvist är det förstås väsentligt att kunna göra en tydlig avgränsning av vad som omfattas av dataskyddsregleringen. Gentemot den registrerade och inte minst för allmänhetens förtroende är det emellertid viktigt att ha en heltäckande strategi för hantering av personuppgifter. Ursäkten att en viss manuell behandling inte omfattades av dataskyddsförordningen är troligen inte särskild hållbar om en allvarlig incident inträffar. Även av andra skäl finns det behov av att organisationen har god kontroll över hur samtliga informationsresurser hanteras inom organisationen.

Från ett generellt integritetsskyddsperspektiv kan det därför vara lämpligt att utgå från en heltäckande riskbedömning. Beroende på omfattning och inriktning av verksamheten bör en organisation ha en generell policy för att skydda personuppgifter oavsett hur de behandlas – automatiserat i it-system, manuellt på papper eller muntligen. En sådan bedömning kan även krävas för att uppfylla andra regelverk än dataskyddsförordningen t.ex. bestämmelser om sekretess och tystnadsplikt, eller för att skydda värdefull information.

Delvis automatiserad behandling

Manuell behandling av personuppgifter kan även förekomma som ett led i en annars automatiserad behandling och därmed omfattas av dataskyddsförordningen såsom delvis automatiserad behandling. Som exempel kan nämnas en enkät som samlas in genom intervjuer på stan, antecknas på papper för att sedan föras in i ett it-baserat register. Ett annat exempel är utskrifter från ett it-baserat register.

Alla delvis automatiserade behandlingar omfattas dock inte av dataskyddslagstiftningen, utan det krävs att de manuella inslagen utgör ett naturligt led i den annars automatiserade behandlingen.[7] Observera att i dessa fall behöver den manuella delen av behandlingen inte vara en del av en strukturerad samling av personuppgifter. I princip kan en papperslapp med en handskriven notering avseende en person vara ett led i en annars automatiserad behandling. Det kan därför vara svårt att vid en snabb blick avgöra om personuppgifterna omfattas av dataskyddsregleringen. I praktiken torde dock syftet med den manuella behandlingen framgå av sammanhanget t.ex. anteckningar i ett pappersformulär. För den som ägnar sig åt mer organiserad manuell insamling av personuppgifter kan det dock vara att rekommendera att det framgår av blanketter m.m. att det handlar om behandling av personuppgifter som omfattas av dataskyddsregleringen.

När det gäller helt manuell behandling av personuppgifter kan muntlig och annan icke strukturerad behandling omfattas om den utförs i ett förled till den strukturerad behandling, dvs. om uppgifterna är avsedda ingå i ett register.

Martin Brinnen är dataskyddsexpert verksam som senior specialist vid Advokatfirman Kahn Pedersen.

7 Personuppgiftslagen – En kommentar, Öman och Lindblom, Zeteo, publicerad 2018-02-16, kommentar till 5 § första stycket. Se även Peter Seipels yttrande såsom det refereras i RÅ 2001 ref. 35.

JUSNYTT

Halvor Manshaus

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

Retten til å bli glemt – utenfor EU

I en uttalelse fra januar 2019 har Generaladvokaten i en sak vurdert rekkevidden av «retten til å bli glemt», der spørsmålet er hvor langt regelen rekker utenfor EU-området. EU-domstolen forventes å nedkomme med sin vurdering i løpet av inneværende år.

Retten til å bli glemt er tidligere slått fast av EU-domstolen og fulgt opp i personvernforordningen artikkel 17, og det kan være greit med en kort oppsummering av hva dette gjelder:

Våren 2014 ga EU-domstolen i storkammer en prejudisiell avgjørelse i tvisten mellom Google og Spania om avindeksering av opplysninger knyttet opp mot en konkret person, ref sak C-131/12. Begrepet avindeksering er gjennomgående benyttet i omtalen av saken, blant annet hos Datatilsynet (*https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/hvordan-slette-soketreff/*):

«Som enkeltperson kan du be om at søkemotorer fjerner søketreff som dukker opp ved søk på navnet ditt (avindeksering).

Det er EU-domstolen som har avgjort dette, og det følger også av personvernforordningen artikkel 6 bokstav f.»

Avindeksering innebærer ikke nødvendigvis at den underliggende informasjonen slettes som sådan, men det skal gjøres en avkobling mellom en persons navn og lenkene i resultatlisten som kommer opp ved søk på dette navnet. Dette fremgår av slutningen i den prejudisielle avgjørelsen C-131/12, avsnitt 100, der det heter under punkt 3 at tilbyderen av søketjenesten:

"…er forpliget til fra den resultatliste, der vises efter en søgning på en persons navn, at fjerne link til websider, som er offentliggjort af tredjemand og indeholder oplysninger vedrørende denne person, også i det tilfælde, hvor dette navn eller disse oplysninger ikke forudgående eller samtidig slettes fra disse websider, og i givet fald selv når offentliggørelsen på disse sider i sig selv er lovlig."

Det vil altså i prinsippet fortsatt være mulig å søke frem den aktuelle informasjonen, men ikke med utgangspunkt i omtaltes navn som søkeord. Det samme gjelder for automatisk genererte søkeforslag koblet sammen med personnavn, eksempelvis der man har skrevet inn et navn og søkefeltet har funksjon for autofullføring som foreslår søkeord som vil lede til nettopp den informasjon som skal avindekseres.

Det er verdt å merke seg at et krav om avindeksering ikke forutsetter rettsstridig publisering av den aktuelle informasjonen på nettstedet hos den tredjepart som resultatlisten viser til. Dersom denne tredjepart er en nettavis, med en artikkel som ikke i seg selv er rettsstridig, kan søkemotoren likevel pålegges å avindeksere søk koblet opp mot omtaltes navn som søkeord. Det er denne mekanismen som gir betegnelsen «retten til å bli glemt». Arkiverte artikler og saker kan ligge uten å bli slettet hos den publiserende tredjepart, men sammenkoblinger av navn og sak som gjør det enkelt å søke opp historikk på enkeltpersoner skal kobles fra hverandre. På denne måten oppstilles det således en begrenset rett til å få sitt navn som søkeord frakoblet opplysningene i den aktuelle saken.

«Retten til å bli glemt» er ikke i seg selv automatisk, det må gjøres en konkret vurdering. I saker med sterk og aktuell allmenn interesse eller der andre forhold gjør det betenkelig å innskrenke tilgangen til informasjon, vil søkemotoren kunne nekte å koble fra navnet på den omtalte.

Rent praktisk vil man som regel først kontakte det nettstedet som opprinnelig har publisert informasjonen. Dersom personnavnet på denne bakgrunn fjernes fra nettsidens innhold eller legges inn på et område der søkemotorene ikke har tilgang, vil søkemotorenes resultatlister normalt være tilsvarende oppdatert etter bare noen dager. Man har også anledning til å klage direkte til søkemotoren, som da vil gjøre en slik konkret vurdering som omtalt ovenfor. Det europeiske personvernråd (tidligere Artikkel 29-gruppen) er EU-kommisjonens rådgivende organ innen personvernspørsmål og har laget egne retningslinjer for denne vurderingen. Fører ikke klagen frem kan man gå til Datatilsynet som neste instans. Det er altså andre alternativer enn å gå

direkte til domstolene for å kreve avindeksering. Etter 29. mai 2014 har Google ifølge egne «transparency reports» mottatt over 750.000 klager med krav om å avindeksere informasjon fra resultatlisten, samt litt under 3 millioner krav om å fjerne konkrete internettadresser.

I en ny sak for EU-domstolen har generaladvokaten avgitt en uttalelse om den geografiske rekkevidden av «retten til å bli glemt». Saken står mellom Google og den franske kommisjonen for informatikk og rettigheter (CNIL, i praksis det franske datatilsynet). Utgangspunktet for saken er et krav fra CNIL om at Google skulle utføre avindeksering globalt, altså ikke bare Google-domener innen EU. Google inntok et motsatt standpunkt, og anførte at det måtte være tilstrekkelig å avindeksere kun på domenenavn som korresponderte til medlemsstatene innen EU, for eksempel .fr, .es, .com, .uk, osv. CNIL svarte med å gi Google en bot på 100.000 Euro. Googles klagesak håndteres av klageinstansen Conseil d'État, som besluttet å henvise prejudisielle spørsmål knyttet til den territorielle rekkevidden av «retten til å bli glemt» til EU-domstolen.

I løpet av denne prosessen kom Google med en mer nyansert anførsel, der det ble lagt opp til såkalt geoblocking. I dette ligger at alle som utfører et søk innenfor EU-området vil motta en avindeksert resultatliste, uavhengig av domenenavnet som benyttes av denne brukeren. Dette betyr at en norsk borger vil få en avindeksert resultatliste enten han søker på google.no eller google.com, det er IP-adressen og domenet det søkes fra som bør bestemme rekkevidden av EU-kravet til avindeksering.

Generaladvokat Maciej Szpunar har i sin anbefaling til EU-domstolen vist til at «retten til å bli glemt» innebærer en avveining av flere kryssende fundamentale rettigheter, herunder personvernet vurdert opp mot allmennhetens legitime interesse i tilgang til informasjon. Som utgangspunkt vises det til at EU-retten ikke gir anvisning på den territorielle rekkevidden av regelen, slik at det må være avgjørende hvor selve søket utføres rent geografisk. I dette ligger at et søk utført utenfor EU ikke skal være omfattet av en avindeksering pålagt innenfor EU-området. Søkeren skal dermed kunne søke på den omtaltes navn og få opp en ordinær og uredigert resultatliste. Generaladvokaten legger stor vekt på den omtalte avveiningen av de fundamentale rettigheter, som vil kunne være ulikt fra jurisdiksjon til jurisdiksjon. Det fremheves i hans uttalelse at anvendelse utenfor EU ville kunne innebære at personer utenfor EU dermed på sviktende grunnlag ville risikere å bli forhindret fra å motta informasjon. Dette ville samtidig innebære en risiko for at fremmede stater forhindrer EU-borgere å motta informasjon som stammer fra utenfor EU-området, med alvorlige konsekvenser for ytringsfrihet på Internett, ref. uttalelsen avsnitt 61:

"Endvidere vil der derfor være fare for, at Unionen hindrer personer i tredjelande i at få adgang til oplysningerne. Hvis en myndighed i Den Europæiske Union kunne anordne en global fjernelse af links, ville det sende et fatalt signal til tredjelandene, som ligeledes kunne anordne en fjernelse af links i medfør af deres egne love. Lad os antage, at nogle tredjelande af en eller anden grund fortolker visse af deres love således, at de hindrer personer, der befinder sig i en EU-medlemsstat, i at få adgang til en oplysning, der søges. Der ville da være en reel risiko for et kapløb mod laveste fællesnævner på bekostning af ytringsfriheden på europæisk og globalt plan."

Generaladvokat Szpunar utelukker ikke at det kan oppstå helt spesielle situasjoner der det kan oppstå et legitimt behov for global anvendelse av en avindeksering, og tar forbehold om at en slik situasjon kan oppstå. Ettersom hans konklusjon var at den nærværende saken ikke åpnet for noen slik diskusjon, utdyper han ikke dette synspunktet noe nærmere. Dette er et punkt som EU-domstolen kanskje vil si noe mer om når den nedkommer med sin prejudisielle uttalelse.

Konklusjonen så langt er altså at Szpunar slår fast at «retten til å bli glemt» ikke får anvendelse på søk utført utenfor EU, men det er gjort et lite kompromiss ved at generaladvokaten har sett hen til Googles argumentasjon knyttet til geoblocking. Han mener dette må inngå som en del av kravet til avindeksering, slik at man innenfor EU-området får en mer effektiv håndtering (ref. avsnitt 79 i uttalelsen):

"I denne forbindelse har udbyderen pligt til at træffe enhver foranstaltning, som vedkommende har til rådighed, til at sikre en effektiv og fuldstændig fjernelse af links. Dette indbefatter bl.a. anvendelsen af den såkaldte geoblokeringsteknik i forhold til en IP-adresse, som antages at være lokaliseret i en hvilken som helst af de medlemsstater, der er omfattet af direktiv 95/46, uafhængigt af, hvilket domænenavn den internetbruger, der udfører søgningen, anvender."

Det er vanskelig å se at EU-domstolen skal kunne gå stort lenger når det gjelder den direkte rekkevidden av «retten til å bli glemt» utenfor EUs grenser. Samtidig er det rom for en del presiseringer med utgangspunkt i generaladvokatens uttalelse, spesielt knyttet til en nærmere anvisning for tilfeller der en global avindeksering vil kunne være aktuelt. Det er heller ikke gitt at EU-domstolen vil slå seg til ro med at geoblocking er et tilstrekkelig effektivt virkemiddel, ettersom dette enkelt kan unngås for brukere av VPN-tjenester som kamuflerer den reelle IP-adressen til brukeren.

Gorrissen Federspiel

Tue Goldschmieding

1. Det danske finansministerium fastslår, at Danmarks Digital Post-løsning er omfattet af den danske "Krigsregel" og derfor ikke må forlade Danmark

Det danske finansministerium ('Finansministeriet') har den 29. april 2019 offentliggjort sit svar på Finansudvalgets spørgsmål nr. 542 af 5. april 2019 om, hvorvidt det i forbindelse med gen-udbuddet af digital post løsningen er tilladt at opbevare personoplysninger i udlandet. Finansministeriet fastslår i sit svar, at *Digital Post-løsningen* er omfattet af den særlige danske *krigsregel,* og at den nye leverandør af løsningen ikke må opbevare kritiske dele af løsningen uden for Danmarks grænser.

Den danske databeskyttelseslov indeholder i § 3, stk. 9 den såkaldte *krigsregel,* der giver Justitsministeren og den relevante ressortminister, (i dette tilfælde den danske innovationsminister Sophie Løhde) mulighed for at bestemme, at bestemte IT-systemer, som behandler personoplysninger og som føres for den offentlige forvaltning, helt eller delvis alene må opbevares i Danmark. Bestemmelsen skal sikre, at fremmede magter i tilfælde af krig ikke har mulighed for at få adgang til nationale personoplysninger, på en måde og i et omfang, der indebærer en risiko for statens sikkerhed.

Den danske digitaliseringsstyrelse ('Digitaliseringsstyrelsen') har, i samarbejde med det danske justitsministerium ('Justitsministeriet'), og det danske politis efterretningstjeneste ('PET'), vurderet at leveringen og driften af *Digital Post*-løsningen, omfatter behandling af personoplysninger, der indebærer en risiko for statens sikkerhed, og derfor er omfattet af Lov nr. 5020 af 23. Maj 2018 ('databeskyttelsesloven') § 3, stk. 9.

Derudover vurderede Digitaliseringsstyrelsen, Justitsministeriet og PET i relation til løsningens kritikalitet, at *Digital Post-løsningen* i sin helhed er af særlig kritisk karakter, hvorfor de kritiske dele af løsningen (eks. infrastruktur, transformationskomponent, databaser og krypteringsnøgler) ligeledes er omfattet af den danske databeskyttelseslovs § 3, stk. 9, og derfor ikke må placeres uden for Danmark.

Finansministeriets vurdering medfører, at leveringen af den ny *Digital Post-løsning* ikke kan udføres af flere af de internationale cloud-leverandører (eks. Microsoft Azure og Amazon Web Services), da disse ikke har infrastruktur/datacentre i Danmark.

Læs hele svaret her:
https://www.ft.dk/samling/20181/almdel/fiu/spm/542/svar/1577230/2050833.pdf

2. Det danske justitsministerium udgiver ny vejledning om frivillige foreningers behandling af personoplysninger

Det danske justitsministerium ('Justitsministeriet') udgav den 4. januar 2019 en ny vejledning om frivillige foreningers behandling af personoplysninger. Vejledningen har til formål at hjælpe frivillige foreninger og organisationer med at overholde reglerne i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') og Lov nr. 5020 af 23. Maj 2018 ('databeskyttelsesloven').

Vejledningen redegør for, hvornår behandling af personoplysninger i frivillige foreninger er omfattet af databeskyttelsesforordningen og databeskyttelsesloven. Foreninger skal på lige fod med andre dataansvarlige opfylde databeskyttelsesforordningen og databeskyttelseslovens regler om behandling af personoplysninger. Det gælder uanset foreningens størrelse, og at foreningen kun består af frivillige. Vejledningen giver desuden svar på ofte stillede spørgsmål fra frivillige foreninger og organisationer.

Justitsministeriet vejledning henviser til flere af det danske datatilsyns specifikke vejledninger, og anbefaler at frivillige foreninger og organisationer læser videre i disse for yderligere information.

Læs hele vejledningen her:
http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Databeskyttelse/endelig_vejledning_med_ofte_stillede_spoergsmaal_om_frivillige_foreningers_behandling_af_personoplysninger.pdf

3. Det danske datatilsyn offentliggør hvilke temaer som Datatilsynet vil fokusere på i første halvår af 2019

Den 31. januar 2019 udgav det danske datatilsyn ('Datatilsynet') en oversigt over, hvilke temaer som Datatilsynet vil fokusere på i deres planlagte tilsyn i første halvår af 2019.

Af oversigten fremgår, at Datatilsynet vil fokusere på følgende temaer:

- Brud på persondatasikkerheden hos offentlige myndigheder og private virksomheder
- Databeskyttelsesrådgiverfunktionen hos kommunerne
- Kryptering af e-mails hos private virksomheder
- Autorisation af medarbejdere hos kommunerne
- Den registreredes indsigtsret hos offentlige myndigheder og private virksomheder
- Brug (og genbrug) af data i den kommunale forvaltning
- Aggregering og sammenstilling af data til brug for videresalg hos private virksomheder

Det følger af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 37, at offentlige myndigheder og visse private virksomheder er forpligtet til at udpege en databeskyttelsesrådgiver. Datatilsynet tilkendegiver i oversigten, at Datatilsynet i deres tilsyn i første halvår af 2019 vil fokusere på tilfælde hvor databeskyttelsesrådgiverfunktionen udøves af et advokatselskab på vegne af en kommune. Herunder hvorvidt databeskyttelsesrådgiveren (advokatselskabet) løser de opgaver som følger af databeskyttelsesforordningen og databeskyttelsesrådgiverens tilgængelighed for kommunens medarbejdere og de registrerede.

Herudover vil Datatilsynet fokusere på hvorvidt private virksomheder har truffet de nødvendige sikkerhedsforanstaltninger i forbindelse med kryptering af e-mails, herunder vil der blive ført tilsyn med to advokatkontorer, et revisionsfirma og en fagforening.

Datatilsynet vil ligeledes fokusere på, hvorvidt offentlige myndigheder og private virksomheder anmelder de brud på datasikkerheden, som er påkrævet efter databeskyttelsesforordningen.

Læs alle temaerne her:
https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/jan/planlagte-tilsyn-i-foerste-halvaar-af-2019/

4. Det danske datatilsyn udgiver vejledning on dataansvar for konsulenter og vikarer

Det danske datatilsyn ('Datatilsynet') udgav den 21. februar 2019 en vejledning til brug for vurderingen af dataansvar for vikarer og konsulenter, herunder IT-konsulenter. Vejledningen er udgivet som følge af flere spørgsmål herom fra dataansvarlige virksomheder og myndigheder, der gør brug af vikarer og konsulenter.

Datatilsynet har opstillet en række vejledende principper for vurderingen af dataansvaret for henholdsvis vikarer og konsulenter.

Ved vurderingen af dataansvaret for vikarer, som skal behandle personoplysninger, har det ifølge Datatilsynet betydning, hvornår en vikar kan anses for at være en del af den dataansvarliges juridiske enhed, i modsætning til at være selvstændig dataansvarlig eller databehandler. Det vil efter Datatilsynets opfattelse typisk være tilfældet, når der foreligger en sådan instruktionsbeføjelse fra den dataansvarlige, at vikarens udførelse af opgaverne er sammenlignelig med de øvrige medarbejderes. Ifølge Datatilsynet vil behandlingen i sådanne situationer kunne anses for at høre under den behandling af personoplysninger, som foretages af den dataansvarliges virksomhed. Er vikaren omvendt ikke underlagt den dataansvarliges ledelsesret, vil vikaren skulle vurderes som enten dataansvarlig eller databehandler.

Ifølge Datatilsynet vil eksterne konsulenters udførelse af deres arbejdsopgaver i de fleste tilfælde ikke kunne anses for sammenlignelig med de øvrige medarbejderes. Eksterne konsulenter vil derfor typisk skulle vurderes som enten dataansvarlige eller databehandlere afhængig af de konkrete omstændigheder. Vurderingen, der her skal foretages, er, om den ydelse der købes af konsulenten, helt eller delvist drejer sig om, at konsulenten skal behandle personoplysninger til den dataansvarliges formål og under dennes instruks, herunder om den ydelse som konsulenten leverer går ud på at behandle personoplysninger på vegne af den dataansvarlige.

Læs hele vejledningen her:
https://www.datatilsynet.dk/media/6939/dataansvar-vikarer-og-konsulenter.pdf

5. Det danske datatilsyn og Danske Revisorer udgiver revisorerklæring om databehandlere

FSR – Danske Revisorer udgav den 1. februar 2019 i samarbejde med det danske datatilsyn ('Datatilsynet') en ny skabelon for revisorerklæringer om persondata (også kendt som en ISAE 3000-erklæring).

Dataansvarlige skal føre løbende kontrol med databehandlere, der behandler personoplysninger på vegne af den dataansvarlige, for at sikre, at disse overholder kravene til lovlig behandling af personoplysninger. Denne kontrol kan foretages ved at anvende en revisorerklæring.

Formålet med den nye revisorerklæring eller "Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til data-

behandleraftale med [Dataansvarlig]" er at hjælpe dataansvarlige med at overholde kravene til kontrol, bl.a. ved at sikre at databehandlere anvender korrekte procedurer til beskyttelse af persondata.

Revisorerklæringen opstiller en række eksempler på kontrolaktiviteter og revisionshandlinger, der kan bruges til inspiration for revisorens kontrol af behandlingssikkerheden. Blandt andet skal revisoren prøve, hvorvidt databehandleren har implementeret passende tekniske foranstaltninger, herunder om der foreligger de fornødne formaliserede procedurer for underretning, sletning mv. Det er forudsat, at parterne tilpasser erklæringen ud fra den konkrete risikovurdering og revisors vurdering.

Læs erklæringen her:
https://fsr.dk/Faglige_informationer/Om_revisor/Persondataforordningen/FSR%20lancerer%20paa%20baggrund%20af%20samarbejde%20med%20Datatilsynet%20ny%20erklaering%20om%20persondata

6. EDPB udgiver sit arbejdsprogram for 2019

Det Europæiske Databeskyttelsesråd ('EDPB') udgav den 12. februar 2019 sit arbejdsprogram for 2019-2020. Arbejdsprogrammet er udstedt i overensstemmelse med artikel 29 i EDPB's forretningsorden, hvorefter EDPB skal vedtage et toårigt arbejdsprogram. Det udstedte arbejdsprogram er således gældende for både 2019 og 2020.

I arbejdsprogrammet er der opstillet en række fokuspunkter og mål for EDPB's arbejde de næste to år. EDPB's liste over kommende aktiviteter indeholder planer om udarbejdelse af en række retningslinjer, vejledninger samt udtalelser, vedrørende bl.a. videoovervågning, Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen')'s territoriale anvendelsesområde og de registreredes rettigheder.

Formålet med EDPB's arbejde er at sikre en ensartet anvendelse af databeskyttelsesforordningen i EU. EDPB kommer ifølge det udstedte arbejdsprogram til at fokusere mere på specifikke områder og teknologier vedrørende fortolkningen af bestemmelserne i databeskyttelsesforordningen. Dette frem for mere generelle retningslinjer, som tidligere har været EDPB's fokus. Derudover forventer EDPB at tage stilling til konkrete sager og spørgsmål.

Læs hele arbejdsprogrammet her:
https://edpb.europa.eu/about-edpb/about-edpb/work-program_en

7. EDPB udgiver vejledning om overførsel af persondata til Storbritannien i tilfælde af et no-deal Brexit

Det Europæiske Databeskyttelsesråd ('EDPB') udgav den 12. februar 2019 en vejledning om overførsel af persondata til Storbritannien i tilfælde af et no-deal Brexit. Vejledningen opsummerer de fire muligheder, der gælder for overførsel af data til tredjelande ifølge Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen').

I tilfælde af et no-deal Brexit vil Storbritannien være et tredjeland i databeskyttelsesforordningens forstand. Som følge heraf skal overførsel af persondata ske ved hjælp af ét af fire instrumenter. I vejledningen redegøres der for hvordan de fire anvendelige instrumenter specifikt kan anvendes i forbindelse med Brexit. Hvilket omfatter standard eller ad hoc databeskyttelsesklausuler godkendt af EU-Kommissionen, bindende virksomhedsregler ('Binding Corporate Rules'), adfærdskodekser eller certificeringsordninger samt undtagelserne i medfør af artikel 49 i databeskyttelsesforordningen. Vejledningen henvender sig både til private og offentlige organisationer, hvorfor den også opsummerer de særlige overførselsgrundlag, der gælder for offentlige institutioner.

Læs hele vejledningen her:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12-infonote-no-deal-brexit_en.pdf

8. EDPS udgiver sin årlige rapport om EDPS aktiviteter i 2018

Den Europæiske Tilsynsførende for Databeskyttelse ('EDPS') udgav den 26. februar deres årsrapport for 2018, hvor Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') ikrafttræden den 25. maj 2018 var i fokus.

Et vigtigt omdrejningspunkt i databeskyttelsesforordningen er princippet om ansvarlighed, hvorefter den dataansvarlige er ansvarlig for og skal kunne bevise, at den dataansvarliges behandling af personoplysninger er i overensstemmelse med reglerne i databeskyttelsesforordningen. EDPS lægger vægt på, at overholdelsen af databeskyttelsesreglerne skal kunne bevises, selv i relation til håndteringen af IT-infrastruktur og –systemer. Princippet om ansvarlighed er en del af EDPS' fokusområder for 2019.

En af EDPS' opgaver er at føre tilsyn med Europols behandling af persondata. EDPS foretog to inspektioner af Europol i 2018, og fandt fire kritikpunkter, herunder behandling af data fra rejsende i konfliktområder og migranter, som EDPS vil følge op på.

Grænsekontrol spillede også en stor rolle i 2018, og EDPS har påpeget risikoen for identitetstyveri ved øget anvendelse af biometrisk data i pas. Dette skyldes ifølge EDPS, at den øgede brug af biometriske data medfører større mulighed for misbrug i tilfælde af et databrud.

EDPS har i 2018 haft fokus på digital etik og afholdt i den forbindelse en international konference om emnet. Herudover lancerede EDPS i juni 2018 en offentlig høring, hvor de indsamlede holdninger til digital etik fra hele verden, herunder fra skoler, universiteter, regeringer, advokatfirmaer og NGO'er. EDPS har som et fokuspunkt i 2019 at opfordre til og opretholde momentum i debatten om digital etik.

EDPS rapporterer herudover om internationalt samarbejde på flere niveauer, herunder angående spørgsmålet om overførsel af persondata til tredjelande. I 2018 indebar dette, at EDPS deltog i anden gennemgang af EU-US Privacy Shield og udstedte en udtalelse om EU-kommissionens afgørelse om tilstrækkeligheden af Japans beskyttelsesniveau.

Læs hele rapporten her:
https://edps.europa.eu/sites/edp/files/publication/ar2018_en.pdf

9. ENISA udgiver rapport om cybersikkerhed i forbindelse med valg

Den Europæiske Unions Agentur for Net- og Informationssikkerhed ('ENISA'), udgav i februar 2019 en rapport om cybersikkerhed i forbindelse med EU-medlemsstaternes politiske valgprocesser.

Udover at udtrykke ENISA's holdning til cybersikkerhed, indeholder rapporten en række anbefalinger, der skal forbedre cybersikkerheden i EU-medlemsstaternes valgprocesser. Anbefalingerne indeholder såvel proaktive som reaktive tiltag, samt forslag til yderligere regulering og samarbejde blandt EU-medlemsstaterne.

På baggrund af den øgede brug af digitale tjenester i valgprocesserne, såsom afgivelse og optælling af stemmer, mener ENISA, at et højt niveau af cybersikkerhed er en forudsætning for en vellykket valgproces.

For at opnå dette, anbefaler ENISA bl.a., at digitale serviceudbydere, sociale medier, online platforme etc., skal anvende teknologi, der kan opdage usædvanlig aktivitet. Den foreslåede teknologi vil kunne indikere, at der er tale om et cyberangreb eller spredning af falsk information. På trods af, at nogle af disse aktører allerede er undergivet selvregulering, mener ENISA, at EU bør overveje, om aktørerne skal reguleres i EU-regi, samtidig med at de enkelte EU-medlemsstater bør overveje at lovgive om onlinespredning af falsk information.

ENISA anbefaler ydermere, at EU bør overveje at indføre regulering der indebærer, at EU-medlemsstaternes valgsystemer skal klassificeres som kritisk infrastruktur, således at EU-medlemsstaterne forpligtes til at indføre den nødvendige cybersikkerhed i medfør af Europa-Parlamentets og Rådets Direktiv (EU) 2016/1148 af 6. juli 2016 ('NIS-direktivet'), således at valgsystemer underlægges de sikkerhedskrav og underretningsforpligtelser der følger af NIS-direktivet.

Læs hele vejledningen her:
https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities

10. ENISA udgiver rapport om standarder i forbindelse med implementering af PSD2-direktiv

I december 2019 udgav Den Europæiske Unions Agentur for Net- og Informationssikkerhed ('ENISA') deres rapport om god skik i forbindelse med implementeringen af Europa-Parlamentets og Rådets Direktiv (EU) 2015/2366 om betalingstjenester i det indre marked ('PSD2-direktivet'). PSD2-direktivet indførte regler for internationale betalingstjenester der skal sikre at betalinger mellem EU-lande, kan foretages med samme effektivitet og sikkerhed som indenrigsbetalinger

Rapportens hovedformål er, at klarlægge hvordan medlemsstaterne har implementeret PSD2-direktivet, herunder forskelle i implementeringen på tværs af medlemsstaterne.

Rapporten har fokus på hvordan medlemsstaterne implementerede ENISAs retningslinjer vedrørende sikkerhedsforanstaltninger for betalingstjenester. Rapporten redegør ligeledes for hvordan medlemsstaterne tilsikrer operationaliteten af betalingstjenester, samt hvordan anmeldelsen af større drifts- eller sikkerhedshændelser indgives til den nationale kompetente myndighed.

Ydermere afdækker rapporten hvordan medlemsstaterne tilsikrer at betalingstjenesteudbydere overholder PSD2-direktivet.

Læs hele rapporten her:
https://www.enisa.europa.eu/publications/good-practices-on-the-implementation-of-regulatory-technical-standards

11. EU-kommissionen udgiver deres årlige redegørelse af Privacy-Shield aftalen

EU-kommissionen offentliggjorde i december 2018 sin årlige redegørelse af EU-US Privacy Shield-aftalen. Aftalen omfatter i øjeblikket mere end 3.850 certificerede virksomheder, herunder Google, Microsoft og IBM.

I redegørelsen fastslår EU-Kommissionen, at USA's beskyttelse ved overførsel af data i henhold til Privacy Shield-aftalen er forbedret i forhold til seneste redegørelse og nu er på et tilstrækkeligt niveau. Forbedringen skyldes USA's implementering af anbefalingerne i den seneste redegørelse, herunder indførelsen af såkaldte "spot checks", hvor virksomheder tilfældigt udvælges til kontrol. Ud af de 100 virksomheder, som blev kontrolleret, blev der hos 21 fundet problemer med behandlingen af persondata. Foruden dette tiltag har USA implementeret et system, der skal sikre at virksomheder ikke kan

påstå, at de er certificerede uden reelt at være det.

Selvom redegørelsen overordnet set beskriver beskyttelsen som tilfredsstillende, fastslår Kommissionen dog, at EU forventer at USA vil udnævne en permanent "Ombudsperson". Ombudspersonen beskrives som en vigtig mekanisme til at sikre klageadgangen for datasubjekter, hvis personoplysninger er blevet overført til USA. På nuværende tidspunkt har USA kun en midlertidig Ombudsperson. I slutningen af januar offentliggjorde USA, at de har nomineret iværksætteren Keith Krach til posten som permanent Ombudsperson. Processen med at udnævne en Ombudsperson er endnu ikke afsluttet.

Læs hele redegørelsen her:
http://europa.eu/rapid/press-release_IP-18-6818_en.htm

12. Det Danske Folketing begrænser arbejdsgivernes adgang til personoplysninger om medarbejdere

Den 1. januar 2019 trådte lov nr. 1522 af 18. december 2018 ('den danske lov om ændring af sygedagpengeloven og lov om aktiv socialpolitik') i kraft. Lovændringen begrænser arbejdsgiveres mulighed for at få adgang til medarbejderes helbredsmæssige og lægelige oplysninger.

Arbejdsgivere har tidligere haft en udvidet adgang til sygemeldte medarbejderes helbredsoplysninger. I en dom fra januar 2017 slog Højesteret fast, at en kommune havde pligt til at give en arbejdsgiver, som modtog sygedagpengerefusion, aktindsigt i oplysninger om en medarbejders psykiske helbred.

Efter lovændringen har en arbejdsgiver som udgangspunkt ikke længere ret til at blive gjort bekendt med helbredsmæssige og lægelige oplysninger om sine medarbejdere.

Arbejdsgiveren kan dog få adgang til oplysningerne, hvis de er af væsentlig betydning for, at arbejdsgiveren kan varetage sine økonomiske interesser i en sag om refusion af sygedagpenge. Selv hvis oplysningerne findes at være væsentlige for arbejdsgiveren, skal adgangen dog afskæres, hvis der foreligger afgørende hensyn til medarbejderens interesse i hemmeligholdelse af oplysningerne.

Kommunen skal foretage en konkret vurdering i hvert enkelte tilfælde.

Læs hele lovændringen her:
https://www.ft.dk/samling/20181/lovforslag/L69/som_vedtaget.htm

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

Delphi

Felix Makarowski

Anmälda personuppgiftsincidenter 2018 och Datainspektionens granskningar 2019-2020

Anmälda personuppgiftsincidenter 2018

Under perioden 25 maj – 31 december fick den svenska Datainspektionen in 2 262 incidentanmälningar, skriver Datainspektionen.[1] Antalet anmälda personuppgiftsincidenter ökade successivt under året. Den absoluta merparten av de incidenter som anmälts under året bedöms utgöra reella personuppgiftsincidenter även om en viss överrapportering förekom – det vill säga att även incidenter som inte är anmälningspliktiga anmäldes.

En fjärdedel av alla incidentanmälningar kom från verksamheter inom den finansiella sektorn eller försäkringsbranschen. Myndigheter och kommuner stod tillsammans för 23 procent av anmälningarna. Hälso- och sjukvård, skola och socialtjänst stod tillsammans för 23 procent av anmälningarna, med 7 till 8 procent vardera, och näringslivet stod i övrigt för 19 procent. Enligt Datainspektionen behöver en hög anmälningsgrad inom en organisation eller bransch inte nödvändigtvis vara en indikation på bristande säkerhet. Tvärtom kan det i vissa fall tyda på att verksamheten har strukturer och rutiner som ger en god förmåga att upptäcka och rapportera personuppgiftsincidenter.

1 Datainspektionensrapport 2019:1 – Anmälda personuppgiftsincidenter 2018, *https://www.datainspektionen.se/globalassets/dokument/rapporter/anmalda-personuppgiftsincidenter-2018.pdf*

Den vanligaste typen av anmälda personuppgiftsincidenter, 42 procent, avser felaktiga brevutskick, det vill säga att brev eller e-post som innehåller personuppgifter oavsiktligen hamnat hos fel mottagare. Obehörig åtkomst och övrigt obehörigt röjande stod för 23 respektive 20 procent av de anmälda incidenterna. Stöld, övrig förlust och phishing stod tillsammans för enbart 13 procent av de anmälda incidenterna.

En majoritet av de anmälda personuppgiftsincidenterna, 61 procent, uppges ha orsakats av den mänskliga faktorn. Enligt Datainspektionen beror dessa incidenter i huvudsak på att individer begått misstag vid hantering av personuppgifter i verksamheten, exempelvis vid utskick av brev eller e-post. Antagonistiska angrepp orsakade cirka 14 procent av de anmälda incidenterna, medan 10 procent av de anmälda incidenterna orsakades av tekniska fel.

Det bör anmärkas att en klar majoritet av alla personuppgiftsincidenter beror på interna faktorer inom en organisation, medan enbart en liten andel beror på externa angrepp på organisationen. Utifrån de personuppgiftsincidenter som anmälts under 2018 har Datainspektionen därför kommit med några allmänna rekommendationer som kan bidra till att förebygga incidenter och mildra konsekvenserna om en incident ändå inträffar. Dessa rekommendationer är:

- Grundläggande åtgärder som att alltid kontrollera att korrekt mottagare är angiven eller att använda funktionen dold kopia (bcc) vid utskick som ska till flera mottagare bör användas,
- Personuppgifter som lagras på flyttbara media – till exempel usb-minnen, bärbara datorer och mobiltelefoner – bör krypteras så att ingen obehörig kan ta del av informationen på dessa media,
- Länkar eller bifogade filer från okända användare bör inte öppnas,
- Alla organisationer som hanterar personuppgifter ska ha stabila rutiner för att säkerställa att behörigheter tilldelas korrekt, att behörigheterna löpande kontrolleras och följs upp samt att åtkomstkontroller genomförs,
- Styrdokument och tekniska informationssäkerhetsåtgärder bör kompletteras med löpande utbildning och andra åtgärder för att öka kunskapen och medvetenheten hos organisationens personal.

Datainspektionens planerade granskningar 2019–2020

Datainspektionen har fattat beslut om ny tillsynsplan för 2019–2020.[2] Tillsynen ska ske inom tre områden där särskilda risker kan identifieras. Dessa är prioriterade rättsområden, specifika branscher eller verksamheter, och nya företeelser.

Datainspektionen avser under 2019 att genomföra tillsyn avseende, bland annat, följande branscher och verksamheter:

- Hälso- och sjukvården,
- Skolan,
- Rättsväsendet,
- Arbetsgivares behandling av anställdas personuppgifter,
- Detaljhandeln, och
- Inkassoverksamhet.

Utöver granskningen av specifika branscher och verksamheter kommer Datainspektionen, som vi berättade om i förra numret, att utöva särskild tillsyn över den rättsliga gränsdragningen mellan rollerna som personuppgiftsansvarig och personuppgiftsbiträde och samtycke som rättslig grund samt över gränsdragningen mellan betaltjänstlagen och kreditupplysningsverksamhet. Den nya företeelse som kommer att granskas är ansiktsigenkänningsteknik. Även annan teknikanvändning kan komma att bli föremål för tillsyn, exempelvis maskininlärning, automatiserade beslut, profilering och blockkedjor. Tillsyn kan även komma att inledas utanför de prioriterade områdena ovan om det på grund av specifika händelser finns anledning att agera på områden där konsekvenserna för den enskildes rättigheter bedöms vara särskilt allvarliga eller om tillsyn är påkallad av andra skäl.

Datainspektionen inleder granskning av åtta vårdgivare

Tillsyn över hälso- och sjukvårdsområdet har redan inletts genom att Datainspektionen har inlett en granskning av åtta vårdgivare för att undersöka hur de reglerar användarnas åtkomst till uppgifter i huvudjournalsystemen. Enligt patientdatalagen ska personal endast kunna komma åt de patientuppgifter som de behöver för att kunna utföra sina arbetsuppgifter. Granskningen inleds med anledning av att Datainspektionen under de senaste åren granskat flera vårdgivare där personalen har haft åtkomst till en majoritet av patienternas uppgifter, utan att ha behov av det. Verksamheterna garanterar därmed inte patienterna det integritetsskydd de har rätt till. Datainspektionen ska även granska om uppgifterna som finns i journalsystemets åtkomstlogg kan svara på vem som gjorde vad, med vilka uppgifter och när.

Felix Makarowski är associate i Advokatfirman Delphi, Stockholm.

2 DI-2019-841 – Tillsynsplan 2019–2020, *https://www.datainspektionen.se/globalassets/dokument/datainspektionens-tillsynsplan-2019-2020.pdf.*


Wiersholm

Pernille Lia
og Rune Opdahl

Nye retningslinjer fra Personvernrådet

Det europeiske Personvernråd (Personvernrådet) publiserte 9. april 2019 foreløpige retningslinjer om forståelsen av det rettslige grunnlaget for behandling av personopplysninger etter GDPR artikkel 6(1)(b) (*avtalegrunnlaget)* i forbindelse med digitale tjenester. Retningslinjene kan forstås som et oppgjør med en praksis som Personvernrådet mener strekker avtalegrunnlaget for langt.

Nødvendighetskriteriet

Avtalegrunnlaget inneholder to alternativer: behandlingen skal være nødvendig for (i) å oppfylle en avtale som den registrerte er part i; eller (ii) å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse.

Nødvendighetskriteriet gjelder for begge alternativene. Personvernrådet fremhever at nødvendighetskriteriet har selvstendig betydning i unionsretten. Blant annet skal vurderingen være faktabasert, og gjenspeile personvernprinsippene og retten til privatliv. Hvis det finnes et realistisk, mindre inngripende alternativ til behandlingen, skal en slik løsning velges i stedet.

For å oppfylle en avtale eller før avtaleinngåelse

Alternativet om *oppfyllelse av en avtale* må forstås i sammenheng med de øvrige bestemmelsene i GDPR. Prinsippet om lovlighet forutsetter at avtalen er gyldig etter nasjonale regler, for eksempel regler om forbrukerbeskyttelse. Prinsippet om formålsbegrensning innebærer at behandling av personopplysninger som er nødvendig etter avtalen spesifiseres og skilles fra informasjon som behandles etter andre rettslige grunnlag.

Behandlingen er bare nødvendig for å oppfylle en avtale hvis den knytter seg til tjenestens hovedinnhold, ikke hvis den knytter seg til en tilleggstjeneste. I tråd med prinsippet om rettferdighet skal det ses hen til mottakerens rimelige forventninger til avtalen, blant annet basert på hvordan tjenesten beskrives og er markedsført. Behandling av opplysninger om en mottakers interesser kan for eksempel være nødvendig for å levere en tjeneste som dreier seg om levering av personalisert innhold hvis dette fremstår som en integrert del av tjenesten.

Personvernrådet presiserer at det finnes et skille mellom nødvendighetskriteriet og kontraktuell nødvendighet. Personopplysninger kan ikke brukes som byttemiddel for en digital tjeneste selv om forretningsmodellen for å levere tjenesten avhenger av en viss bruk av mottakerens personopplysninger. Behandling av personopplysninger som er pålagt mottakeren i tjenestevilkårene kan ikke begrunnes i avtalegrunnlaget med mindre behandlingen også er objektivt nødvendig for å gjennomføre tjenesten.

Alternativet om *gjennomføring av tiltak før en avtaleinngåelse* knytter seg til avtaleforberedelser, altså behandling som legger til rette for en forestående avtale. For eksempel gjelder alternativet for behandling av en mottakers adresse for å undersøke om tjenesten kan leveres, mens uoppfordret kontakt fra en tjenestetilbyder vil ikke omfattes.

Avtalegrunnlagets rekkevidde

Etter avtalens opphør må behandling av personopplysninger i utgangspunktet ha et annet behandlingsgrunnlag enn avtalegrunnlaget, med mindre slik etterfølgende behandling med rimelighet kan forutses ved avtaleinngåelsen, slik som utsendelse av fakturapåminnelser.

Behandling som faller utenfor bestemmelsens snevre virkeområde, for eksempel behandling av særlige kategorier av personopplysninger, kan ha andre behandlingsgrunnlag. Dette må imidlertid avklares før behandlingen finner sted, blant annet av hensyn til prinsippet om åpenhet og informasjon til mottakeren.

Forbedring av egne tjenester, og det å forhindre svindel og målrettet markedsføring trekkes frem som eksempler på behandlingsaktiviteter som faller utenfor avtalegrunnlaget, mens tjenestetilpasning kan være omfattet hvis det er en viktig eller forventet del av tjenesten. Sammenslåing av flere tjenester kan ifølge Personvernrådet heller ikke gjøres med hjemmel i avtalegrunnlaget,

selv om tjenestene er fra samme tjenestetilbyder. For slike aktiviteter må tjenestetilbyderen eventuelt søke rettslig grunnlag i for eksempel interesseavveiningen.

Konsekvenser

For det første er avtalegrunnlaget begrenset i omfang. Konsekvensen av dette er at tjenesteleverandørens eventuelle behandling av personopplysninger i randsonen av eller utenfor avtalen må skje etter andre rettslige grunnlag, som *interesseavveiningen* eller *samtykke*.

For det andre er avtalegrunnlaget tidsbegrenset. Som utgangspunkt vil ikke avtalegrunnlaget kunne brukes etter avtalens opphør, med mindre det er tale om umiddelbar oppfølging av avtalen. Eventuell etterfølgende oppbevaring og behandling må da ha et annet rettslig grunnlag. Informasjon om dette må gis ved innsamlingen.

Retningslinjene er ute til høring frem til 24. mai. Personvernrådet vil vurdere eventuelle innspill før retningslinjene blir endelig vedtatt.

Forutsatt at de endelige retningslinjene ikke vil skille seg vesentlig fra de som nå er publisert, vil de kunne endre hvordan digitale tjenesteleverandører behandler personopplysninger, og hvordan de utformer sine tjenester og sine personvernerklæringer. Retningslinjene vil trolig også være retningsgivende for tjenester som ikke leveres online.

Pernille Lia er advokatfullmektig i Advokatfirmaet Wiersholm, Oslo.

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

Gorrissen Federspiel

Tue Goldschmieding

1. EU-Kommissionen, EU-Parlamentet samt Europa Rådet vedtager forslaget til det nye Ophavsretsdirektiv

Den 26. marts 2019 vedtog EU-parlamentet et nyt direktiv om ophavsret på det digitale indre marked ('Ophavsretsdirektivet'). Ophavsretsdirektivet forventes at reformere beskyttelsen af immaterielle rettigheder på internettet. Ophavsretsdirektivet erstatter ikke den øvrige EU-lovgivning på området, men supplerer og modificerer denne, jf. ophavsretsdirektivets artikel 1, stk. 2. Direktivet skal implementeres inden for 2 år i de enkelte medlemsstaters lovgivning.

Det nye ophavsretsdirektiv betyder, at udbydere af onlineplatforme i langt højere grad end tidligere kan ifalde erstatningsansvar, for materiale uploadet af brugerne. En udbyder af en platform er, jf. ophavsretsdirektivets artikel 2, stk. 5, en udbyder af informationssamfundstjenester, der har som hovedformål eller som et af sine hovedformål, at lagre eller kommunikere ophavsretligt beskyttet materiale til offentligheden. Et eksempel herpå er YouTube.

Det følger af ophavsretsdirektivets artikel 13, at udbydere af onlineplatforme, vil kunne blive ansvarlige for krænkelser af ophavsretten, som sker på baggrund af materiale uploadet af brugerne, såfremt udbyderen af platformen ikke har gjort et reelt og hæderligt forsøg på, at opnå en licens til det brugeruploadede materiale, der er beskyttet af ophavsretten. Dette er en betydelig skærpelse i forhold til Europa-Parlamentets og Rådets Direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester ('Direktivet om elektronisk handel') artikel 14, hvoraf det fremgår at udbydere af onlineplatforme ikke er ansvarlige for brugeruploadet indhold, såfremt udbyderen ikke var vidende om indholdet.

Herudover følger det af ophavsretsdirektivets artikel 2, at en række leverandører af plaforme ikke vil blive omfattet af direktivet, herunder non-profit encyklopædier, eks. Wikipedia, og udviklingsplatforme for open-source software.

Endvidere indfører ophavsretsdirektivet i artikel 11 en særlig beskyttelse for udgivere af pressepublikationer. Selvom det allerede efter de nuværende regler ikke er tilladt uden tilladelse fra rettighedshaveren at kopiere pressepublikationer, eksempelvis artikler og fotos, fra onlinemedier, pålægger ophavsretsdirektivet nu eksplicit medlemsstaterne at tilsikre udgivere af pressepublikationer eneretten til online brug af sådanne publikationer, jf. Europa-Parlamentets og Rådets Direktiv 2001/29/EF af 22. maj 2001 om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet ('InfoSoc-direktivet') artikel 2 og 3, litra 2.

Beskyttelsen sigter på, at sikre rettighederne for udgivere af pressepublikationer, i forbindelse med at leverandører af informationssamfundstjenester henviser til publikationerne fra andre websider.

Beskyttelsen af pressepublikationerne gælder dog ikke brugen af enkelte ord, meget korte uddrag eller hyperlinks til artiklerne. Beskyttelsen varer ifølge ophavsretsdirektivet i 2 år efter den første offentliggørelse af artiklen.

På visse punkter kodificerer ophavsretsdirektivet nu retten til at benytte ophavsretligt beskyttet materiale til citater, kritik, anmeldelse, karikatur, parodi eller pastiche. Eksempelvis er såkaldte *'memes'* og *'GIFs'*, som ofte gør brug af ophavsretligt beskyttet materiale til at parodiere eller karikere, ikke omfattet af ophavsretsdirektivet.

Læs hele direktivet her:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6637_2019_INIT&qid=1551167820610&from=EN

2. McDonald's mister retten til EU-varemærket "Big Mac"

Den Europæiske Unions Kontor for Intellektuel Ejendomsret ('EUIPO') afsagde den 11. januar 2019 afgørelse i sag nr. 14 788 C, om ophævelse af McDonald's EU-varemærke "Big Mac", som McDonald's siden 1998 havde været indehaver af. Sagen blev rejst på baggrund af en anmodning om ophævelse fra Supermac's Holdings Ltd ('Supermac') fra 2017.

Supermac gjorde gældende, at McDonald's ikke havde opfyldt sin brugspligt efter artikel 58, stk. 1 litra a i Europa-Parlamentets og Rådets forordning (EU) 2017/1001 af 14. juni 2017 om EU-varemærker ('EU-varemærkeforordningen'). Det følger af denne bestemmelse, at en EU-varemærkeindehavers ret til varemærket fortabes efter manglende reel brug i en periode på 5 år.

McDonald's forsøgte gennem fremlæggelse af tre erklæringer fra McDonald's repræsentanter i Tyskland, Frankrig og England, som indeholdt en angivelse af salgstallene for "Big Mac"-burgeren, at løfte bevisbyrden for at varemærket reelt var i brug. Derudover fremlagde McDonald's markedsføringsmateriale, herunder menuer og emballage, indeholdende varemærket samt en udskrift fra Wikipedia om "Big Mac". EUIPO fandt imidlertid, at dette ikke var tilstrækkeligt til at bevise et reelt brug af varemærket, herunder omfanget af et eventuelt brug eller om produkter under varemærket reelt var blevet udbudt til salg i den 5-årige periode.

EUIPO kom på denne baggrund frem til at McDonald's ikke havde fremkommet med tilstrækkelig dokumentation for at brugspligten var opfyldt, og ophævede på dette grundlag registreringen af varemærket "Big Mac". EUIPO fremhæver at McDonald's skulle have fremlagt bevis for, at markedsføringsmaterialet var blevet uddelt, hvem det var blevet uddelt til samt om dette havde ført til potentielle eller faktiske ordrer. Derudover skulle McDonald's have fremlagt uafhængig dokumentation for omfanget af brugen af varemærket.

Afgørelsen medfører, at McDonald's ikke længere har eneret til brugen af betegnelsen "Big Mac", men har dog fortsat mulighed for at anvende denne betegnelse for sine produkter. Derudover er McDonald's stadig indehaver af flere nationale varemærker, som kan beskytte brugen af varemærket "Big Mac". McDonald's har appelleret sagen til ankenævnet Boards of Appeal.

Afgørelsen fra EUIPO understreger vigtigheden af at kunne fremlægge klar dokumentation for reel brug af varemærket. Det er herunder uden betydning, om der er tale om et velkendt varemærke.

Læs hele afgørelsen her:
https://euipo.europa.eu/eSearchCLW/#basic////number/000014788*

3. Den danske forbrugerombudsmand udgiver ny vejledning om elektronisk markedsføring

Den danske forbrugerombudsmand ('Forbrugerombudsmanden') udgav i december 2018 en ny vejledning om elektronisk markedsføring. Vejledningen er udgivet i forlængelse af den nye lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov'). Den nye vejledning vil kun angå spamforbuddet (dvs. henvendelser ved brug af elektronisk post, herunder mail, sms og sociale meder), som omhandlet i den danske markedsføringslovs § 10, i modsætning til den gamle vejledning om "uanmodet henvendelse til bestemte modtagere", som også indeholdte en vejledning angående telefoniske henvendelser. Forbrugerombudsmanden forventer, at udgive en rapport om telefoniske henvendelser i løbet af 2019.

I vejledningen redegøres for, hvad der skal forstås ved spamforbuddet. Vejledningen gennemgår

således, hvem og hvilke kommunikationsformer der er omfattet af forbuddet, og hvad der skal forstås ved direkte markedsføring. Dernæst gennemgås gyldigt samtykke, samtykkets ophør og dokumentation for samtykket. Sidst beskrives betingelserne for markedsføring til en tidligere kunde, kravene til henvendelsens indhold og det strafferetlige ansvar og medvirken. Vejledningen indeholder også et bilag om sociale medier, der beskriver hvilke typer henvendelser på sociale medier, der er omfattet af spamforbuddet.

Vejledningen er tænkt som dels en kvikguide til overholdelse af spamforbuddet, dels et bidrag til en større forståelse af elementerne heri.

EU forhandler nu om en ePrivacy-forordning, som skal erstatte EU-direktiv 2009/136/EF, hvorfra den danske markedsføringslov § 10 er implementeret. Når forordningen er vedtaget, vil Forbrugerombudsmanden opdatere vejledningen i det omfang, det er nødvendigt.

Læs hele vejledningen her:
https://www.forbrugerombudsmanden.dk/media/46499/spamvejledning-2018.pdf

4. Domænet reddit.dk skulle overføres til klageren

Det danske klagenævn for domænenavne ('Klagenævnet') traf den 13. december 2018 afgørelse i klagesagen, j.nr.: 2018-0495, mellem Reddit, Inc. ('klager'), C ('indklagede 1') og HTML24 ApS ('indklagede 2'). Sagen angik, hvorvidt klager kunne kræve domænenavnet "reddit.dk" overdraget fra indklagede 1 og 2. Indklagede 1 var registrant af domænenavnet, mens domænenavnet var registreret til brug for indklagede 2.

Klager havde siden 2005 drevet virksomhed under domænenavnet "reddit.com", som fungerede som en social nyheds- og underholdningshjemmeside. Klager anmodede i 2010 om EU-varemærkeregistrering af ordmærket "REDDIT", hvorefter varemærket blev registreret i 2012. Klager mente derfor at indklagedes brug af domænenavnet "reddit.dk" udgjorde en krænkelse af klagerens varemærkerettigheder samt en overtrædelse af forbuddet mod at opretholde registreringer af domænenavne alene med videresalg for øje.

Indklagede 1 drev IT-virksomheden *indklagede 2*, hvori indklagede 2 solgte et IT-produkt kaldet 'REDDIT'. I forlængelse heraf registrerede indklagede 1, på vegne af indklagede 2, i 2009 domænet "reddit.dk", med henblik på benytte domænet til at markedsføre dette produkt. Klagenævnet lagde i sin afgørelse vægt på, at indklagede 2 ikke havde dokumenteret erhvervsmæssig brug af domænenavnet før klagers varemærkeregistrering, hvorfor klager kunne forbyde en sådan brug efter artikel 9, stk. 1 og 2 i Europa-Parlamentets og Rådets forordning (EU) 2017/1001 af 14. juni 2017 om EU-varemærker.

Indklagedes 2's anvendelse af domænenavnet "reddit.dk" ville udgøre en utilbørlig udnyttelse af REDDIT-varemærkets særpræg og renommé. Klagenævnet bemærkede, at indklagede 2's manglende brug af domænenavet ikke i sig selv var nok til at godtgøre, at indklagede 2 alene opretholdt registeringen af domænenavnet med henblik på videresalg, hvorfor § 25, stk. 2 i lov nr. 164 af 26. februar 2014 om internetdomæner ('domæneloven') ikke var overtrådt.

Klagenævnet fandt på baggrund af ovenstående, at klager kunne kræve domænenavnet "reddit.dk" overdraget fra indklagede.

Læs hele afgørelsen her:
https://www.domaeneklager.dk/sites/default/files/2018-12/2018-0495%20reddit.dk_.pdf

5. Tre udgivelser vedrørende Femern-broen var ikke omfattet af markedsføringsloven

Den 7. januar 2019 afsagde den danske Sø- og Handelsret ('Sø- og Handelsretten') dom i sagen, V-39-17, mellem Scandlines Danmark ApS ('Scandlines') og Femern Bælt A/S ('Femern'). Femern havde udgivet et børnehæfte med et spil og to brochurer, alt sammen omhandlende Femern Bælt-forbindelsen. Scandlines mente, at disse brochurer var i strid med bl.a. god markedsføringsskik og forbuddet mod vildledende markedsføring efter lov nr. 426 af 3/5/2017 ('den danske markedsføringslov'), idet materialet, efter Scandlines opfattelse, indeholdt urigtige og misrekommanderende oplysninger om Scandlines. Et af hovedspørgsmålene i sagen var først og fremmest, om udgivelserne var omfattet af den danske markedsføringslov.

Sø- og Handelsretten fastslog indledningsvist, at Femern var at betragte som en offentlig myndighed som var omfattet af den danske markedsføringslov, jf. dennes § 1, stk. 1.

Sø- og Handelsretten fandt herefter, at Femern tidligst kunne tilbydes offentligheden fra år 2028, hvorfor Femern ikke på tidspunktet for udgivelserne havde et produkt, der kunne tilbydes markedet. Sø- og Handelsretten fandt i denne forbindelse, at ibrugtagningen af forbindelsen lå i en fjern og usikker fremtid, hvorfor det forberedende og opmærksomhedsskabende materiale, som Femern havde udgivet, ikke havde en aktualitet, der gjorde den danske markedsføringsloven anvendelig.

Retten konkluderede derfor, at Femerns udgivelser ikke var omfattet af den danske markedsføringslov og vurderede således ikke, om udgivelserne var i strid hermed. Retten konkluderede endvidere, at spørgsmålet om hvorvidt Femern havde handlet uden for deres informationspligt skulle afgøres ved administrativ rekurs.

Læs hele dommen her:
http://domstol.fe1.tangora.com/media/-300011/files/V0039000.pdf?rev1

6. Den danske højesteret tager stilling til underordnet brug af ophavsretligt beskyttede værker i markedsføring

Den 18. december afsagde den danske højesteret ('Højesteret') dom i sagen, 171/2017, mellem Coop Danmark A/S ('Coop') og K.H. Würtz ved Kasper Würtz ('Würtz'). Coop havde siden 2012, uden aftale, anvendt Würtz' keramikservice som rekvisit i deres emballage til fødevarer og i tilbudsaviser. Spørgsmålet var således, om Coop derved havde krænket Würtz' rettigheder efter bl.a. lovbekendtgørelse nr. 1144 af 23/10/2014 om ophavsret ('den danske ophavsretslov').

Den Danske Sø- og Handelsret var i deres dom i første instans kommet frem til, at Würtz' keramikservice var beskyttet efter den danske ophavsretslovs § 1, som brugskunst, og at Coops brug af keramikservicen ikke var omfattet af de minimis-princippet i den danske ophavsretslovs § 23, stk. 3, og dømte derfor Coop for at have krænket Würtz' ophavsret.

Coop ankede sagen, som herefter blev indbragt for Højesteret. Efter at have konstateret, at anvendelsen var sket uden aftale, fastslog Højesteret, at Würtz' keramik, som kunne betegnes som brugskunst, var beskyttet efter den danske ophavsretslov i medfør af dennes § 1, stk. 1, og stadfæstede derfor den danske Sø- og Handelsrets dom.

Coop gjorde gældende, at anvendelsen af Würtz' keramik var berettiget som følge af en kutyme inden for reklame- og dagligvarebranchen for brug af genstande som rekvisitter. Højesteret fastslog, at det kræver stærke holdepunkter at fastslå eksistensen af en sådan kutyme, og at Coop ikke havde løftet bevisbyrden for disse.

Coop gjorde ydermere gældende, ligesom de havde gjort under sagen for den danske Sø- og Handelsret, at der, ifølge princippet i den danske ophavsretslovs § 23, stk. 3, gælder et de minimis-princip, hvorefter brugen af et ophavsretligt beskyttet værk er tilladt, hvis brugen heraf er af underordnet betydning i den pågældende sammenhæng. Højesteret gav Coop medhold i eksistensen af en sådan ulovbestemt regel, men fandt, at en sådan undtagelse til ophavsretten skal fortolkes restriktivt. Det indebærer, at anvendelsen ikke må påvirke den normale udnyttelse af værket på en skadelig måde, og at anvendelsen ikke på en urimelig måde gør indgreb i ophavsmandens interesser.

Højesteret fandt, at Coops anvendelse af keramikken fremtrådte tydeligt og udgjorde et væsentligt element i gengivelserne på emballage og i tilbudsaviser. Højesteret fandt, at anvendelsen i størstedelen af tilfældene ikke kunne anses af så underordnet betydning i den pågældende sammenhæng, at gengivelserne kunne undtages fra den ophavsretlige beskyttelse. Højesteret pålagde endvidere Coop, at betale et rimeligt vederlagt til Würtz for brugen af keramikservicen, som Højesteret fastsatte til 200.000,00 kr. Højesteret fandt dog ikke, at Würtz havde løftet bevisbyrden for at have lidt et tab pga. markedsforstyrrelse hvorfor Højesteret fastslog, at Würtz ikke var berettigede til yderligere kompensation.

Læs hele dommen her:
http://domstol.fe1.tangora.com/media/-300016/files/171-17.pdf?rev1

7. Den danske forbrugerombudsmand vurderer at invitationer på LinkedIn kan være omfattet af spamforbuddet

Den danske forbrugerombudsmand ('Forbrugerombudsmanden') traf den 9. januar 2019 afgørelse i sag 18/16364, der omhandlede, hvorvidt invitationer på LinkedIn kan være omfattet af spamforbuddet i lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov') § 10, stk. 1. Forbrugerombudsmanden havde modtaget en forespørgsel fra en erhvervsdrivende, der ønskede at invitere beslutningstagere til sit netværk.

Forbrugerombudsmanden vurderede, at invitationer på LinkedIn er elektronisk post, som omtalt i den danske markedsføringslovs § 10, stk. 1. Hvis henvendelserne sendes med henblik på markedsføring, vil betingelserne i den danske markedsføringslovs § 10, stk. 1 være opfyldt, og henvendelserne vil dermed være omfattet af spamforbuddet.

I den pågældende sag ville den erhvervsdrivende i forbindelse med invitationen skrive: "jeg har set din profil her på LinkedIn og tror, at vi måske kan drage nytte af hinandens viden. Jeg håber derfor, at du vil være en del af mit netværk." Det var efter Forbrugerombudsmandens opfattelse en invitation med henblik på markedsføring af den virksomhed, som den erhvervsdrivende var direktør i. Således var en sådan invitation omfattet af spamforbuddet.

Læs hele afgørelsen her:
https://www.forbrugerombudsmanden.dk/find-sager/markedsfoeringsloven/sager-efter-markedsfoeringsloven/spam/invitationer-paa-linkedin-kan-vaere-omfattet-af-spamforbuddet/

8. Forbrugerombudsmanden træffer afgørelse i sag om e-mails sendt via affiliate-netværk

Den 20. februar 2019 traf den danske forbrugerombudsmand ('Forbrugerombudsmanden') afgørelse i sag 18/12182, mellem 12 personer og en bank. Sidstnævnte havde via et såkaldt affiliate-netværk sendt mails med markedsføring til forbrugere. Personerne havde modtaget 18 mails sendt fra 15 forskellige domæner, som alle indeholdt markedsføring fra Banken.

Spørgsmålet i sagen var herefter, om de omtalte e-mails var sendt i strid med spamforbuddet i § 10 i lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov').

Banken forklarede under sagen, at den ikke ejede de 15 domæner, hvorfra de omhandlede e-mails var afsendt. Endvidere forklarede ban-

ken, at den ikke vidste at e-mailene var blevet fremsendt til personerne, idet Banken havde indgået et samarbejdet med et medie- og markedsføringsbureau om markedsføring via e-mails. Medie- og markedsføringsbureauet havde i den forbindelse overladt opgaven til et affiliate-netværk, som sendte de pågældende e-mails ud til de 12 personer.

Banken kunne ikke dokumentere, at personerne, der havde modtaget de pågældende e-mails havde givet samtykke hertil. Forbrugerombudsmanden fandt derfor, at banken havde overtrådt den danske markedsføringslovs spamforbud i § 10, og bemærkede i denne forbindelse, at banken ikke kunne undgå strafansvar ved at lade samarbejdspartnere, herunder affiliate-netværk, håndtere markedsføring. Forbrugerombudsmanden indskærpede derfor markedsføringsreglerne over for Banken, og underrettede ligeledes affililate-netværket om, at de kunne ifalde ansvar for medvirken til overtrædelse af den danske markedsføringslov.

Læs hele afgørelsen her: *https://www.forbrugerombudsmanden.dk/find-sager/markedsfoeringsloven/sager-efter-markedsfoeringsloven/spam/mails-sendt-via-affiliate-netvaerk-var-spam/*

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

simonsen vogtwiig

Hedda Baumann Heier
og Rune Ljostad

Oslo tingrett:

JALLASPRITE funnet å stride med varemerkeloven

Den 16. april 2019 avsa Oslo tingrett dom i tvisten mellom The Coca-Cola Company («Coca-Cola») og O. Mathisen AS («O. Mathisen»). Saken gjaldt spørsmål om varemerkeinngrep, brudd på god forretningsskikk og erstatning.

Bakgrunnen for tvisten er at O. Mathisen, som er en norsk brusprodusent, lanserte i februar 2018 et mineralvann med sitronsmak under navnet JALLASPRITE. Coca-Cola, som eier varemerket SPRITE i Norge, reagerte negativt på dette og henvendte seg til O. Mathisen med krav om at bruken av kjennetegnet skulle opphøre. I løpet av våren var det korrespondanse mellom partene. Utover høsten ble saken omtalt i media. I begynnelsen av oktober gjorde O. Mathisen det kjent overfor Coca-Cola at man ville endre navnet til JALLAXXXXXX.

Coca-Cola tok deretter ut søksmål og midlertidig forføyning for Oslo tingrett. I forføyningssaken fikk Coca-Cola delvis medhold ved at O. Mathisen AS ble pålagt å ikke benytte navnet JALLAXXXXXX i salg, distribusjon og markedsføring av sine brusprodukter. Avgjørelsen ble anket av begge parter, men lagmannsretten forkastet ankene.

I tingrettens dom av 16. april, som gjelder avgjørelsen av hovedkravet i saken, behandles tre hovedspørsmål. For det første om bruken av navnet JALLASPRITE innebar et inngrep i Coca-Colas varemerke SPRITE etter varemerkeloven § 4. For det andre om bruken av navnet JALLAXXXXXX var i strid med god forretningsskikk etter markedsføringsloven § 25. For det tredje om O. Mathisen skal svare erstatning til Coca-Cola i form av rimelig lisensavgift.

Tingretten besvarte alle spørsmålene bekreftende. Bruken av navnet JALLASPRITE ble funnet å være en krenkelse av varemerkelovens § 4 annet ledd som bygger på varemerkedirektivets artikkel 5.2 om velkjente varemerker. Bruken av navnet JALLAXXXXXX ble funnet å være i strid med markedsføringslovens § 25 som angir at det i næringsvirksomhet ikke må foretas handling som strider mot «god forretningsskikk» næringsdrivende i

mellom. Retten fant at bruken av navnet var en slik illojal konkurransehandling og begrunnet dette med særlig henvisning til bakgrunnen for navnevalget og O. Mathisens bruk av media og publisiteten rundt konflikten for å markedsføre produktet. Retten fant også at det skulle tilkjennes en rimelig lisensavgift for bruken av både JALLASPRITE og JALLAXXXXXX etter varemerkelovens § 58 og markedsføringsloven § 48b. Ved utmålingen ble det lagt vekt på at det var snakk om inngrep i et sterkt varemerke med en høy markedsandel, og lisensavgiften ble satt til 17 % av omsetningen av O. Mathisens sitronbrus ved bruk av de ulovlige kjennetegnene. I tillegg til kompensasjon, ble O. Mathisen ilagt forbud mot å bruke JALLASPRITE og JALLAXXXXXX alene eller som del av et kombinert kjennetegn. Selskapet ble også pålagt ulike plikter knyttet til tilbakekallelse, merking og destruering av flasker, etiketter og annet markedsføringsmateriell med kjennetegnene.

I skrivende stund er det ikke kjent om avgjørelsen er anket.

Les hele avgjørelsen med referanse TOSLO-2018-149601-2.

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

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

Bird & Bird

Karin Söderberg
och Kajsa Zenk

Beräkning av skälig ersättning vid upphovsrättsintrång

Högsta domstolen har gett vägledning i frågan om bestämmande av skälig ersättning vid intrång i upphovsrätt genom tillgängliggörande av filer på en webbplats för illegal streaming. Domstolen underkände den fiktiva licensupplåtelse som rättighetshavaren åberopat som beräkningsgrund och baserade istället bedömningen på den utredning som presenterats av parterna.

Bakgrund

Den som i strid mot upphovsrättslagen utnyttjar ett verk ska betala skälig ersättning för utnyttjandet till rättighetshavaren (54 § 1 st. upphovsrättslagen (URL)). Tanken är att skälig ersättning ska utgå med ett belopp som utgör den licensavgift, eller motsvarande, som rättighetshavaren skulle ha erhållit om utnyttjandet skett på laglig väg. Hur sådan skälig ersättning ska beräknas är dock inte helt tydligt.

Fyra person dömdes av tingsrätten i maj 2017 till ansvar för att ha gjort intrång i Aktiebolaget Svensk Filmindustris (SF) upphovsrätt under perioden 2 december 2013 till 19 januari 2015 genom att olovligen tillgängliggöra filmverk för allmänheten genom illegal streaming på webbplatsen dreamfilm.se.[1] I samband med åtalet mot de fyra hade SF yrkat skälig ersättning med avseende på en av filmerna som fanns tillgängliga på streaming webbplatsen, "Maria Wern – Drömmen förde dig vilse". Som grund för yrkandet om skälig ersättning åberopade SF en hypotetisk licensavgift, baserad på en uppskattning av vad en tänkt licenstagare skulle ha betalat för att få utnyttja verken på det sätt som de tilltalade gjort. Den hypotetiska licensavgiften bestämdes med hjälp av utlåtanden från sakkunniga inom filmbranschen och utgjorde en "totallicens", utan begränsning i tid och antal utnyttjanden. Beräkningen utgick från att SF vid en licensiering skulle ha erhållit ersättning för hela filmens produktionskostnad, samt en försäljningsvinst om 20 %. Slutligen gjordes ett rejält säkerhetsavdrag om 2/3, med beaktande av att den hypotetiska licensen inte utgjorde en etablerad licensmodell. Den skä-

1 Dom i mål nr B 226-15 meddelad 2017-05-09

liga ersättning som yrkades landade på 8 miljoner kr.

Tingsrätten bestämde den skäliga ersättningen till 1 miljon kr. Att beloppet sattes så mycket lägre än det yrkade motiverades av tingsrätten med att även om metoden med en hypotetisk licensavgift är etablerad i praxis så måste principens tillförlitlighet i det enskilda fallet vara "avhängig sakförhållandenas närhet till verklig upplåtelse". I det aktuella fallet menade tingsrätten att den hypotetiska licens som åberopats innehöll brister som var nödvändiga att beakta. Bland annat ansågs att modellen var baserad på en distributionsmodell som inte var genomförbar med hänsyn till hur marknaden faktiskt fungerar.

Hovrätten, som inte ifrågasatte den åberopade beräkningsmetoden i sig och inte heller ansåg att det fanns anledning att betvivla de uppgifter som modellen baserats på, höjde ersättningen i förhållande till vad som utdömts i tingsrätten till 4 miljoner kr.[2] Att beloppet ändå tydlig understeg det yrkade förklarades av att det enligt hovrätten framstod som mycket osäkert vad verket faktiskt hade varit värt för rättighetshavaren vid en sådan förhandling som beräkningsmodellen grundats på. Inte heller ansågs det klart att en sådan licensavgift skulle täcka hela filmens produktionskostnad.

Efter att hovrättens dom överklagats av två av de fyra tilltalade, MD och AI, meddelade Högsta domstolen (HD) prövningstillstånd med avseende på hur den skäliga ersättningen skulle beräknas. Domen meddelades i januari i år.[3]

Högsta domstolens avgörande

Skälig ersättning

HD inledde med att konstatera att den skäliga ersättningen som ska utgå enligt 54 § 1 st. URL ska ses som en värdeersättning för obehörigt nyttjande och ska betalas ut oavsett om intrånget skett i ond eller god tro. Vidare angavs att den skäliga ersättningen ska betalas även om rättighetshavaren inte har lidit någon förlust. Ersättning är att se som vederlag för det otillbörliga utnyttjandet och ska ses som separat från eventuellt skadestånd som kan utbetalas i händelse av ytterligare skada.

Vad gäller storleken på den skäliga ersättningen konstaterade HD att tanken är att den skäliga ersättningen ska bestå av den fullständiga ersättning som rättighetshavaren skulle ha erhållit om utnyttjandet skett på lagenlig väg. Det här motiveras av att en intrångsgörare inte ska hamna i ett mer fördelaktigt läge än den som följer upphovsrättslagen. HD hänvisade till förarbetena och det som anges där om att ersättningen därför ofta kan bestämmas baserat på gällande avgiftsprinciper inom en viss bransch. Ersättningen fastställs då som om ett avtal på förhand ingåtts avseende ersättning, det vill säga genom en hypotetisk licens.

HD fortsatte sitt resonemang med att konstatera att även för de fall någon sådan etablerad avgiftsprincip inte står att finna kan en rättighetshavare välja att grunda den yrkade ersättningen på en fingerad licens. Då är utgångspunkten ett fingerat avtal mellan rättighetshavaren och någon i branschen avseende förvärv av rätten att förfoga över ett verk av aktuellt slag "på det sätt, i den omfattningen och för det ändamål" som skett genom intrånget. HD påpekade dock att beräkningsmetoden i en sådan situation kan vara förenad med svårigheter. Särskilt anges att den baseras på antagandet att parterna i en sådan avtalssituation skulle ha kommit överens om en licensavgift. Som en sista möjlighet får, för de fall det saknas förutsättningar för att tillämpa en sådan fingerad licens som beräkningsgrund, ersättningen istället bestämmas baserat på den utredning som har lagts fram i målet av parterna.

Bevisskyldighet för skälig ersättning

HD påpekade att det är rättighetshavaren som har bevisskyldigheten för vad som är ett marknadsmässigt pris eller, då sådant pris saknas, för de omständigheter som ligger till grund för domstolens bedömning av vad som utgör en skälig ersättning. Det konstaterades också att graden av bevissvårighet kan behöva beaktas samt att det kan finnas anledning att beakta bevislättandsreglerna i 35 kap 5 § första meningen rättegångsbalken (regeln avser skadestånd men kan tillämpas analogt i förhållande till skälig ersättning).

Bedömningen av den skäliga ersättningen i det aktuella fallet

HD gjorde sedan en bedömning av SF:s fiktiva licens (användningen av begreppet fiktiv licens verkar i sammanhanget användas som ett samlingsord för den hypotetiska licens och den fingerade licens som HD tidigare nämnt). Vid bedömningen uttryckte HD inledningsvis att det kan "hållas för visst" att en förhandling mellan en rättighetshavare och en licenstagare i form av en aktör som erbjuder gratis streaming av en stor mängd filmer inte hade kunnat leda till att rättighetshavaren erhållit 4 miljoner kr för rättigheterna att utnyttja en film. Vidare påpekade HD att den av SF åberopade beräkningsgrunden inte utgått ifrån det faktum att utnyttjandet varit tidsbegränsat samt att det endast avsett överföring till allmänheten genom streaming. Den fiktiva totallicens som SF presenterat, där licensavgiften grundats på filmens produktionskostnad och SF:s vinstkrav, kunde av den anledningen inte läggas till grund för bestämmandet av den skäliga ersättningen.

Då den presenterade beräkningsmodellen, den fiktiva licensupplåtelsen, inte kunde läggas till grund för beräkningen fick ersättningen istället bestämmas med beaktande av den utredning som parterna har lagt fram i målet. Här beaktade HD bland annat att filmen gjorts tillgänglig via en av SF:s webbplatser, hade kunnat kö-

2 Dom i mål nr B 1565-17 meddelad 2018-02-20

3 Dom i mål nr B 1540-18 meddelad 2019-01-21

pas på DVD samt visats på TV4. I samband med det påpekades att den höga efterfrågan som inledningsvis råder då en film offentliggörs är snabbt avtagande. Vidare uppmärksammade HD att det tillgängliggörande som skett på dreamfilm.se pågick under 13 månader samt att webbsidan var en känd webbsida för streaming. HD beaktade också att det hade gjorts sannolikt att filmen funnits tillgänglig på åtminstone en annan webbplats under samma period.

HD hänvisade till de uppgifter som lämnats av sakkunniga avseende vinster vid internetbaserad uthyrning och licenser för betal-tv samt det proportionerliga förhållandet mellan legal och illegal konsumtion men angav härefter att flera av dessa uppgifter måste bedömas med "betydande försiktighet". Det påpekades också att någon utredning avseende antalet tillfällen som filmen gjorts tillgänglig via dreamfilm.se, eller under vilken tid de lagliga transaktionerna skett, inte lagts fram. HD ifrågasatte också om det inte funnits andra uppgifter som hade kunnat presenteras av parterna i målet men uttryckte i sammanhanget att det varit svårt att få fram uppgifter som varit relevanta för bedömningen.

HD:s beslut

Ersättningen bestämdes baserad på den utredning som lagts fram i målet, trots att den enligt HD inte gav någon mer bestämd ledning. HD beaktade den relativt långa tid under vilken intrånget pågick, när och under vilka former filmen hade gjorts tillgänglig på laglig väg, uppgifter om förekommande licensuppgifter, den faktiska försäljningen och om illegal streaming samt intäkten efter avdrag för kringkostnader vid internetbaserad uthyrning. Vid en samlad bedömning fastställde HD att den skälig ersättning uppgick till 400 000 kr (det vill säga 1/10 av den ersättning som utdömts av hovrätten).

Kommentar

Avgörandet presenterar en metod för hur den skäliga ersättningen ska fastställas vid den här typen av upphovsrättsintrång. I första hand ska som framgått ersättningen bestämmas utifrån en hypotetisk licensavgift, baserad på etablerade avgiftsprinciper inom en viss bransch. Att en sådan beräkningsmetod ska användas framgår av förarbeten och tidigare praxis. En hypotetisk licensavgift används alltså då det går att fastställa något som liknar en färdig avtalsmodell som kan tillämpas i det specifika fallet.

För det fall en etablerad avgiftsprincip inte står att finna ger HD genom avgörandet uttryck för ett andra steg av bedömningen, nämligen beräkning av ersättningen baserad på vad HD uttrycker som ett "fingerat licensavtal". Det framstår således som att HD avser göra en distinktion mellan ett "hypotetiskt" och ett "fingerat" licensavtal. Det som avses med tillämpningen av det sist nämnda är att beräkningsmodellen baseras på ett tänkt avtal mellan rättighetshavaren och någon som önskar utnyttja verket på det sätt som är aktuellt. Utgångspunkten är alltså inte, som vid tillämpningen av en hypotetisk licens, någon typ av färdig, etablerad, avtalsmodell som kan anses föreligga i branschen. Beräkningsgrunden är i det här steget baserad på antaganden om att en överenskommelse av ett visst slag skulle ha nåtts mellan parterna och därmed är den också, som HD angett i domen, förenad med svårigheter. Frågan kan ställas när ett sådant fingerat licensavtal kan anses bevisat ligga tillräckligt nära verkligheten för att faktiskt kunna läggas till grund för en beräkning.

Då förutsättningar saknas för både en hypotetisk- och en fingerad licens som grund för beräkningen får bedömningen i sista hand göras baserad på parternas utredning.

Avgörandet, där ersättningen baserades på den utredning som presenterats av parterna, motiverar upphovspersoner och rättighetshavare, i egenskap av part som bär bevisbördan, att presentera fullgod utredning i målet. HD ifrågasatte i det aktuella målet om det inte funnits andra uppgifter som kunnat presenteras av parterna samt påpekade att den utredning som presentats i målet inte gav någon närmare ledning för bedömningen. Anledningen är förmodligen att den lagts fram med den fiktiva licensen som utgångspunkt.

Även om HD sänkte ersättningen betydligt i förhållande till det belopp som utdömts av hovrätten får avgörandet anses innebära ett tydligt ställningstagande mot den typ av intrång som var aktuellt i målet. Det faktum att den skäliga ersättningen som utdömdes enbart avsåg utnyttjandet av en enda film visar på att domstolen är öppen för att ålägga organisatörer av liknande illegala webbplatser att betala betydande summor i ersättning till rättighetshavare. Webbplatser av det aktuella slaget innehåller nämligen sällan ett enda verk, utan tvärt om en mycket stor mängd skyddade verk, tillhörande olika rättighetshavare. De enorma summor som organisatörerna riskerar att få betala i ersättning måste (förhoppningsvis) verka avskräckande för den som funderar på att skapa en sådan webbplats.

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

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

SELMER

Dan Sørensen

Tradisjonelle escrow-avtaler er ikke tilpasset dagens teknologileveranser

Bruken av escrow-avtaler øker. Nye teknologier og leveransemodeller utfordrer leverandører av escrow-tjenester og reguleringen i tradisjonelle escrow-avtaler.

Det er ikke uvanlig at kunder som anskaffer it-systemer krever at leverandøren inngår avtale med en uavhengig tredjepart om deponering av kildekode og annet relevant materiale (som blant annet dokumentasjon, databasestruktur og konfigurasjoner) hos denne tredjeparten – såkalte escrow-avtaler. Som regel er kunden også part i slike avtaler, og avtalene er mest aktuelle ved anskaffelse av forretningskritisk programvare.

Tradisjonelt har programvare blitt anskaffet ved et engangskjøp av en evigvarende lisens, men hvor leverandøren har levert vedlikehold, videreutvikling og brukerstøtte som en løpende tjeneste. Programvaren har kunden driftet selv eller hos en driftsleverandør.

En escrow-avtale skal sikre kundens interesser hvis leverandøren går konkurs eller av andre grunner ikke vil eller ikke er i stand til å levere vedlikehold og videreutvikling av den leverte programvaren. I slike tilfeller vil kunden kunne få utlevert kildekode og annet deponert materiale som gjør kunden i stand til selv eller ved hjelp av andre å vedlikeholde og eventuelt videreutvikle programvaren. Dette vil kunne sikre kundens investering og kontinuerlig vedlikehold av programvaren.

Deponering av kildekode kan også være en fordel for nystartede eller mindre leverandører med lite historikk og få referanser. Disse leverandørene vil dermed likevel kunne bli akseptert av kunden fordi kunden har sikret sine interesser hvis umodne eller svake leverandører ikke klarer å levere som avtalt.

Vi opplever nå en tydelig økning i bruk av escrow-avtaler – spesielt når det gjelder anskaffelse av ny teknologi som ofte er under utvikling hos nystartede eller mindre teknologiselskaper. Selv om slik teknologi i seg selv ikke nødvendigvis blir kategorisert som forretningskritisk programvare, kan teknologien likevel gi kunden en stor konkurransefordel og den potensielle fortjenesten og/eller innsparing kan være betydelig. I tillegg ser vi også at flere og flere kunder investerer i nystartede selskaper – enten ved å bli deleier eller ved å medfinansiere utviklingen av ny teknologi. I disse situasjonene vil escrow-avtaler kunne være en fordel for både kunden og leverandøren. Kunden kan sikre sine investeringer og leverandøren får innpass i et marked til tross for mangel på historikk og omdømme.

Det er imidlertid flere forhold som gjør at flere av de tradisjonelle escrow-avtalene ikke er tilpasset dagens leveransemodeller av programvare. Leverandører som utvikler ny teknologi og/eller er umodne leverandører vil kontinuerlig både utvikle og publisere nye versjoner av programvaren. Flere av de tradisjonelle escrow-avtalene/-leverandørene har ikke tilrettelagt for hyppige – kanskje daglige – utgivelser av nye versjoner med etterfølgende verifikasjon av det deponerte materialet.

De norske standardavtalene for leveranse av programvare, vedlikehold og tjenester har svært begrenset regulering av leverandørens plikt til å tilby escrow-avtaler. Det er spesielt viktig for kunden å være oppmerksom på dette når partene avtaler endringer i reguleringen av rettigheter til kildekode som begrenser kundens mulighet til selv å vedlikeholde programvaren.

I tillegg er det nå vanlig å levere programvaren som en skytjeneste – typisk som en "-as-a-Service". Dette gjør at kunden i mindre grad enn tidligere har kontroll på programvaren som brukes, dokumentasjon av programvaren og databaser. Kunden har også mindre kontroll på sine egne data. For disse leveransemodellene er verken escrow-leverandørene eller escrow-avtalene tilpasset, og deponeringstjenesten og

avtalen bør også ta høyde for deponering av kjørende programvare og kundens data i tillegg til kildekode og annet relevant materiale. Verifikasjonsprosedyrene blir følgelig også viktigere og mer omfattende for å sikre mot avbrudd i bruk av tjenesten.

Selv om det antas at konkursboet til en programvareleverandør ikke kan hindre en utlevering av deponert materiale til kunden under en escrow-avtale i henhold til dekningsloven § 7-3, har ikke denne problemstillingen blitt satt på spissen – ennå. En medvirkende årsak til dette kan være at boet i utgangspunktet ikke har muligheten til å hente ut økonomiske verdier ved å hindre utlevering av kildekode (med en begrenset lisens til eget vedlikehold) til en kunde som allerede har betalt en evigvarende lisens for bruksretten.

Det kan imidlertid bli interessant å se om de konkursrettslige problemstillingene blir satt på spissen i fremtidige escrow-avtaler og om disse avtalene vil stå seg. Dette gjelder spesielt escrow-avtaler knyttet til ny teknologi hvor utleveringen av deponert kildekode gjør at kunden får full innsikt i selve teknologien som i seg selv kan representere en betydelig økonomisk interesse for et konkursbo. Videre vil leveranse av programvare som en løpende tjeneste gjøre at konkursboet i større grad kan realisere verdier ved fortsatt leveranse til kundene – spesielt ved for eksempel salg av boet til selskaper som vil videreføre leveransene.

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

ANNET NYTT

Gorrissen Federspiel

Tue Goldschmieding

Det danske virksomhedsråd for IT-sikkerhed anbefaler en ny mærkningsordning for it-sikkerhed

Det danske virksomhedsråd for IT-sikkerhed ('Virksomhedsrådet') udgav i januar 2019, en rapport hvori virksomhedsrådet anbefalede at indføre en frivillig mærkningsordning for it-sikkerhed rettet mod små- og mellemstore virksomheder.

Virksomhedsrådet er et råd nedsat under det danske Erhvervsministerium, med det formål at komme med anbefalinger til den danske regering om digital sikkerhed og datahåndtering.

Mærket skal signalere, at deltagerne har implementeret en række it-sikkerhedsforanstaltninger, sådan at virksomheden er i stand til at modstå de mest almindelige sikkerhedshændelser. Mærket kan således være et værktøj for de deltagende virksomheder til at vise, at de efterlever eksempelvis leverandørkrav om datasikkerhed. Dette kan ifølge Virksomhedsrådet sikre at den deltagende virksomhed ikke fravælges til fordel for større virksomheder pga. manglende it-sikkerhed eller manglende synlighed omkring virksomhedens it-sikkerhed.

Mærket skal således, ifølge Virksomhedsrådets anbefaling, sigte på at hjælpe deltagerne med at få styr på deres it-sikkerhed, og hjælpe virksomhedens potentielle kunder med at tage en informeret beslutning når de vælger deres leverandører.

Virksomhedsrådet anbefaler, at mærket skal være frivilligt, og at det bør blive udviklet i samarbejde med relevante parter, herunder myndigheder og brancheorganisationer. Det specifikke indhold, organisation, pris og certificeringsproces fremgår ikke af anbefalingen.

Virksomhedsrådet anbefaler dog, at øget medarbejderbevidsthed skal indgå som et vigtigt element i mærket og at krav til back-up løsninger og løbende opdatering ligeledes bør indgå.

Læs hele udtalelsen her: *https://em.dk/media/12881/anbefaling-om-et-maerke-for-it-sikkerhed-2.pdf*

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

Returadresse:
Lovdata
Postboks 2016 Vika
NO-0125 Oslo
Norge

Nytt fra

LOVDATA

Markering av tekst i Lovdata Pro

I Lovdata Pro kan man i hvilket som helst dokument markere tekst på tre måter:

- Utheving
- Understreking
- Margering (vertikal strek i marg)

Det kan også skrives merknader til den markerte teksten. Merknaden blir synlig i høyre marg. Aktiver markeringsverktøyet fra toppmenyen ved å hake av for «Bruk markeringsverktøy» og marker ved å bruke musepekeren – plasser markøren på ønsket sted, hold museknappen inne, beveg markøren over ønsket tekst og slipp.

Markeringer og merknader kan du få med i nedlastede dokumenter – hak av i boksen «Med merknader og markeringer» i vinduet for nedlasting.