Lov & Data

Nr. 149
Mars 2022
Nr. 1/2022

Innhold






Lov&Data

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

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

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

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

Abonnementspriser for 2022
Norge: nkr 385,- pr. år
Utland: nkr 468,- pr. år
Studenter, Norge: nkr 182,- pr år
Studenter, utland: nkr 244,- pr. år
Alle fritt tilsendt.

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

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

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

Trykk og layout: 07 Media – 07.no

Leder

Fremtidens it-kontraktret

Den kontraktuelle regulering af it-leverancer har været et voksende arbejdsområde for jurister gennem mange år. I dag udgør området en egentlig disciplin i egen ret, og mange jurister har it-kontraktretten som eneste eller væsentligste arbejdsområde. Den specialviden, som fagets udøvere besidder, er blevet øget i takt med at også kompleksiteten er blevet øget. En dygtig it-kontraktjurist skal have indgående viden om obligationsret, kende de relevante standardkontrakter og markedsstandarderne for de forskellige reguleringstemaer, have brancheindsigt, teknologikendskab, forståelse for projektstyring m.m. Sådan har det været gennem mange år, uanset om der skal udarbejdes kontrakter om systemudvikling, systemimplementering eller outsourcing af drift til en it-leverandør. Noget er imidlertid ved at ændre sig i disse år, og it-kontraktretten er under en større udvikling, end den har været længe. Dette skyldes navnlig to forhold.

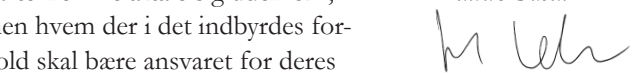
Det først, og væsentligste, forhold er den massive overgang til cloudbaseret ydelser, vi ser i disse år. Denne overgang, der med rette kan kaldes for en egentlig cloud-revolution, påvirker it-kontraktretten på flere måder. Selvom der er mange udbydere af forskellige cloudløsninger, præges markedet af få store aktører, særligt når det kommer til infrastrukturydelser (med Microsoft Azure og AWS som de førende). Dette betyder, at it-kontraktjurister må kende disse aktørers standardvilkår (der kan være komplekse og svært gennemskuelige), have en fornemmelse af, hvilke dele af vilkårene, der kan forhandles og være i stand til at afdække den risikoprofil, som vilkårene giver. Det betyder endvidere, at den type aftale, hvor en leverandør påtager sig at integrere clouddydelser fra tredjeparter med kundens øvrigt it-landskab, får stigende betydning. Ofte vil det være en form for hybridaftaler, der både kan omfatte rådgivning, udvikling, klassisk drift, datakonvertering mv.

Det andet forhold er en øget mængde regulering af betydning for it-kontraktretten. Denne tendens blev for alvor indledt med databeskyttelsesforordningen (GDPR) fra 2018. Databeskyttelsesretten påvirker alle dele af it-kontraktretten, uanset om der reguleres system-

udvikling (hvor der bl.a. skal iagttages principper om data beskyttelse gennem design og begrænsninger i adgang til at bruge personoplysninger som testdata), klassisk (on premise) drift (hvor der skal indgås databehandleraftale og bl.a. tages stilling til erstatningsansvaret for persondatabrud) eller cloudydelser (hvor navnlig spørgsmålet om tredjelandsoverførsler fylder meget). Også øgede regulatoriske krav til it-sikkerhed som det kendes fra den finansielle sektor og det kommende NIS2-direktiv påvirker it-kontraktretten. Denne udvikling på forventes at fortsætte, fordi it-systemer og data har så stor samfundsbetydning i dag. Af andre kommende lovgivningsinitiativer, der vil påvirke it-kontraktretten, kan nævnes AI forordningen og Kommissionens netop fremsatte forslag til en Data Act. Det er nyt, at så mange præceptive lovregler har betydning for it-kontraktretten. Fagets udøvere skal selvsagt kende disse regler, men skal også forholde sig til, hvordan de skal håndteres kontraktuelt. De grundlæggende forpligtelser kan parterne ikke aftale sig uden om, men hvem der i det indbyrdes forhold skal bære ansvaret for deres overholdelse og betalingen knyttet hertil, vil ofte kunne aftales.

Cloudrevolutionen vil betyde, at nogle af de klassiske it-kontrakttyper, særligt on premise driftsaftalerne, vil få mindre betydning i de kommende år. De vil dog næppe helt forsvinde. I stedet vil udviklingen betyde, at it-kontraktretten udvides med nye kontrakttyper og nye lovregler, der påvirker området. Det er derfor en både krævende og spændende fremtid, som it-kontraktjurister kan se ind i.

Henrik Udsen



Selvbetjent rettshjelp

Av Dag Wiese Schartum og Sunniva Slotten

Våren 2021 gjennomførte vi en kartlegging av rettshjelptjenester på nett i Norge. Dette er tjenester som skal sette brukerne i stand til å finne ut av rettsspørsmål på egenhånd. Vi ønsket å undersøke hvor utbredte slik tjenester var, og gi en ytre beskrivelse av hver tjeneste. Undersøkelsen inneholdt altså ingen kvalitativ vurdering av den rettshjelpen tjenestene kunne gi. Likevel gir den overordnede beskrivelsen indikasjoner på spørsmål om kvalitet. I denne artikkelen skal vi kort gjøre rede for noen hovedresultater fra undersøkelsen og dele noen refleksjoner om verdien av slike tjenester.[1]

Dag Wiese Schartum

Sunniva Slotten

Hva slags tjenester?

Undersøkelsesopplegget var åpent og skulle legge til rette for å finne ulike typer tjenester, uavhengig av våre forventninger. Likevel fant vi stort sett bare tjenester som vi forventet: Chatboter, rettskalkulatorer og dokumentutformingstjenester.

En «chatbot» er en robot brukere kan føre en verbal dialog med, i skrift eller tale. Begrepet chatbot forutsetter ingen bestemt teknologi. Tjenestene kan være basert på enkle løsninger som er styrt av forekomst av forhåndsdefinerte stikkord, slik at svar blir gitt ut ifra hvilke slike stikkord eller kombinasjoner av stikkord som forekommer i input fra brukeren. Mer avanserte chatboter bruker maskinlæring og analyse av meningsinnhold i input fra brukeren, basert på statistiske metoder. I de 21 chatboter vi fant var alle bygget på maskinlæring og skriftlig dialog.

Kartleggingen fant også frem til 38 «rettskalkulatorer» pluss flere mindre, lignende tjenester. Dette er digitale tjenester der hovedfunksjonen er å beregne et beløp i samsvar med rettsregler som gir plikter eller rettigheter til å betale, motta eller fordele penger på en bestemt måte.[2] Beregningsmåten vil ofte være avhengig av om visse vilkår er oppfylt, og det vil derfor ofte eksistere alternative beregningsmåter. I tillegg til informasjon om tall vil en rettskalkulator derfor ofte trenge informasjon for å avgjøre om slike vilkår i regelverket er oppfylt.

Rettskalkulatorer inneholder gjerne en forenklet representasjon av rettsreglene, og er ofte utviklet for at brukeren skal kunne gjøre raske anslag, heller enn å komme frem til nøyaktige resultater. En rettskalkulator kan imidlertid tenkes utviklet til et fullverdig beslutningsstøttesystem, med bred representasjon av rettskilder, automatiserte beregninger, og med tett veiledning av brukeren for å sikre at hun leg-

1 Her går vi ikke inn på enkelttjenester. Den interesserte kan lese rapporten og beskrivelsene av hver tjeneste i CompLex 3/2021 *https://www.jus.uio.no/ifp/forskning/om/publikasjoner/complex/2021/*

2 Populært er det vanlig å bruke betegnelsen «kalkulator». Dette er imidlertid en helt generell betegnelse som ikke gir informasjon om at beregningene skjer på bakgrunn av rettsregler. Vi har derfor valgt å føye til «retts» for å markere den særpregede tilknytningen til retten.

ger inn korrekte, fullstendige og oppdaterte opplysninger. Opplysningene brukeren legger inn i rettskalkulatorer kan beskrive virkelige eller tenkte forhold, og kan like gjerne brukes for å undersøke mulige effekter av et regelverk som å finne riktig løsning i en virkelig, aktuell sak.

Rettskalkulatorer er basert på forhåndsdefinerte, faste algoritmer som uttrykker de relevante rettsregler som er bestemmende for hvordan inngitte opplysninger skal behandles for å komme frem til et rettsriktig resultat. Programmet som styrer rettskalkulatorer inneholder med andre ord regler for prøving av vilkår (jf. «hvis – så») og beregninger. Slike algoritmer er statiske, dvs. ikke lærende slik maskinlæringsalgoritmer er.

I tillegg til chatboter og rettskalulatorer fant vi andre tjenester, primært dokumentutformingstjenester. Dette er digitale tjenester som er utformet for å hjelpe brukere å sette opp ulike slag rettslige dokumenter, f.eks. testamenter eller samboerkontrakter. I sin enkleste form er dette dynamiske skjemaer, dvs. forhåndsdefinert oppsett som viser hvordan en bestemt dokumenttype skal struktureres. Tjenestene fungerer slik at brukeren svarer på spørsmål som er bestemmende for utformingen av dokumentet. Dokumentet tilpasser seg basert på svarene brukerne gir. Til slutt produserer systemet et skreddersydd, rettsriktig dokument. De fleste dokumentutformingstjenester vi fant blir tilbudt av advokatfirmaer og forutsetter kundeforhold og innlogging. Vi fikk ikke tilgang til de fleste av disse tjenestene, og kunne derfor ikke gi tilstrekkelig beskrivelse av dem. I det følgende legger vi derfor vekt på chatboter og rettskalkulatorer.

Klassifiseringen i chatboter og rettskalkulatorer er i stor grad uttrykk for konvensjoner om hvordan teknologi kan sette den lege mann og kvinne i stand til å løse rettsspørsmål uten hjelp fra juridisk ekspertise – eller til å oppdage at spørsmålene er så vanskelige at eksperthjelp er nødvendig. Enkelte tjenester vi kartla kan imidlertid sies å overskride typiske kjennetegn for den kategori vi i utgangspunktet plasserte dem i. En tjeneste for økonomisk oppgjør ved skilsmisse, hadde f.eks. et klart bredere tjenesteinnhold enn en typisk rettskalkulator. Selv om sluttresultatet i skillsmissekalkulatoren f.eks. var forslag til økonomisk oppgjør, var det en rekke rettsspørsmål som måtte løses før beregning kunne skje.

Det vil alltid være mulig å utvikle rettskalkulatorer til å gi fullverdig beslutningsstøtte; dvs. slik at brukeren kan få tilgang til forklaring av begreper, vilkårsstrukturer, beregningsmåter, krav til registrering av opplysninger mv. Høye utviklings- og driftskostnader er trolig én viktig grunn til at tjenestene for selvbetjent rettshjelp holdes på «kalkulatornivå» og ikke bygges videre ut til å gi god støtte i andre spørsmål enn det som direkte gjelder beregninger.

De fleste tjenestene i undersøkelsen var beregnet for bruk av PC. Vi fant imidlertid også seks eksempler på bruk av selvbetjent rettshjelp ved hjelp av app på mobiltelefon. Det kan være grunn til å minne om det store potensialet som trolig ligger i interaktive rettshjelpstjenester basert på mobiler «i lomma», innen rettsområder der enkel input fra brukeren (typisk oppholdssted, jf. GPS), kan utløse input fra databaser som er avgjørende for rettslige reguleringer. Dette gjelder ikke bare identifisering av lokale forskrifter (jf. f.eks. kommunale covid-19-forskrifter), men opplysninger knyttet til naturforhold (fredningsbestemmelser, tilskudd i landbruket mv.), bygningsvern, og oppholdssted/situasjon (f.eks. handel i matvarebutikk og regler om tilsettingsstoffer og produktmerking). Poenget er at interaktive, selvbetjente rettshjelpstjenester også kan være styrt av oppholdssted og situasjon; ikke bare brukerens eksplisitte spørsmål til programvaren. Slik sett kunne en f.eks. tenke seg at Tolletatens app for innførsel av alkohol mv. ble automatisk tilgjengelig på folks mobil på ethvert norsk tollsted, dvs. med GPS-posisjon eller lignende som utløsende input. Vi kommer ikke her inn på de problemstillingene om personvern som dette vil reise.

Noen fellestrekk ved chatbotene i undersøkelsen

Undersøkelsen viser at chatboter brukes i både privat og offentlig sektor. Innen banksektoren ser slike tjenester ut til å være vanlige, og det er ikke skarpt skille mellom støtte til løsning av rettsspørsmål og informasjon om banktjenester mv. virksomheten tilbyr. Det ser ut til å være et typisk trekk ved rettshjelpstjenester som tilbys i en salgssituasjon at formålet både er å bidra til å løse rettsspørsmål og til å fremme salg. Det kan være grunn til å være bevisst på faren for at rettshjelpen ikke alltid er bredere og bedre enn salgsformålet begrunner, og at det derfor bør gis god informasjon om hva rettshjelpstjenesten kan og *ikke* kan bistå med. I motsatt fall kan slike tjenester stå i fare for å villede.

Med ett unntak har vi ikke funnet chatboter hos advokatkontorer. En forklaring kan være at disse lever av å gi juridisk rådgivning, og selger ikke samtidig andre tjenester slik f.eks. bank- og forsikringsbransjen gjør. Profesjonell juridisk rådgivning må normalt være på et helt annet faglig nivå enn hva chatboter kan gi. Allment tilgjengelige chatboter som gir ufullstendige og upresise svar på rettslige spørsmål, vil neppe rekruttere betalingsvillige kunder til fullgode rettshjelpstjenester. Samtidig vil tjenester basert på chatbot kunne gi opphav til misforståelser og feil, og dermed rettstap som et advokatfirma ikke vil ønske å bli assosiert med.

De fleste chatbotene i undersøkelsen er basert på plattformløsninger fra Boost.ai og Kindly, og brukergrensesnittet er likt for alle chatbotene. Likt brukergrensesnitt må forventes å ha stor positiv betydning fordi det gir gjenkjennelse. Det kan trolig også gi felles forventninger om tjenesten ut over det som gjelder den grunnleggende funksjonaliteten i plattformen. Felles plattform gir imidlertid ingen garanti for samme kvalitetsnivå.

Det er veldig vanlig å chatbotene navn, ofte personnavn som Frida, Lucy, Ella, Kommune-Kari, Lara, Ida, Aino og Robot-Anne. Det totale fraværet av mannsnavn kan gi assosiasjoner til kjønnsstereotype oppfatninger om kvinners roller i servicenæringer.

Alle chatbotene som ble kartlagt er styrt gjennom skriftlig kommunikasjon. Det var ingen eksempler i undersøkelsen på stemmestyrte tjenester. Det er vanlig at det i tjenesten blir oppfordret til å bruke stikkord og korte spørsmål i stedet for lengre formuleringer. Tjenestene synes å være følsomme for feilstaving.

Flere av chatbotene dekker alt fra smale til brede emneområder, og er ikke nødvendigvis knyttet til ett bestemt rettsområde. Input fra bruker vil ofte resultere i at tjenesten presenterer brukeren for valgalternativer. På den måten blir det mulig å la chatboten dekke et forholdsvis vidt rettsområde. Chatboten Frida i arbeids- og velferdsforvaltning (NAV) hadde opprinnelig spørsmål om foreldrepenger som utgangspunkt, men er senere utviklet til å svare på en rekke generelle spørsmål innen de fleste av ytelsene NAV arbeider med. Presentasjon av valgalternativer kan sies å «snu dialogen», ved at det snarere er tjenesten som «intervjuer» brukerne enn omvendt. Fordelen er at brukerne ikke trenger å kjenne den relevante begrepsbruken og ha god problemforståelse ellers i like stor grad som om det kun er brukeren og svarene som brukeren gir som styrer dialogen. Jo færre ukonvensjonelle og «uvitende spørsmål» brukeren får stille, jo mindre avansert trenger analysen av input fra brukeren å være for å sikre at det kan gis svar og at svaret oppfattes som relevant av brukerne.

Noen fellestrekk ved rettskalkulatorene i undersøkelsen

Det er markert forskjell mellom offentlige etaters og private virksomheters bruk av rettskalkulatorer. Med ett unntak er det bare banker og forsikringsselskaper som tilbyr slike tjenester i privat sektor, og de aller fleste av disse gjelder pensjoner og boliglån. Til sammenligning fant vi til sammen 21 rettskalkulatorer i offentlige virksomheter, fordelt på 8 forvaltningsetater. En viktig forskjell mellom privat og offentlig sektor, er at offentlige etater har spesielt ansvar for å sette lovgivning ut i livet. De har derfor en spesiell motivasjon og oppfordring til å utvikle hjelpemidler for lett og forsvarlig anvendelse av sine regelverk.

I motsetning til chatbotene holder rettskalkulatorene seg innenfor én bestemt rettighet eller forpliktelse. Slike tjenester bygger altså på en forutsetning om at brukerne kjenner til hvilken ordning deres problem gjelder. I chatboter kan perspektivet i stedet være å hjelpe brukerne til å finne ut hvilken ordning deres problembeskrivelse kan sies å angå. Chatboter kan derfor være godt egnet i kombinasjon med rettskalkulatorer ved at brukeren først får hjelp til å finne ut av om det finnes en ordning som dekker brukerens behov, og deretter blir henvist til en rettskalkulator som hjelper henne å undersøke den konkrete effekten av en aktuell ordning. Kartleggingen vår viser at det er forholdsvis vanlig at chatboter lenker til en kalkulator. Det er også vanlig at chatbotene svarer på spørsmål brukerne har ved å lenke til tekst på nettsider der personen kan lese seg opp på problemstillingen på egenhånd.

Rettskalkulatorene i offentlig sektor gjelder offentligrettslige ordninger om økonomiske plikter og rettigheter. Selv om det er relativt mange av disse (21 av 38), er det samtidig klart at det er mange muligheter for rettskalkulatorer på andre områder for skatter, avgifter, trygder og økonomiske rettigheter. Bare folketrygdloven alene inneholder 17 kapitler som omhandler ulike typer ytelser. NAV har kun utviklet rettskalkulatorer for fem av disse.[3] Et enda viktigere potensial for økt antall rettskalkulatorer, er imidlertid knyttet til etater som i dag ikke har slike tjenester.

Om rettskildebruk og forutsetninger for god rettslig kvalitet

Et fellestrekk ved de tjenester vi har fått tilgang til er at rettskildene som er bestemmende for innholdet av tjenestene er lite fremtredende. Bare et mindretall av tjenester gjør aktivt og tydelig bruk av rettskildene. Det er kun én av kalkulatorene som direkte viser til rettskilder. I andre tilfeller er det mulig å finne relevante rettskilder ved å bruke lenker som oppgis underveis. Navnet på lenkene er gjerne «mer informasjon om ...», noe som ikke spesielt indikerer at lenken går til relevant lov og forskrift mv. Tilbyderne av tjenestene begrunnet gjerne fraværet av rettskilder i at målgruppen ikke er jurister. Et annet argument er at tjenestene bør gi korte og enkle svar. Slike argumenter kan likevel neppe begrunne fravær av rettskilder. For det første vil det være brukere uten juridisk utdanning som likevel har tilstrekkelig juridisk forståelse til å ha stor nytte av relevant lovtekst mv. For det andre behøver ikke informasjon om rettskilder ligge på øverste innholdsnivå, men likevel være synlig og tilgjenge-

3 Pensjonskalkulator, bidragskalkulator, samværskalkulator, dagpengekalkulator (krever innlogging) og foreldrepengekalkulator.

lig i lenker og menyer for den som er interessert.

Rettskalkulatorene representerer en forenklet og ufullstendig representasjon av rettskildene. Noen tjenester opplyser om dette, men ikke alle. Dessuten gis det sjelden anvisning på hva som er dokumentasjonsområdet for tjenesten, dvs. hva som er avgrensingen mot tilstøtende rettsområder og hvilke dette er.

Det kan selvsagt være gode grunner for å gjøre forenklinger i forhold til rettsmaterialet tjenestene bygger på. Et mulig prinsipielt skille går imidlertid mellom åpen forenkling, og skjulte forenklinger og begrensninger. I først nevnte tilfeller får brukerne en oppfordring til selv å vurdere om det er behov for nærmere undersøkelser, mens i det sist nevnte tilfellet skjer en trivialisering av den rettslige situasjonen som fratar brukeren muligheten til å forholde seg til komplekse rettsforhold. Trivialisert regelrepresentasjon kan lede brukerne til å stole på resultatene, også når det ikke er grunnlag for det.

Tilbyderne av selvbetjente rettshjelpstjenester kan alltid velge å gjøre eksplisitt rede for dokumentasjonsområdet, usikkerheter i rettsmaterialet, beregninger mv. Et dilemma som kan oppstå er imidlertid at tydelig avgrensinger i innholdet kan skape usikkerhet blant brukerne og generere individuelle henvendelser med videre spørsmål. Er det tale om gratis selvbetjente tjenester, kan dette ses på som en uønsket effekt. Dersom en også har betalte, individuelle rettshjelpstjenester, kan mangler ved gratistilbud være gagnlig for forretningsvirksomheten dersom den leder til flere betalende kunder. Det er imidlertid måte på hvor usikre og dårlige gratis selvbetjente løsninger kan være og samtidig gi positive effekter på etterspørselen etter betalte tjenester.

Undersøkelsen vår viser at det blir viet lite oppmerksomhet til spørsmål om i hvilken grad og med hvilken frekvens endringer i rettskildebildet fører til oppdatering av tjenestene. Kun én av rettskalkulatorene i undersøkelsen sier når kalkulatoren sist ble oppdatert. I andre tilfeller er det angitt for hvilket år kalkulatoren gjelder for. Ifølge våre undersøkelser ser det ut til å være sjelden at tjenestene er knyttet til automatiske rutiner/varsler om endringer i relevante rettskilder. Dette er i motsetning til tjenester på nettsider mv. som gir rettsinformasjon uten interaktivitet, der det er vanlig at det er lenket direkte til Lovdatas databaser.

Manglende redegjørelse for rettskildemessig grunnlag og ajourhold innebærer at det ikke blir lett for at brukerne å bedømme om tjenesten gir pålitelige svar eller ikke. Brukerne har ofte ikke grunnlag for å bedømme risiko for feil og ufullstendigheter, og om det er behov for å søke supplerende rettshjelp. Samlet sett betyr dette at tjenestene i stor grad er basert på tillit, snarere enn på pålitelig dokumentasjon. På en måte er dette paradoksalt fordi, etter hva vi kan forstå, er alle tjenester forenklet og begrenset, dvs. det er *ikke* grunn til å ha tillit til at tjenestene alltid gir dekkende og riktige resultater. Tilliten må derfor snarere være til at tjenestene «ofte er gode nok».

Avslutning

Vår lille undersøkelse av selvbetjente rettshjelptjenester på nett gir en oversikt over hva som i dag eksisterer med norskspråklige tilbud. Inntrykket er at tjenestene som tilbys er teknisk velfungerende, men likevel enkle. Kanskje *for* enkle. Det er særlig to typer forbedringspotensialer som blir tydelige: For det første kan de fleste tjenester være mye flinkere til å beskrive dokumentasjonsområdet, herunder begrensninger i tjenesten, samt oppdateringsfrekvens. For det andre kan de fleste tjenestene i større grad aktivt bruke og vise til rettskilder; særlig lover og forskrifter som tjenestene direkte bygger på. Poenget er ikke å tvinge brukerne til å forholde seg til vanskelige lovbestemmelser, men å gi dem *anledning* til å sammenholde den rettshjelp som systemene formidler og sentrale deler av det rettskildemessige grunnlaget for rettshjelpen.

Dag Wiese Schartum er professor ved Senter for rettsinformatikk, Det juridiske fakultetet, Universitetet i Oslo.

Sunniva Slotten er masterstudent i forvaltningsinformatikk, Det juridiske fakultetet, Universitetet i Oslo.

Förmedling av programvara omfattas i vissa fall av Agentlagen

– EU-domstolen förändrar förutsättningarna för programvaruförsäljning

Av Johan Hübner

Den 16 september 2021 meddelade EU-domstolen dom i målet ”The Software Incubator Ltd vs Computer Associates (UK) Ltd” (C-410/19)[1] (”The Software Incubator”). Domen kommer att förändra rättsläget för vidareförmedlare av programvara i situationer där slutkunden ges rätt att använda en programvara genom att erhålla en licens direkt från programvarutillverkaren. Så är exempelvis fallet med så kallade partneravtal inom programvaruindustrin. Innan jag går in på omständigheterna i målet bör en viss bakgrund ges.

Sedan 1991 gäller lagen (1991:351) om handelsagentur (”Agentlagen”)[2]. Lagen är en indispositiv skyddslagstiftning för handelsagenter. Genom Agentlagen genomförs direktiv 6/653/EEG[3] av den 18 december 1986 om samordning av medlemsstaternas lagar rörande självständiga handelsagenter.

Johan Hübner

Med en handelsagent förstås enligt 1 § ”den som i en *näringsverksamhet* har avtalat med en annan, huvudmannen, att för dennes räkning *självständigt och varaktigt* verka för försäljning eller köp av *varor* genom att ta upp anbud till huvudmannen eller sluta avtal i dennes namn” (mina kursiveringar).

Direktivets motsvarande skrivning är (kap 1, art 1.1):

”Med handelsagent avses i detta direktiv en *självständig* agent med *varaktig* behörighet att förhandla om försäljning eller köp av *varor* för en annan persons räkning, här nedan kallad huvudman, eller att förhandla om och slutföra sådana affärsuppgörelser i huvudmannens namn och för dennes räkning.”

Som bekant ska tvingande skyddslagstiftning på civilrättens område tolkas restriktivt. Detta har upprätthållits avseende Agentlagen. Det har i svensk rätt fram till nu ansetts att programvaror inte är *varor* i Agentlagens mening. Exempelvis skriver Högsta domstolen i NJA 2008 s 24[4] att (som jag skrivit om i Lov & Data nr nr. 93/08):

”*En tidsbegränsad nyttjanderätt till ett dataprogram [sic!] kan inte anses som en vara. [Agentlagen] är således inte direkt tillämplig på parternas förhållande, och avtalet kan inte heller ges sådan innebörd.”*

Detta uttalande har tillsammans med vissa av tingsrättens uttalanden i samma mål om att Agentlagens tillämpningsområde omfattar ”lösöre” tagits till uttryck för att Agentlagen inte omfattar andra agenter än sådana som säljer lösa saker, dvs fysiska föremål. Agentlagen har således inte ansetts omfatta förmedling av programvarulicenser, olika typer av tjänster m.m.

1 *https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:62019CJ0410&from=EN*

2 *https://lagen.nu/1991:351*

3 *https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:31986L0653&from=EN*

4 *https://lagen.nu/dom/nja/2008s24*

EU-domstolens dom i The Software Incubator ändrar detta förhållande. Frågan i målet rörde The Software Incubator, som i England och Wales, hade vidareförmedlat Computer Associates programvaror genom att tillhandahålla en nedladdningslänk för slutkunderna. The Software Incubator fick provision för de förmedlade affärerna. Programvaran kunde tillhandahållas enligt två olika typer av licenser: en tidsbegränsad licens och en licens som var i tiden obegränsad (dvs. en evig licens). I praktiken tillhandahölls kunderna en evig licens. The Software Incubator väckte talan när Computer Associates sade upp avtalet och krävde avgångsvederlag under den engelska motsvarigheten till Agentlagen (dvs. baserad på samma direktiv). The Supreme Court ställde följande frågor till EU-domstolen (p.24 i domen):

> När ett exemplar av en programvara tillhandahålls en huvudmans kunder på elektronisk väg och inte på ett fysiskt medium, utgör den en 'vara' i den mening som avses med detta begrepp, såsom detta återges i definitionen av en handelsagent i artikel 1.2 i [direktiv 86/653]?
>
> När programvara tillhandahålls en huvudmans kunder på så sätt att kunden beviljas en i tiden obegränsad licens att använda ett exemplar av programvaran, utgör detta 'försäljning av varor' i den mening som avses med detta begrepp, såsom detta återges i definitionen av en handelsagent i artikel 1.2 i direktiv 86/653?"

EU-domstolen konstaterar i den ganska korta domen inledningsvis att begreppen "försäljning" och "vara" inte givits en enhetlig tolkning inom den Europeiska unionen genom direktivet (p.33). Domstolen påpekar att den i sin praxis på andra områden har definierat begreppet "varor" som produkter som kan värderas i pengar och som därmed kan vara föremål för affärstransaktioner (p. 34). Enligt domstolen kan en programvara, såsom den aktuella programvaran, omfattas av denna definition" (p. 35).

Vidare slår EU-domstolen fast att det är en *försäljning* i direktivets mening om ett exemplar av en programvara tillhandahålls genom nedladdning och att ett varaktigt licensavtal för dess användning ingås, mot en ersättning som ger upphovsrättsinnehavaren en ersättning som motsvarar det ekonomiska värdet på exemplaret av rättsinnehavarens verk (p. 40-42). I ett sådant scenario är det således fråga om en övergång av äganderätten till exemplaret.

EU-domstolen kommer således fram till att en programvara, som laddas ned mot en ersättning och köparen får en i tiden obegränsad licens är en försäljning av en vara enligt agentdirektivet och således att den som för någon annans räkning verkar för en sådan försäljning är att anse som en handelsagent enligt samma direktiv. The Software Incubator hade således rätt till avgångsvederlag (som är en av de tvingande rättigheterna en handelsagent erhåller under både direktivet, den engelska lagen och Agentlagen)

För svenskt vidkommande innebär detta en viss förändring av hur begreppet "varor" ska tolkas enligt Agentlagen. EU-rätten säger att svensk rätt ska tolkas direktivkonformt, men det innebär inte att svensk rätt ska tolkas mot sin ordalydelse. Som framgår ovan används ordet "varor" både i direktivet och i Agentlagen. Denna dom kommer således ha betydelse för tolkningen av begreppet "varor" i svensk rätt, och som också framgår tidigare har svenska domstolar hittills tolkat detta närmast som "lösöre"[5].

Som tidigare beskrivits så innehåller många s.k. partneravtal, dvs där en programvarutillverkare ingår avtal med exempelvis en systemimplementatör, bestämmelser med innebörd att systemimplementatören förmedlar programvarutillverkarens produkter till en slutkund och avtal och betalning sker mellan programvarutillverkare och slutkund. Dessa avtal, så länge som de avser tidsobegränsade licenser, kommer nu att anses vara agentavtal och således omfattas av Agentlagens regler om exempelvis avgångsvederlag.

Den uppmärksamma läsaren har säkert redan konstaterat att Högsta domstolens dom från 2008 tog sikte på *tidsbegränsade* licenser medan EU-domstolens dom avsåg *eviga* (dvs i tiden obegränsade) licenser.

Därmed återstår frågan om hur tillhandahållandet av *tidsbegränsade* licenser, liksom det alltmer vanligt förekommande affärsupplägget där programvara levereras i form av en tjänst ("software-as-a-service"), påverkas av EU-domstolens dom. EU-domstolen har inte direkt berört frågan, men följande uttalande kan nog ses som en indikation på hur EU-domstolen kommer behandla frågor om förmedling av tidsbegränsade licenser, och kanske till och med när programvara levereras som en tjänst, om dessa kommer under EU-domstolens prövning:

> 49 Den ändamålsenliga verkan av det skydd som ges genom direktiv 86/653 skulle härvidlag äventyras om tillhandahållandet av en programvara, under de förutsättningar som avses i punkt 43 ovan, skulle uteslutas från begreppet "försäljning av varor" i den mening som avses i artikel 1.2 i direktivet.
>
> 50 En sådan tolkning av nämnda bestämmelse skulle nämligen innebära att personer som med hjälp av modern teknik utför ar-

5 Se för utveckling av detta "Agentlagen, Kommentar till lagen om handelsagentur m.m." Söderlund, Svarts, Tonell, 2014 s. 23

betsuppgifter som är jämförbara med dem som utförs av handelsagenter vilkas uppgifter består i försäljning av fysiska varor, bland annat genom kartläggning och uppsökande av potentiella kunder, inte omfattades av detta skydd.

Vad som talar mot denna eventuella framtida tillämpningsutvidgning är EU-domstolens hänvisningar till bl a *UsedSoft (C128/11)*[6] som rör konsumtion av spridningsrätten av exemplar enligt upphovsrätten. Ett av kriterierna i UsedSoft är bl a att den ursprungliga licensen som upplåtits med en evig licens.

Agentlagens tillämpning kommer således med viss sannolikhet att utvidgas ytterligare. Det finns anledning för programvaruföretag att se över sina avtal och affärsmodeller för antingen hantera dessa risker, eller, om det är möjligt, undvika dem.

Johan Hübner är partner och advokat samt ansvarig för Advokatfirman Delphis Corporate Commercial grupp.

6 *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62011CJ0128&from=SV*

Bruk av konkurrenters kjennetegn i søkemotorannonsering

Høyesterett med endelig avklaring i «Google Ads-saken».

Av Jan Magne Langseth og Nicholas Foss Barbantonis[1]

Innledning

Høyesteretts ferske dom i saken anlagt av flere konkurrerende banker mot Bank Norwegian kommer med viktige avklaringer av hva som er tillatt bruk av konkurrenters kjennetegn i søkemotorannonsering. Det er nå fastlagt at å benytte konkurrenters kjennetegn i seg selv ikke vil kunne være et brudd på god forretningsskikk, og at slik bruk i utgangspunktet er tillatt.

Saken mot Bank Norwegian ble anlagt i 2017 etter at Næringslivets konkurranseutvalg (NKU) hadde kommet til at bankens bruk av konkurrenters kjennetegn for å generere treff for egne annonser ved bruk av Google Ads og Bings annonsetjeneste var i strid med markedsføringsloven § 25. NKUs uttalelse var en oppfølging av dets konsistente praksis fra 2012 (i den såkalte Teppeland-saken). I *Teppeland*-saken ble kjøp av konkurrenters varemerke eller forretningskjennetegn, for å få vist egne annonser, omtalt som illojal snylting på andres opparbeidede goodwill. NKUs konklusjon var at slik praksis er i strid med lovens generalklausul i § 25 hvor det heter at *«I næringsvirksomhet må det ikke foretas handling som strider mot god forretningsskikk næringsdrivende imellom»*.

Jan Magne Langseth

Nicholas Foss Barbantonis

NKUs praksis har vært gjenstand for en hel del kommentarer i juridiske kretser, spesielt etter EU-domstolens dom i *Interflora*-saken i 2011. I *Interflora* kom EU-domstolen til at varemerkeinnehaver ikke er beskyttet mot slik bruk, men derimot at annonsepraksisen – i utgangspunktet – er et uttrykk for sunn og lojal konkurranse næringsdrivende imellom. Noe varemerkerettslig vern kan derfor på generell basis ikke etableres med mindre en gjennomsnittlig internettbruker ikke forledes til å tro at det foreligger en økonomisk forbindelse mellom annonsøren og varemerkeinnehaveren. Varemerketten er fullharmonisert innenfor EØS, og det forelå dermed en klar normkollisjon mellom NKUs praksis og gjeldende varemerkerett. I motsetning til varemerketten er imidlertid ikke markedsretten fullt ut harmonisert.

Dette åpner for at bestemmelsene i markedsføringsloven kapittel 6 om beskyttelse av næringsdrivendes interesser kan anvendes som *supplement* til varemerketten. Konkret i *Bank Norwegian*-saken var det anført brudd på markedsføringsloven § 25. Denne adgangen var uomtvistet, og spørsmålet som Høyesterett måtte ta stilling til var rekkevidden av markedsføringsloven § 25 når det angivelige inngrepet i stor grad var omfattet av spesialbestemmelsene i varemerkeloven.

Saksøkerne anførte for samtlige instanser at Bank Norwegians praksis i seg selv var tilstrekkelig for å konstatere brudd på god forretningsskikkstandarden i markedsføringsloven § 25 – altså at den bakenforliggende «metodikken» – selve *kjøpet* av det betale søkeordet eller frasen var nok til å konkludere med at det forelå brudd på markedsføringsloven.

1 Jan Magne Langseth var Bank Norwegians prosessfullmektig for Høyesterett.

Både tingretten og lagmannsretten konkluderte med at Bank Norwegians praksis ikke var i strid med god forretningsskikk. Høyesterett har nå kommet til samme konklusjon og rettstilstanden er dermed endelig avklart.

Kort om søkemotorannonsering

Søkemotorer muliggjør søk på internett. I praksis skriver brukere ord eller fraser i søkefeltet, hvoretter søkemotoren presenterer en liste med nettsider som rangeres etter hva søkemotoren mener er relevant å vise. Den markedsledende søkemotoren leveres av Google. Det finnes imidlertid flere alternativer som eksempelvis leveres av Microsoft Bing, Baidu, Yahoo, Yandex og DuckDuckGo. Søkemotorer er primært tilgjengelige via nettleser, eksempelvis ved å navigere til Google.com. Populære nettlesere er Chrome, Edge og Safari. Disse kan brukes på datamaskin, mobiltelefoner, nettbrett mv. De fleste moderne nettlesere muliggjør søkemotorsøk direkte i nettadressefeltet, slik at man ikke behøver å først besøke søkemotorens forside, for så å søke. Enkelte søkemotortilbydere tilbyr også søkefunksjonalitet via egne applikasjoner.

Ved søkemotorsøk presenteres søkeren en søketreffliste bestående av «organiske» (ubetalte) og «betalte» treff. I motsetning til organiske treff, korrelerer betalte søketreff med annonsørens betaling for at en konkret nettsideannonse skal komme med i søkeresultatet ved søk på forhåndsbestemte søkeord- eller fraser. Foreliggende sak omhandlet betalte treff. Betalte søketreff (eller annonser) vises i den øvre delen av søketrefflisten. Det er gjerne opp til fire slike annonser øverst til venstre i søketreffet, over de øvrige organiske treffene som kommer under, og på høyre side av søketreffet.

For den enkelte bruker vil annonsene skille seg fra de organiske treffene ved at de er merket med en tekstboks hvor det står «Annonse». Søkemotorenes forretningsmodell avhenger av inntekter fra betalte søketreff. Dersom det er flere annonsører som betaler for plassering under et bestemt søkeord, så rangeres disse i henhold til to primære kriterier. Det første kriteriet knytter seg til såkalte «kvalitetspoeng» som fastsettes i samsvar med blant annet annonsen og den aktuelle nettsiden som annonsen peker mot, herunder relevans og øvrig kvalitet. Det andre kriteriet knytter seg til det aktuelle pengebeløpet som annonsøren byr per klikk for visning under det aktuelle søkeordet. Den annonse som får høyest total poengsum av kvalitetspoeng og bud, vises øverst i trefflisten. Kvalitetspoengene gjør at Google bare vil vise annonser som antas relevante for den som søker.

Google begrenser ikke mot kjøp av konkurrenters kjennetegn som betalte søkeord. Det er imidlertid ikke helt fritt frem. Googles egne retningslinjer inneholder visse begrensinger på bruken av tredjeparters kjennetegn dersom bruken medfører økt forvekslingsfare. Skoleeksemplet på dette er når noen kjøper tredjeparts kjennetegn som søkeord og i tillegg inkluderer kjennetegnet i selve annonseteksten som presenteres overfor brukeren av søkemotoren. Såfremt man ikke inkluderer innehaverens kjennetegn i selve annonseteksten så er det imidlertid etter Googles retningslinjer fullt mulig å kjøpe konkurrenters varemerker som søkeord.

Høyesteretts dom

Høyesterett avsa den 14. desember 2021 (HR-2021-2479-A) dom i sak mellom Komplett Bank ASA, Ikano Bank AB og BRAbank ASA («konkurrentene») mot Bank Norwegian ASA, hvor ankepartenes anke ble forkastet. Hovedorganisasjonen Virke og Google LLC var partshjelpere for henholdsvis de ankende parter og ankemotparten.

Høyesterett innledet sin vurdering ved å vise til Bank Norwegians søkemotorannonsering, hvor det var uomtvistet at man hadde brukt konkurrentenes kjennetegn som betalte søkeord. Dette medførte blant annet at konkurrentene selv ser seg nødt til å by på egne kjennetegn for å komme med på listen av betalte søketreff, og at prisen per klikk for de aktuelle søkeordene kunne øke.

I vurderingen av de rettslige utgangspunkter viser Høyesterett til EU-domstolspraksis vedrørende bruk av kjennetegn som betalte søkeord i Google Ads. Konkret vises det til dom 23. mars 2010 i de forente sakene C-236/08 til C-238/08 *Google France*, dom 25. mars 2010 i sak C-278/08 *BergSprechte*, dom 8. juli 2010 i sak C-558/08 *Portakabin* samt dom 22. september 2011 i sak C-323/09 *Interflora*. Fellesnevneren for disse avgjørelsene er at de er varemerkerettslige vurderinger. Konkurrentene anførte ikke brudd på varemerkelovgivningen. Likevel var Høyesterett av den klare oppfatningen at disse avgjørelsene likevel var relevante, da «*markedsføringslovens generalklausul ikke kan anvendes på bruk av varemerker og kjennetegn uten at man ser hen til rekkevidden av det varemerkerettslige vernet*».

I Google France-dommen ble det slått fast at bruk av kjennetegn som søkeord i Google Ads utgjør varemerkerettslig bruk, og faller dermed innenfor anvendelsesområdet for varemerkedirektivet artikkel 5. Det foreligger imidlertid ikke ulovlig inngrep såfremt bruken gjør inngrep i varemerkets funksjoner. For varemerkets funksjoner viser Høyesterett konkret til det førende EU-domstolsprejudikatet vedrørende søkemotorannonsering, den såkalte *Interflora*-dommen. Det er særlig tre funksjoner som skal vurderes, opprinnelsesgarantifunksjonen, reklamefunksjonen og investeringsfunksjonen.

For opprinnelsesgarantifunksjonen uttaler Høyesterett at krenkelse

kun vil foreligge dersom «*tredjemands annonce antyder tilstedeværelsen af en økonomisk forbindelse mellem denne tredjemand og varemærkeindehaveren*» eller om annonsen «*er så uklar i relation til varernes eller tjenesteydelsernes oprindelse, at en internetbruger, der er almindeligt oplyst og rimeligt opmærksom, ikke på grundlag af det salgsfremmende link og den dertil knyttede kommercielle meddelelse kan vide, om annoncøren er en tredjemand i forhold til varemærkeindehaveren, eller om han tværtimod er økonomisk forbundet med denne.*» Høyesterett utleder på bakgrunn av dette at spørsmålet om «*kjennetegnets opprinnelsesgarantifunksjon krenkes, beror på den nærmere utformingen av annonsen og om denne innebærer en risiko for forveksling*».

For reklamefunksjonen viser Høyesterett igjen til Interfloradommen og øvrig tidligere EU-domstolspraksis, hvor det er fastslått at «*brugen af et tegn, der er identisk med en andens varemærke, i forbindelse med en søge- og annonceringsydelse som 'AdWords' ikke krænker denne funktion ved varemærke.*» Dette gjelder uavhengig av om kjennetegnsinnehaveren i enkelte tilfeller må betale en høyere pris per klikk enn konkurrensen, dersom man ønsker at egen annonse skal fremstå øverst i søkeresultatet.

Investeringsfunksjonen er den funksjonen kjennetegnet har opparbeidet gjennom bruk og som bidrar til å tiltrekke og sikre kundelojalitet. I følge Interflora-dommen vil denne funksjonen kunne bli krenket dersom bruken av kjennetegnet «*foreligge dersom andres bruk af kjennetegnet «mærkbart generer» innehaverens «brug af sit varemærke med henblik på at opnå eller opretholde et omdømme, der kan tiltrække forbrugerne og sikre deres loyalitet*»» For allerede opparbeidet goodwill vil krenkelse foreligge «*når tredjemands brug af et tegn, der er identisk med varemærket, for varer eller tjenesteydelser af samme art, påvirker dette omdømme og dermed bringer opretholdelsen af det i fare.*»

En forskjell mellom Bank Norwegian-saken og *Interflora* er at sistnevnte omhandlet bruken av et velkjent merke. I Bank Norwegian-saken var det ikke anført at konkurrentenes kjennetegn var innarbeidet som velkjente merker. EU-domstolens konkrete vurderinger relatert til vurderingene av det velkjente merket Interflora er likevel interessant ettersom det foranlediger en nærmere vurdering av «*snylting*» eller «*urettmessig oppnådd fortjeneste på grunnlag av varemerkets særpreg eller rennomé*». Dette er nemlig et relevant vurderingsmoment i forhold til vurderingen av om det foreligger brudd på generalklausulen i markedsføringsloven § 25. I Interflora var det etablert at et større antall internettbrukere ville bruke Interflora som søkeord for å «*finne opplysninger eller tilbud vedrørende varemerkets varer eller tjenester*», likevel vil konkurrenters bruk av Interflora som søkeord ikke medføre krenkelse såfremt annonsen «*foreslår et alternativ til varemærkeindehaverens varer eller tjenesteydelser, uden at tilbyde en simpel efterligning af varemærkeindehaverens varer eller tjenesteydelser, uden at forårsage en udvanding eller en tilsmudsning og uden i øvrigt at krænke varemærkets funktioner*». Slik bruk utgjør dermed i prinsippet «*en sund og loyal konkurrence inden for sektoren for de omhandlede varer eller tjenesteydelser*» og medfører en rimelig grunn, jf. varemerkedirektivets artikkel 5(2).

På basis av EU-domstolspraksisen konkluderer Høyesterett i premiss 66 med at «*EU-domstolens avgrensning av det varemerkerettslige vernet mot konkurrenters bruk av kjennetegn som betalte søkeord, er konsekvent og gjør det etter mitt syn klart hvorfor Bank Norwegians gjeldende annonsepraksis ikke innebærer varemerkeinngrep.*» Dette betyr imidlertid ikke at Bank Norwegians bruk ikke skulle kunne ansees som rettsstridig etter øvrige bestemmelser, inkludert markedsføringsloven § 25.

I sin vurdering av markedsføringsloven § 25 innleder Høyesterett med å klarlegge aktuell harmonisering av EU-rett. Nærmere bestemt er handelspraksis på forbrukerområdet og markedsføringsloven § 26 om villedende og sammenlignende totalharmonisert. Markedsføringsloven § 25 er imidlertid ikke harmonisert i EU-retten. Bestemmelsen er dessuten en rettslig standard, hvis innhold må «*fastlegges ut fra normer utenfor bestemmelsen selv – i første rekke næringslivets egen oppfatning av forretningsskikken*». Domstolene er imidlertid ikke bundet av hva som anses akseptabelt i bransjen. I rimelighetsvurderingen er «*både subjektive og objektive momenter*» relevante. Også forbrukerhensyn er relevante, jf. Rt-1994-1584 (Lego). Dessuten rammet ikke generalklausulen «*enhver kritikkverdig adferd. Det må oppstilles en terskel ut fra de konkrete omstendighetene i saken, jf. Rt-1995-1908 Mozell på side 1918.*»

Høyesterett legger i premiss 75 klart til grunn at «*varemerkeretten ikke er uttømmende, og at markedsføringsloven § 25 derfor i prinsippet kan ramme handlinger som er lovlige etter varemerkeretten.*» Markedsføringsloven § 25 kan supplere både varemerkeretten og de øvrige reglene i markedsføringsloven kapittel 6. Anvendelsen av generalklausulen opp mot aktuell spesialbestemmelse må vurderes konkret i den enkelte sak. Det er særlig aktuelt

«… der det foreligger elementer i saken som ellers ikke fanges opp, typisk forhold av en annen karakter enn de som reguleres av spesialbestemmelsen. Videre må hensynet til sunn konkurranse tale for at det innrømmes et supplerende vern. Ansees spesialbestemmelsen å regulere det aktuelle forholdet uttømmende, må dette være avgjørende.»

Det skal utvises noe forsiktighet ved anvendelse av supplerende vern etter generalbestemmelsen, da den «*avveining av kryssende hensyn som den enkelte spesialbestemmelsen gir uttrykk for, særlig der denne regulerer forhold av lignende karakter.*»

Konkurrentene anførte at markedsføringsloven § 25 gir anvisning på en bredere vurdering, og at Bank Norwegians aktuelle bruk ikke lig-

ger i kjernen av varemerkeretten, men snarere enn illojalitet som *ikke* fanges opp av den varemerkerettslige vurderingen. Med andre ord, så ønsket konkurrentene at de subjektive elementene som preskriberes av generalklausulen skulle tillegges ytterligere vekt, kontra de objektive vurderingsmomentene som følger av varemerkeretten. Høyesteretts oppfatning er at den angivelige ulovlige bruken nettopp knytter seg til bruken av konkurrentenes kjennetegn, og at påstandsgrunnlaget sånn sett saklig sett faller inn under varemerkerettens regulering. Selv om EU-domstolspraksisen kun omhandler varemerkeretten, så vil de vurderte hensyn og interesser «*ikke gi grunnlag for en supplerende anvende av markedsføringsloven*».

Når det gjelder konkurrentenes snyltingsargument, så viser Høyesterett til at dette momentet allerede er vurdert og avveid i *Interflora*. Høyesterett «*kan ikke se at det foreligger noe grunnlag for å overprøve eller sette til side den interesseavveiningen EU-domstolen her har gjort, heller ikke i markedsføringsrettslig sammenheng.*» At kjennetegnsbruken er skjult for søkere på Google endrer ikke dette. «*Den annonseringspraksisen som EU-domstolen har vurdert, gjelder tilsvarende bruk, og dette elementet er derfor fanget opp av den varemerkerettslige vurderingen.*»

Når det gjaldt tidligere uttalelser fra Næringslivets konkurranseutvalg (NKU), hvor det gjennomgående var konkludert at kjøp av konkurrenters kjennetegn medfører brudd på god forretningsskikk, så viser Høyesterett til at forutsetningene for NKUs vurderinger kun omfatter en isolert vurdering av bestemmelsene i markedsføringsloven kapittel 6, og ikke tar høyde for de varemerkerettslige spørsmålene. NKU «*vurderer dermed heller ikke om forutsetningene for å innrømme et supplerende vern for kjennetegn etter markedsføringsloven er oppfylt*». Dette er et logisk utfall av at NKU ikke har kompetanse til å vurdere rettsspørsmål utover markedsføringsloven. Dokumentert bransjepraksis tilsier at mange ikke bruker den aktuelle annonsepraksisen. Det kan likevel ikke bli avgjørende ettersom det ikke er gitt at praksisen bygger på rettslige, og ikke kommersielle avveininger hos den enkelte annonsør.

Konkurrentene argumenterte videre for at EU-domstolens konklusjon om at annonsepraksisen ikke utgjorde en sunn og lojal konkurranse, slik det ble lagt til grunn i Interflora-dommen. Hertil la konkurrentene vekt på at en slik konkurransepraksis vil bidra til å styrke større aktører på bekostning av små, og at det vil negativt kunne påvirke innovasjon og kvalitetsutvikling. Økte markedsføringskostnader vil også kunne medføre økte kostnader for forbrukerne. Til dette uttaler Høyesterett at, til tross for at man ikke er bundet av EU-domstolens syn, så utgjør ikke konkurrentenes argumentasjon tilstrekkelig grunnlag for å fravike vurderingen. Dette fordi at det allerede etter EU-domstolspraksis ligger vesentlige begrensninger i annonsepraksisen. Videre er EU-domstolens konklusjon fastsatt på basis av en avveining mellom

«varemerkeeiers behov ro beskyttelse blant annet av den innsats og de investeringer som er nedlagt, og på den andre siden hensynet til en mest mulig fri konkurranse. Jeg kan da vanskelig se at en avveining av de samme hensyn i medhold av markedsføringsloven § 25 kan falle annerledes ut.»

Avslutningsvis viser Høyesterett til konkurrentens anførsel om at Bank Norwegians har opptrådt illojalt. Til dette konkluderer Høyesterett kort at man «*vanskelig kan se at handlinger som i varemerkerettslig sammenheng anses som uttrykk for sunn og lojal konkurranse, samtidig kan bedømmes som illojale og derved forbys som stridende mot god forretningsskikk*».

Kommentarer

Høyesteretts dom innebærer en viktig avklaring av hva som er gjeldende rett ved søkemotorannonsering. Selve «kjøpet» av konkurrentens kjennetegn for å vise egne annonser vil ikke rammes av markedsføringsloven, her er det varemerkerettslige vernet uttømmende og beskytter ikke kjennetegnsinnehaver. Dommen bidrar også til å belyse markedsføringslovens § 25 begrensede rekkevidde ved forhold som i det vesentligste reguleres av spesiallovgivning, herunder varemerkeloven § 4.

Det bemerkes at Høyesterettsdommen ikke medfører at enhver bruk er tillatt. Bruk som skaper inntrykk av at det foreligger en økonomisk forbindelse mellom annonsøren og varemerke- eller kjennetegnsinnehaveren vil fremdeles kunne rammes. Dette vil måtte baseres på en konkret vurdering av annonsens innhold. I en slik konkret vurdering kan det være rom for både varemerkerettslig og markedsføringsrettslig vern. Utformingen av annonsens innhold vil derfor kunne lede til krenkelse, men ikke selve metodikken for å få annonsen vist. Særlig annonser som inkorporerer konkurrentens kjennetegn i selve annonseteksten vil kunne medføre brudd. Bruk av konkurrenters kjennetegn som metode for å få vist egne annonser er imidlertid noe konkurrenter må tåle.

Jan Magne Langseth er partner og advokat i advokatfirmaet Simonsen Vogt Wiig.

Nicholas Foss Barbantonis er advokat i advokatfirmaet Simonsen Vogt Wiig.

Hjemmekontor og personvern

Av Ove A. Vanebo

1. Innledning

Covid-19-nedstengingen skapte enorm vekst i bruk av hjemmekontor. I tillegg til de mer praktiske problemene, har også spørsmål om personvern dukket opp. Hvilke rammer gjelder for bruk av hjemmekontor? Hva kan vi sende av informasjon ut til hjemmekontorene? Hvordan skal informasjon sikres mot ulike trusler? En sikkerhetsekspert spissformulerte den plutselig oppståtte situasjonen slik:[1]

«*Questions that a business may not have considered suddenly become of the utmost importance. What does the workplace look like when working from home? Is there a physical office available, or a cupboard or closet that can be locked in order to guarantee privacy of data and devices? Are there children in the household, and if so, is the device or devices the employee uses for work used for other purposes? It's all too tempting to allow the family to use a work laptop, or to use it for casual private browsing. Conversely, security risks can also be introduced in the opposite way – if private devices that might not be equipped with security tools are used for work purposes.*»

Personopplysingsloven gjør EUs personvernforordning (GDPR) til norsk rett, og regulerer som kjent behandling av personopplysninger. Verken loven eller GDPR har naturligvis noe eget «hjemmekontor-kapittel», og virksomheter må dermed forholde seg til de generelle reglene for personopplysningsbruk.

I utgangspunktet er det ingenting i veien for å benytte hjemmekontor, men det krever en kartlegging av risiko og bruk av egnede tiltak for å håndtere de særegne problemene

Ove A. Vanebo

som melder seg når en skal jobbe utenfor kontoret. Det islandske datatilsynet, Persónuvernd, har oppsummert situasjonen her:[2]

«*Beslutningen om å sette ansatte til å jobbe hjemmefra er ikke i seg selv et personvernproblem. Beslutningen om hvorvidt det er riktig å gi ansatte muligheten til fjernarbeid, dvs. med tilgang til systemer som inneholder personopplysninger utenfor arbeidsplassens intranett, må generelt være basert på en risikovurdering, som tar hensyn til arten av informasjonen som ansatte jobber med. Jo mer sensitiv eller omfattende informasjonen er, desto strengere krav må stilles for å ivareta sikkerheten til interne nettverk i tilknytning til de aktuelle aktivitetene.*»

Det er altså særlig informasjonssikkerheten som er kritisk å ivareta. I punkt 2 vil jeg derfor redegjøre for de særlige forholdene som bør tas i betraktning ved bruk av hjemmekontor.

I og med at det er de generelle reglene for informasjonssikkerhet kravene springer ut fra, må vurderingen være om arbeidsgiver har gjennomført «egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen».[3] I punkt 3 kommer jeg inn på aktuelle tiltak.

2. Kartlegging og risikovurdering

2.1 Innledning

Risikovurdering innebærer kartlegging og vurdering av trusler mot virksomheten, samt vurdering av konsekvensene truslene kan få.[4] Selv om de ansatte i varierende grad bruker hjemmekontor, må det tas hensyn til at de fleste vil bruke det i noe omfang. I lys av GDPR er det viktig å huske at forordningen dreier seg om å håndtere trusler mot personers rettigheter og friheter, slik at man ikke foretar kun en risikovurdering som fokuserer på infrastruktur eller bedriftens «upersonlige» informasjonsverdier (som er mer vanlig i tradisjonell IT-sikkerhet).

Enkelte teoretikere har argumentert for at det bør gjennomføres en mer omfattende vurdering av personvernkonsekvenser, i samsvar med GDPR artikkel 35.[5] Dette kan være fornuftig, særlig hvis det er tale om høyrisikoaktivitet med sensitivt materiale, men vanligvis vil det være tilstrekkelig med en mer alminnelig risikovurdering.

2.2 Generelt om risikobildet

Normalt skal virksomheter ha utført mer generelle risikovurderinger, og det er derfor klokt å fokusere på særskilte risikoer ved hjemmekon-

1 Marc Lueck, *GDPR in the new remote-working normal*. I: Computer Fraud & Security, 2020 nr. 8, s. 15.

2 Persónuvernd, *COVID-19 og persónuvernd*, 2020. Lest 16. november 2021: *https://www.personuvernd.is/personuvernd/frettir/covid-19-og-personuvernd#*

3 GDPR art. 32 nr. 1.

4 Bruvoll, J. A., Brattekås, K. & Nystuen, K. O. (2020). *Kapittel 9 Funksjonsbasert risikovurdering*. I H. Bergsjø, R. Windvik & L. Øverlier (Red.), *Digital sikkerhet. En innføring*, s. 187.

5 Lueck, 2020, s. 15.

tor. Nasjonal Sikkerhetsmyndighet melder om «nye sårbarheter som følge av hjemmekontor og endrede arbeidsmønstre, økt risiko for uønskede strategiske investeringer og omfattende global påvirkning og desinformasjon».[6] Kritiske samfunnsfunksjoner og helsesektoren er særlig utsatt. Antallet trusselaktører øker, ved at også politisk og statlig motiverte aktører har interesse av kunnskap og sabotasje.

For hjemmekontorvurderingen er det naturlig å se særlig på:

- Virksomhetens og de ansattes lokalisering på hjemmekontor
- Kriminalitetsbilde i områdene
- Antallet ansatte med hjemmekontor
- Vekst og utvikling, med stadig flere ansatte de siste årene, som kan medføre at organisasjonen ikke har rukket å få på plass en helhetlig praktisering og sikkerhetskultur
- Hva slags utstyr de ansatte bruker og om det kan medføre særlig risiko

2.3 Verdivurdering

Verdier betegner vanligvis det som er «en del av og til nytte for virksomheten».[7] Her er det særlig personopplysninger som skal vurderes for å unngå at tap får kritiske konsekvenser for de registrertes rettigheter. Som Datatilsynet påpeker om denne vurderingen:[8]

«*Verdier identifiseres ved å anslå taps- eller skadepotensial – i form av kostnad for gjenanskaffelse, indirekte kostnader som tap av 'goodwill', osv. I personvernsammenheng vil verdiene kunne representeres ved å anslå tap/skadepotensial for enkeltmenneskers liv, helse, økonomisk tap, tap av anseelse eller integritet. Kartlegging av verdier resulterer i oversikt hvor antatt sikkerhetsbehov knyttes til den enkelte verdi.*»

Både datasystemer (sentralt i virksomheten og hjemme hos de enkelte ansatte) og informasjon er svært viktig å ivareta. Informasjon på avveie eller datasystemer som ikke fungerer optimalt kan føre til salgsnedgang, søksmål fra kunder, produksjons- og kundetap og tap av forretningshemmeligheter – i tillegg til de rene personvernproblemene. Det tilsier høye krav til informasjonssikkerhet.

2.4 Akseptkriterier

Risikonivået ledelsen kan akseptere, betegnes som «akseptkriterier». Risikobildet og verdiene tilsier ofte en streng tilnærming til informasjonssikkerhet og lav risikoappetitt. Dette vurderes opp mot prinsippene for informasjonssikkerhet, som beskrives under:[9]

- Konfidensialitet (informasjon skal ikke tilflyte uvedkommende på uautorisert vis)
- Integritet (informasjon skal være nøyaktig og skal ikke kunne endres uten tillatelse)
- Tilgjengelighet (tjenester skal være stabile slik at informasjon er tilgjengelig ved behov)

I forbindelse med beslutningen om akseptkriterier, er det vanlig å konkretisere disse. Eksempelvis kan et kriterium være at det aksepteres manglende tilgjengelighet i maksimalt to timer.

2.5 Den konkrete risikovurderingen

Risiko uttrykker vanligvis trusler som en kombinasjon av sannsynlighet og konsekvens. En vanlig risikovurderingsmodell er å vurdere hendelser opp mot hvilke sikkerhetsprinsipper som utfordres (og som forkortes ved bruk av forbokstav), dvs. konfidensialitet (K), integritet (I) og tilgjengelighet (T). Sannsynlighet og konsekvens kan f.eks. kvantifiseres fra 1 til 5, der 1 er liten/lav og 5 er stor/alvorlig, som i matrisen under synliggjør om

Hendelse	Sikkerhets-prinsippp	Konsekvens	Sannsynlighet	Risiko	Vurdering
1. Informasjon lekker fra video--konferanse, f.eks. ved at nabo eller personer i hjem fanger opp informasjon.	K	Informasjon om patenter, strategier og kunderelasjoner kan tilfalle uvedkommende. Tillitstap samt økonomisk tap. Informasjon om privatpersoner kan komme på avveie. Score: 4.	De fleste har trygge, lydsikre rom. Sjelden fiendtlige aktører får informasjon. Score: 2.	Middels	Akseptabel

6 Nasjonal Sikkerhetsmyndighet. (2021). *Risiko 2021 - helhetlig sikring mot sammensatte trusler*. Lest 16. november 2021: https://nsm.no/getfile.php/136165-1612871437/Demo/Dokumenter/Rapporter/Risiko%202021%20hand-out.pdf

7 Bergsjø, H. & Windvik, R. (2018). *Datasikkerhet for ledere - hvordan beskytte din virksomhet*, s. 55.

8 Datatilsynet, *Risikovurdering av informasjonssystem*, s. 9.

9 Bergsjø & Windvik, 2018, s. 25-26.

risiko er akseptabel.[10] Dette kan litt forenklet se slik ut:

For å gjøre den oppsummerende fremstillingen pedagogisk, kan det være fornuftig å sette den opp som en risikomatrise, som kan sette hendelsesnumre inn et «trafikklyssystem». Grønt kan visualisere akseptabelt nivå, mens gult nivå er akseptabelt – men bør møtes med tiltak. Rødt viser en uakseptabel risiko, som skal avbøtes med tiltak. Dette kan visualiseres på denne måten:[11]

2.6 Oppfølging av risikovurderingen

I kjølvannet av risikovurderingen er det naturlig å følge opp med ulike tiltak, og jeg vil under i punkt 3 nevne noen konkrete tiltak som er aktuelle – og som er foreslått av ulike offentlige organer og europeiske tilsyn. Hvilke tiltak som til syvende og sist bør benyttes, må bero på trusselbildet.

Ofte må tiltakene fremlegges for ledergrupper eller bestemte beslutningstakere. Ut fra rent praktiske hensyn bør tiltakene også «kvantifiseres», ved at det tydeliggjøres hva det vil koste å få på plass tilstrekkelige tiltak.

3. Aktuelle tiltak for informasjonssikkerhet tilknyttet hjemmekontor

3.1 Bruk av intranett og skytjenester mv. gjennom fjerntilgang

Danmarks datatilsyn nevner disse tiltakene:[12]

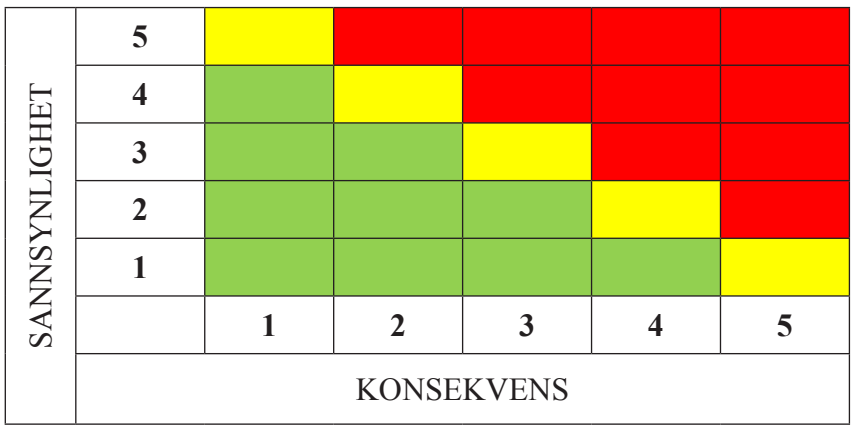
- Virksomheten må sørge for å etablere og informere de ansatte om klare retningslinjer for hjemmearbeid – og sørge for at ansatte følger dem.
- Bruk den klart sikre tilgangen til interne systemer (VPN eller andre sikre tjenester/former for direktetilkobling).
- Så langt det er mulig, bør det vanlige (sentrale) saksbehandlingssystemet benyttes. Videre anbefales at dette systemet bør ha både tilgangskontroll, løsning som muliggjør utforming og synliggjøring av ulike dokumentversjoner, back-up og øvrige generelle sikkerhetstiltak.

Det islandske datatilsynet har understreket at en ansatt som jobber eksternt, må sørge for at han eller hun bare jobber på intranettet i forbindelse med den aktuelle aktiviteten. I tillegg bør vedkommende sørge for å følge alle organisatoriske tiltak knyttet til den enkelte tjenesten.[13]

3.2 Oppbevaring og bruk av bærbart utstyr mv.

Det er fort gjort at ulike former for utstyr kommer på avveie, og at USB-brikker eller nettbrettet legges igjen på kafé. I tillegg kan det også skje at naboer eller familiemedlemmer får innsyn på utstyr – noe som potensielt sett kan være i strid med taushetsplikt. Bruk av bærbart utstyr utenfor etablerte, sikre kontornettverk kan også i større grad blir utsatt for ulike forsøk på urettmessig uthenting av informasjon. Jeg vil også komme noe inn på det sistnevnte i punkt 3.4. Hva gjelder behandling/oppbevaring av ulike former for bærbart utstyr, nevner det irske datatilsynet følgende:[14]

- Pass ekstra på at enheter (for eksempel USB-er, telefoner, bærbare datamaskiner eller nettbrett) ikke mistes eller blir lagt på et sted de kan bli borttatt.
- Sørg for at alle enheter har de nødvendige oppdateringene, for eksempel operativsystemoppdateringer (som iOS eller Android) og programvare-/antivirusoppdateringer.
- Lås enheten hvis du av en eller annen grunn må la utstyret stå uten tilsyn.
- Sørg for at enhetene dine er slått av, låst eller lagret på betryggende vis når de ikke er i bruk.
- Sørg for at datamaskinen, bærbar PC eller annen enhet brukes på et trygt sted, for eksempel der du kan holde øye med den og begrense hvem andre som kan se skjermen. Dette er særlig viktig hvis du arbeider med særlige kategorier av (eller andre typer sensitive) personopplysninger.
- Bruk effektive tilgangskontroller (som multifaktorautentisering og sterke passord) og (hvis det er tilgjengelig) kryptering for å begrense tilgangen til enheten. Dette vil også redusere risikoen hvis en enhet blir stjålet eller forlagt.



10 Gjort i bl.a. Bergsjø & Windvik, 2018, s. 79.

11 Inspirert av Bergsjø & Windvik, 2018, s. 76.

12 Datatilsynet, *Gode råd om hjemmearbejde*, 16. mars 2020. Lest 25. oktober 2021: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/gode-raad-om-hjemmearbejde*

13 Persónuvernd, COVID-19 og persónuvernd; Öryggi persónuupplýsinga í fjarvinnu. Lest 25. oktober 2021.

14 Data Protection Commision, *Protecting Personal Data When Working Remotely*, 2020.

Hvis en enhet mistes eller blir stjålet, bør du umiddelbart prøve å fjernslette harddisken.

3.3 E-post og intern kommunikasjon

Det islandske datatilsynet har anbefalt følgende tiltak for tilstrekkelig sikker e-post-kommunikasjon:[15]

- Følg arbeidsgivers retningslinjer for arbeidsplassen når du bruker e-post.
- Bruk jobb-e-post (og ikke privat e-post) for jobbkommunikasjon når du sender personopplysninger.
  - Hvis du må bruke privat e-post for å sende viktig informasjon, bør du kryptere dokumenter (som inneholder personopplysninger) med et sterkt passord.
- Sørg for at du sender til riktig mottaker og at riktig fil er vedlagt. Det kan være nødvendig å åpne vedlegget i eposten for å være sikker på at riktig vedlegg følger med.
- Unngå å kommunisere på sosiale medier med kolleger om sensitive saker. Her må du følge prosedyrene på arbeidsplassen i alle sammenhenger.

3.4 Lokal lagring

Generelt anbefales det å lagre informasjon i sentrale systemer. Hvis det er et behov for å lagre dokumenter eller andre filer lokalt, på selve datamaskinen, har det danske Datatilsynet følgende anbefalinger:[16]

- Enheten eller filen med dokumentet bør være kryptert.
- Ingen andre (heller ikke egne barn) bør ha tilgang til enheten.
- Arbeidstaker må ha kontroll over gjeldende versjon av filen, slik at data ikke går tapt eller er ukorrekte.
- Filen skal lastes opp til saksbehandlingssystemet eller andre sentrale løsninger så snart som mulig
  - Den lokale kopien bør deretter slettes umiddelbart.

3.5 Bruk av videokonferanseverktøy

Formidling av bildemateriale og lyd vil naturligvis kunne innebære behandling av personopplysninger. For mange kom det likevel som en overraskelse at også videokonferanseverktøy (f.eks. Zoom, Teams og Skype) må oppfylle grunnleggende krav til informasjonssikkerhet. Undersøkelser viser også at konferanseverktøyene har hatt klare svakheter.[17]

Noen praktiske råd fra det irske datatilsynet er:[18]

- Sørg for at konferanseverktøyet har de nødvendige programvare-/antivirusoppdateringer.
- Les gjennom tjenestens personvern- eller informasjonssikkerhetspolicy for å vite hvem personopplysninger blir delt med, hvor de vil bli lagret og hvilke formål de vil bli brukt til.
- Tenk gjennom hvilke tillatelser du gir og hvilke personopplysninger som behandles. Trenger du f.eks. å dele lokasjonen/posisjonen din eller listen over kontakter?
- Pass på hva som kan sees under videokonferansen, f.eks. hva som kan observeres via kameraet ditt. Sørg for å logge ut, dempe lyd eller slå av videooverføring ved behov, bl.a. når du tar en pause.

3.6 Papirdokumenter

Potensielt sett kan også bruk av papirdokumenter med personopplysninger være underlagt personopplysningslovens regulering. Dette er typisk dersom de inngår i et register, og dermed er omfattet av personopplysningsloven, se personopplysningsloven § 2 første ledd og GDPR art. 2 nr. 1.

Det kan også tenkes at papirdokumenter utgjør en informasjonsbærer mellom to systemer, og at behandlingen derfor er «delvis automatisert» – og dermed er omfattet av GDPR.[19] Det er også tenkelig at dokumenter på avveie kan utgjøre et brudd på personopplysningssikkerheten.[20]

Det irske Datatilsynet har nevnt disse punktene vedrørende behandling av papirdokumenter:[21]

- Hvis man arbeider utenfor kontoret med papirbasert informasjonsbehandlingen, må arbeidstaker ivareta sikkerheten og konfidensialiteten til dokumentene, bl.a. ved å oppbevare dem låst i arkivskap eller skuff når de ikke er i bruk. Dokumentene bør også kasseres på en sikker måte (f.eks. makulering) når de ikke lenger er nødvendige, og sørge for at de ikke blir liggende et sted hvor de kan bli forlagt eller stjålet.
- Hvis du har å gjøre med dokumenter som inneholder spesielle kategorier av personopplysninger (f.eks. helsedata), bør du være ekstra forsiktig for å ivareta sikkerhet og konfidensialitet. Slike dokumenter bør bare tas ut fra et sikkert sted når det er strengt nødvendig å utføre arbeidet.
- Der det er mulig (og hensiktsmessig) bør arbeidstaker føre en skriftlig oversikt over hvilke dokumenter og filer som er tatt med hjem, for å opprettholde

15 Persónuvernd, *COVID-19 og persónuvernd*, 2020.

16 Datatilsynet, *Gode råd om hjemmearbejde*, 16. mars 2020. Lest 25. oktober 2021: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/gode-raad-om-hjemmearbejde*

17 Se f.eks. Bill Marczak og John Scott-Railton, Move Fast and Roll Your Own Crypto; A Quick Look at the Confidentiality of Zoom Meetings, 2020. Lest 21. februar 2022: *https://tspace.library.utoronto.ca/bitstream/1807/104313/1/Report%23126--zoom.pdf*

18 Data Protection Commission, *Data Protection Tips for Video-conferencing*, 2020. Lest 21. februar 2022: *https://www.dataprotection.ie/en/dpc-guidance/blogs/data-protection-tips-video-conferencing*

19 GDPR art. 2 nr. 1.

20 GDPR art. 33 nr. 1, jf. art. 4 nr. 12.

21 Data Protection Commision, *Protecting Personal Data When Working Remotely*, 2020.

konfidensialitet og kontroll/styring.

3.7 Arbeid med å forbedre digital sikkerhetskultur

Digital sikkerhetskultur betegner verdier, holdninger, antakelser, normer og kunnskaper som ansatte har når de forholder seg til digitale verdier.[22] Poenget er å påvirke handlingsmønstre og grunnleggende antakelser om hvordan man skal forhold seg til nevnte verdier. Dette kan være et organisatorisk tiltak i henhold til GDPR.

Videreutviklingen av en digital sikkerhetskultur kan beskrives slik:[23]

- **Hva?** – Virksomheten må få kunnskap om hva som skal gjøres. Dette forutsetter at det er oversikt over hva den ansatte kan, og hva som eventuelt mangler.
- **Hvorfor?** – Bevisstgjøring for å forstå informasjonssikkerhet og hvordan man skal handle. Dette knyttes opp mot den senere prosessen med å få ansatte til å tenke over ulike situasjoner og gis et opplæringstilbud.
- **Hvordan?** – Ansatte må få kunnskap om hva som praktisk skal gjøres for å oppnå tilfredsstillende målsettinger. Planen skal derfor også omfatte styrking av de ansattes digitale kompetanse. Hva som konkret må gjøres vil bli synliggjort gjennom oversikt over ansattkompetanse og bevisstgjøringsprosessen.

Til sammen skal disse aspektene bidra til å «bygge» holdninger, slik at bevissthet og forståelse av risikobildet følges opp med handling.

Et eksempel på tiltak er nettundervisning om hvordan hjemmekontorer kan brukes effektivt og trygt. Det bør også legges opp til mottak av spørsmål fra ansatte om hvordan de opplever situasjonen og hva de kan dele av nyttige tips. Noen eksempler på tiltak er:

- Grunnleggende kurs om informasjonssikkerhet
- Kurs om mulige trusler ved bruk av hjemmekontor, herunder oppfølging av avvik
- Kurs om hvordan informasjon skal innhentes, lagres og formidles til andre. I dette kurset bør arbeidsgiver også informere om ulike hjelpemidler for å oppnå tilstrekkelig informasjonssikkerhet, som VPN-løsninger og kryptering ved oversending av eposter.

Hvis de ansatte har noe varierende dager og mye tidspress, kan kursene også legges ut på intranettet i videoopptak. Det bør legges inn mekanismer som registrerer når en ansatt har deltatt eller sett alle videoene, og oppfølging for å sikre at alle får med seg informasjon og rutiner.

Arbeid med og endring av digital sikkerhetskultur er et ledelsesansvar. Både ledelsen og resten av organisasjonen må være samordnet underveis i prosessen. Innretning av planen bør også ta hensyn til at ledelsen må ha legitimitet blant ansatte når de pålegges hjemmekontor og nye rutiner.

3.8 Avvikshåndtering

Ulike former for avvik kan naturligvis oppstå. Det kan være hensiktsmessig å få på plass ulike former for monitorering for å fange opp abnormiteter.[24] I tillegg bør naturligvis ansatte gjøres oppmerksom på at de må varsle avvik. Arbeidsgiver vil i henhold til GDPR artiklene 33 og 34 har en plikt til å underrette henholdsvis Datatilsynet og registrerte personer.

Ove A. Vanebo er assosiert partner i CMS Kluge.

22 Malmedal, B. (2020). *Kapittel 2 Sikkerhetskultur*. I H. Bergsjø, R. Windvik & L. Øverlier (Red.), *Digital sikkerhet: En innføring*, s. 36.

23 Digitaliseringsdirektoratet, *Bakgrunnsinformasjon for kompetanse- og kulturutvikling innen digital sikkerhet*. Lest 16. november 2021: *https://www.digdir.no/informasjonssikkerhet/bakgrunnsinformasjon-kompetanse-og-kulturutvikling-innen-digital-sikkerhet/2177*

24 Agencia Española de Protección de Datos, *Recommendations to protect personal data in situations of mobility and telecommuting*, 2020, s. 3.

Halvor Manshaus

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

Høyesterett gir avklaring på kjøp av annonseplass i søkeresultater

Tradisjonell markedsføring ved bruk av trykk, radio og tv-reklame har i stor grad veket plass for digitale plattformer som tilpasser budskapet og retter seg direkte mot den enkelte forbruker. Dette skjer gjennom søkemotorer, sosiale medier og digitale underholdningstjenester som samtidig trekker på store mengder data samlet om brukerens kjøpemønster og adferd. Slik markedsføring har skapt grobunn for flere komplekse juridiske problemstillinger, deriblant grensesnittet mellom ulike annonsører som alle skal markedsføre sitt innhold, tjenester og produkter i konkurranse med andre aktører på markedet.

Høyesterett avsa nylig en prinsipiell avgjørelse vedrørende adgangen til å gjøre bruk av konkurrenters navn og varemerke i forbindelse med digital markedsføring (HR-2021-2479-A). Den sentrale problemstillingen som Høyesterett tok stilling til omhandlet Bank Norwegians bruk av konkurrenters navn som betalende søkeord i Google Ads (tidligere Google AdWords). De fleste lesere vil være kjent med utformingen av Googles søkemotor, der søkeresultatet er rangert i en kvalifisert liste, i to adskilte deler. Den første listen er plassert øverst og viser annonsørinnhold i tilknytning til det valgte søkeordet, mens treffene på selve søket følger i en separat hovedliste rangert etter relevans. Hvilket annonsørinnhold som havner i den første listen avgjøres på grunnlag av et auksjonssystem utført for hvert enkelt individuelle søk i Googles søkemotor.

Dette er et system som jeg har beskrevet i en tidligere artikkel i Lov & Data (LoD-2010-102-4) «Ord om AdWords». Der ble det forklart hvordan annonsørene kan by mot hverandre på de samme søkeordene, og hvordan dette åpner for flere rettslige problemstillinger knyttet til bruk av varemerker. Google er den ledende aktøren som tilbyr denne typen tjenester, og kaller sitt annonseprodukt Google Ads (tidligere kjent som AdWords). Innenfor Ads konseptet kan altså konkurrenter by mot hverandre, og annonseplass kan kjøpes blant annet basert på eget eller konkurrenters navn og registrerte varemerker.

Ved at flere byr på samme virksomhetsnavn eller varemerker, vil dette igjen kunne bidra til et prispress på virksomhetens eget navn og varemerker hos Google Ads. Dette gjelder spesielt dersom disse er attraktive enten for å beskrive et produkt eller en tjeneste, eller ved at navnet i seg selv har gjennomslagskraft som søkeord. Prisen for annonsen betales normalt først når noen klikker på selve annonsen i resultatlisten, dette betegnes som CPC – «Cost Per Click». Ved utvelgelsen av søkeord tilbyr Google annonsøren verktøyet Keyword Planner. Prosessen starter med at annonsøren legger inn sin egen nettadresse, samt et budsjett som angir betalingsvillighet per dag. Basert på denne informasjonen genereres det forslag til søkeord fra Google verktøy. Attraktive søkeord får en høyere pris, ved at det er flere annonsører som er villige til å betale for disse. Dette vil typisk være ord som beskriver tjenester og produkter, for eksempel «forbrukerlån».

I saken for Høyesterett hadde Bank Norwegian betalt for å legge inn navn fra konkurrenter i bank-

markedet som sine søkeord. Dersom forbrukeren søkte på for eksempel «Ikano» Bank på Google, kom det en resultatliste med to treff angitt som annonser plassert øverst i resultatlisten. Den første var for Ikano Bank, den andre annonsen var for Bank Norwegian. Ved at flere aktører byr på samme søkeord, driver dette prisen opp. Eieren av et varemerke vil da kunne se prisen for å tilby annonser basert på eget varemerke gå opp, ettersom konkurrentene byr på samme merke.

Hvem som kommer øverst på den første annonselisten vil kunne variere fra dag til dag. En aktør som har levert inn et bud på et søkeord hos Google har ikke dermed kjøpt retten til annonseplassering på den første listen. I stedet holdes det en auksjon hver eneste gang noen utfører et søk hos Google. Det er selve søket som utløser en komplisert algoritme som igjen styrer budprosessen og annonsens plassering i resultatlisten. Dette innebærer at innen du har lest denne setningen så er det allerede avholdt tusenvis av slike automatiserte auksjoner basert på søk som utføres rundt om i verden.

Algoritmen ser hen til blant annet prisen annonsøren er villig til å betale for at brukeren klikker på annonsen, samt relevansen av annonsørens egen nettside opp mot det aktuelle søket. En annonsør som tilbyr høy relevans inn mot søket, vil i praksis kunne betale mindre enn andre annonsører med lavere kvalitet. I eksempelet med Ikano Bank ovenfor, vil Ikano Bank kanskje betale mindre enn Bank Norwegian for øverste plassering, ettersom Ikano Bank sin nettside kan forventes å inneholde mer informasjon om Ikano. Dette gjør annonsen mer relevant, og skal i prinsippet redusere prisen. Likefult vil det forhold at Bank Norwegian tydeligvis også har betalt for å bruke søkeordet Ikano mest sannsynlig drive opp prisen for Ikano Bank. Googles algoritme justeres og tilpasses over tid, og legger vekt på også andre kriterier. Blant annet sees det hen til hvor mange som klikker på annonseresultatet, som igjen kan påvirke hvordan annonsen senere vektes i vurderingen.

Jeg har tidligere skrevet om denne saken for lavere instans, og sjekket da litt om prisene for ulike kategorier søkeord i Google Ads. Markedsføringsfirmaet Wordstream har opplyst at de to dyreste søkeordkategoriene du kan kjøpe er *insurance* og *loans*. Den gjennomsnittlige CPC (cost-per-click) for disse søkekategoriene lå da på henholdsvis $55 og $44. Enkeltord i disse kategoriene kan være enda dyrere. Dette er altså prisen annonsøren betaler bare for at forbrukeren klikker på annonsen. Det er nærliggende å anta at prisen på den generiske søkekategorien «forbrukslån» også ligger høyt i vårt lokale marked. Disse prisene er i seg selv en indikasjon på at markedet anser denne formen for markedsføring som viktig og effektiv.

Problemstillingen i denne saken var om den aktuelle bruken av konkurrentenes navn og varemerker utgjorde en handling i strid med markedsføringsloven § 25 om god forretningsskikk. Saken hadde tidligere vært behandlet for Næringslivets konkurranseutvalg (NKU), som fant at det forelå en krenkelse etter § 25 (NKU-2017-6). Avgjørelsen fra NKU var også konsistent med tidligere praksis i lignende saker om bruk av konkurrentenes navn og varemerker som søkeord, ref. sakene NKU-2006-6 (YTT) og NKU-2012-12 (Teppeabo). Avgjørelsen ble også fulgt opp av NKU i etterfølgende praksis, ref. NKU-2018-10 (Kondomeriet).

Bank Norwegian hadde lagt inn bud på slike søkeord i Google Ads som beskrevet ovenfor. På denne måten hadde Bank Norwegian lyktes i å sikre seg øverste plass i annonselisten for konkurrentene Komplett Bank, Ikano Bank og Monobank sine navn som betalt søkeord i Google Ads. Dette medførte at for hvert søk som ble foretatt ved bruk av søkeordene *«ikano bank», «komplett bank»* eller *«monobank»*, så viste resultatlisten annonser fra Bank Norwegian øverst på listen. Saksøkerne i denne saken, de tre bankene hvis navn ble brukt som betalt søkeord av Bank Norwegian, anførte at denne praksisen var i strid med kravet om «god forretningsskikk» etter markedsføringsloven § 25. Som allerede omtalt konkluderte NKU med at det forelå brudd på bestemmelsen. Saken ble deretter behandlet i Oslo tingrett og Borgarting lagmannsrett, som begge kom til motsatt resultat. Dette skyldtes at disse to instansene i større grad trakk veksler på praksis fra EU-domstolen.

Praksis fra EU-domstolen viser at det generelt føres en mer liberal linje for bruk av markedsføringstiltak som trekker på kjente varemerker, og saksøkerne anførte derfor i stedet brudd på reglene om god forretningsskikk. Som følge av dette, var en av hovedproblemstillingene for Høyesterett å analysere hvorvidt markedsføringsloven § 25 ga saksøkerne et ytterligere vern i tillegg til, og atskilt, fra reguleringene for varemerkeretten generelt. I domspremissene oppsummerte Høyesterett først utstrekningen av varemerkerettens vern i relasjon til auksjonspraksisen som Google Ads tilbyr, med særlig henblikk til praksis fra EU-domstolen. Høyesterett konkluderte under denne problemstillingen med at EUs varemerkedirektiv og praksis fra EU-domstolen ikke er til hinder for anvendelse av nasjonale regler som vil gi en ytterligere beskyttelse for næringsdrivende, i vårt tilfelle for de tre saksøkerne. Følgelig vil det altså være grunnlag for å anvende markedsføringsloven § 25 som selvstendig hjemmel i de tilfellene hvor varemerkerettens reguleringer ikke behandler særlige sider av det pretenderte brudd på bestemmelsen i § 25. Dette standpunktet er i samsvar med tidligere prejudikatsavgjø-

relser fra domstolen, slik som Rt. 1998 s. 1315 (Iskrem) og Rt. 1995 s. 1908 (Mozell).

Følgen av dette er dermed at Høyesterett må foreta en helt konkret vurdering av hvorvidt generalklausulen i markedsføringsloven § 25 kan supplere de mer spesifikke varemerkereguleringene, også i de tilfellene det ikke kan fastslås brudd på sistnevnte. I premissenes avsnitt 48 påpeker førstvoterende at den handling som potensielt er i strid med bestemmelsen, er Bank Norwegians bruk av konkurrentenes kjennetegn, altså en problemstilling som i sin kjerne faller innenfor varemerkeretten. Dette gir følgelig en begrenset adgang til å supplere med varemerkerettsliknende argumenter i relasjon til markedsføringsloven § 25. Høyesterett viser så til EU-domstolens avgjørelse i Google France-saken (forente saker C-236/08 til C-238/08) avsnitt 87:

"Selv om det således fremgår, at annoncører på internettet i givet fald kan ifalde ansvar i henhold til regler på andre retsområder, såsom regler om illoyal konkurrence, forholder det sig ikke desto mindre således, at den påståede ulovlige brug på internettet af tegn, der er identiske med eller ligner varemærker, må behandles i henhold til varemærkeretten".

I praksis innebar dette at argumenter med en side til varemerkeretten allerede hadde blitt vurdert og konsumert. Dermed var det kun en begrenset adgang til å anvende de samme eller i stor grad like argumenter i vurderingen av hvorvidt terskelen under markedsføringsloven § 25 var overskredet. Som en følge av dette, kunne dermed ikke saksøkernes argumenter om "snylting", i den forstand at Bank Norwegian gjennom sin praksis fikk markedsføre seg selv på andres vegne, føre fram under § 25. Det samme gjaldt for anførsler om at auksjonsprosessen og utvelgelse av relevante annonser var ukjent for den enkelte internettbruker, da dette ble ansett for å være et varemerkerettslig spørsmål. Endelig fant Høyesterett heller ikke grunnlag for å fravike tidligere praksis fra EU-domstolen, som har slått fast at auksjoner av denne typen stimulerer til sunn og lojal konkurranse mellom næringsdrivende.

Dette sistnevnte aspektet om sunn konkurranse utgjør et viktig punkt i Høyesteretts avgjørelse, ettersom dette knytter seg direkte opp mot vurderingen under markedsføringsloven § 25. likevel er dette temaet om lojal konkurranse i tråd med prinsipper og forventninger om *fair play* undergitt en begrenset behandling helt avslutningsvis i premiss 94-95. Et viktig punkt for anvendelsen av markedsføringsloven § 25 vil normalt være vurderingen av eventuell illojal opptreden fra en av markedets konkurrenter mot en eller flere andre aktører. Men siden Høyesterett allerede hadde konkludert med at kjøp av konkurrentenes navn som søkeord bidrar til en sunn og rettferdig konkurranse i varemerkerettslig forstand og i tråd med EU-retten, var det liten plass for å lande på motsatt konklusjon i relasjon til markedsføringsloven § 25.

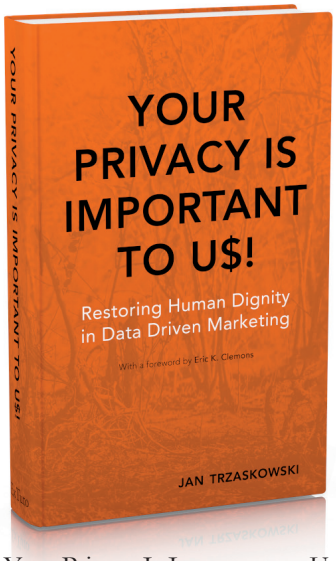
Høyesterett gir avslutningsvis en oppsummering av hvordan domstolen oppfatter gjeldende rett både i et europeisk og norsk perspektiv, og oppstiller ytterligere retningslinjer for vurderingen av hvorvidt det ved svært spesifikke rettslige reguleringer, slik som varemerkeloven § 4, vil være adgang til å supplere med generalklausuler slik som markedsføringsloven § 25. For fremtidige saker vil det måtte foretas en helt konkret vurdering av forholdene i den enkelte sak, hvor hensynet til illojalitet og avstanden fra bransjepraksis utgjør vektige argumenter. Der slike forhold allerede er vurdert opp mot spesielreglene, skal det mye til for å snu en slik vurdering til motsatt konklusjon ved anvendelsen av den videre hjemmelen i markedsføringsloven § 25.

Høyesterett konkluderte som forventet på samme resultat som tingretten og lagmannsretten. Bank Norwegians bruk av Google Ads utgjorde ikke brudd på markedsføringsloven § 25 om god forretningskikk. Når jeg skriver "som forventet", skyldes dette at EU-praksis her gir klar anvisning på en slik løsning med sine uttalelser om at kjøp av søkeord og plassering på resultatllister ligger innenfor den sunne og lojale konkurransen markedet forventet. Dette er ikke ensbetydende med at det er "fritt frem" for enhver – der det foreligger illojal bruk eller klanderverdig adferd vil resulatet kunne bli at reglene om god forretningsskikk får direkte anvendelse selv om det ikke foreligger varermerkeinngrep.

Litteratur

Your Privacy Is Important to Us! – Restoring Human Dignity in Data-Driven Marketing

Jan Trzaskowski.



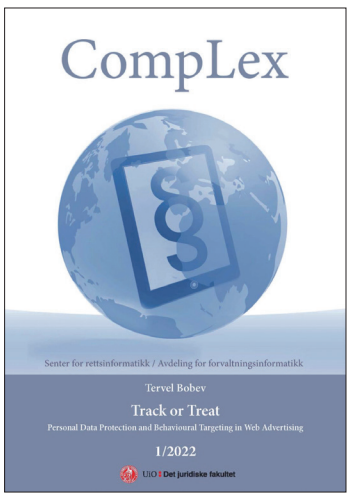
Your Privacy Is Important to Us! explores the application of EU consumer law—including data protection law and other fundamental rights—to data-driven business models that infringe on human agency, social cohesion and democratic debate. It suggests how our current legal framework can be informed by psychological, technological and societal perspectives to curb predatory business models of surveillance capitalism.

The book elucidates the potential for cross-fertilisation between data protection law and marketing law, and it demonstrates how the protection of human dignity, privacy and nondiscrimination may corroborate these legal disciplines. It is argued that 'paying with personal data' is a misleading framing when, in fact, we pay with attention and agency—which are both scarcer and more precious than personal data and are also important in social and societal contexts. A three-tiered model of information asymmetry is introduced to illustrate why information does not ensure transparency, which is a prerequisite for user empowerment.

The aim is to inform and amplify ongoing debates by providing a coherent framing of data-driven marketing in the context of law, psychology, technology and society.

Jan Trzaskowski, Ph.D., is Law Professor at Copenhagen Business School and Aalborg University. Since the mid-1990s, he has dealt with legal and regulatory aspects of information technology, and his research focuses on the protection of consumers and fundamental rights, including privacy. He was Head of the Danish delegation negotiating the 2000 E-Commerce Directive and is founder of the Business in Democracy Initiative (BiDEM).

Eric K. Clemons, Ph.D., is Professor Emeritus at The Wharton School and author of *New Patterns of Power and Profit* (2019). He has studied the impacts of large online platforms on individuals, on societies, and on civilization itself.



Tervel Bobev. »Track or Treat«

Personal Data Protection and Behavioural Targeting in Web Advertising. Oslo: Universitetet i Oslo, Juridisk fakultet 2022, 1/2022. ISSN 2703-8777 Complex (online)

https://www.jus.uio.no/ifp/forskning/om/publikasjoner/complex/2022/2022-01.html

Gorrissen Federspiel

Tue Goldschmieding

Psykisk udviklingshæmmet, som havde udleveret sine NemID-oplysninger til en ukendt person, hæftede ikke for lån

Højesteret afsagde den 17. november 2021 kendelse i sag 61/2021 mellem sagsøgte og Ekspres Bank A/S. Sagen angik, hvorvidt sagsøgte, der var psykisk udviklingshæmmet, hæftede for et lån optaget hos Ekspres Bank A/S. Lånet var blevet optaget af en ukendt person i forbindelse med sagsøgtes udlevering af NemID-oplysninger.

Sagsøgte havde i midten af 2018 udleveret sine NemID-oplysninger til en ukendt person, hvorefter der var optaget et lån på 13.400 kr. hos Ekspres Bank A/S den 10. juli 2018. Fogedretten afsagde den 5. marts kendelse 2020 om, at sagsøgte ved sin handlemåde var klar over, at oplysningerne ikke kunne udleveres til hvem som helst. Fogedretten fandt, at sagsøgte ikke manglede evnen til at handle fornuftsmæssigt, jf. § 46 i lovbekendtgørelse nr. 1015 af 20. august 2007 med senere ændringer (»den danske værgemålslov«). Låneaftalen kunne derfor ikke erklæres ugyldig, og sagen blev fremmet til udlæg. Sagsøgte kærede fogedrettens afgørelse til Østre Landsret, hvorefter landsretten stadfæstede fogedrettens afgørelse. Sagsøgte fik efterfølgende tredjeinstansbevilling fra Procesbevillingsnævnet og ankede landsrettens kendelse til Højesteret.

For Højesteret angik sagen, hvorvidt der aftaleretligt var indgået en gyldig aftale, og i forlængelse heraf om den danske værgemålslovs § 46 fandt anvendelse, så aftalen var ugyldig. Indledningsvist henviste Højesteret til tidligere retspraksis, hvor det var lagt til grund, at en person efter omstændighederne godt kan hæfte for lån ved udlevering af NemID-oplysningerne. Aftaleretligt fandt Højesteret derfor, at der var indgået en låneaftale, selvom den digitale underskrift ikke var tilføjet af indehaveren af det pågældende NemID. Sagsøgte skulle derfor som udgangspunkt hæfte for lånet. Efterfølgende tog Højesteret stilling til rækkevidden af den stærke ugyldighedsregel i den danske værgemålslovs § 46. Højesteret fandt, at sagsøgte på baggrund af lægelige oplysninger havde samme mentale niveau som en 7-årig. Endvidere kunne sagsøgte ikke selv overføre penge. På baggrund heraf lagde Højesteret til grund, at sagsøgte ikke selv besad evnen til at handle fornuftsmæssigt efter § 46 i den danske værgemålslov. Låneaftalen var derfor ikke bindende for sagsøgte, og fogedforretningen blev ikke fremmet.

Læs resumé af dommen her: https://domstol.fe1.tangora.com/Domsoversigt-(H%C3%83%C2%B8jesteretten).31478.aspx?recordid31478=2205

Læs hele dommen her: https://domstol.fe1.tangora.com/media/-300016/files/anomiseret-612021.pdf

Datatilsynet udtalte alvorlig kritik af Familieretshusets behandling af personoplysninger

Det danske Datatilsyn traf den 29. oktober 2021 afgørelse i en sag med journalnummer 2021-32-2143 vedrørende en klage over Familieretshusets behandling af personoplysninger.

Datatilsynet udtalte alvorlig kritik af, at Familieretshusets behandling af personoplysninger ikke var sket i overensstemmelse med reglerne i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 32, stk. 1.

Familieretshuset havde ved en fejl givet klagerens søns biologiske far del i forældremyndigheden over sønnen. Den biologiske far havde derved i omtrent et døgn adgang til en række oplysninger om sønnen, herunder oplysninger om sønnens adresse og skole, uanset at sønnen havde navne- og adressebeskyttelse som følge af blandt andet vold og trusler fra den biologiske far mod klageren og sønnen. Det var Datatilsynets opfattelse, at der bør sikres passende uddannelse af medarbejderne og højere krav til omhyggelighed ved sager om tildeling af forældremyndighed.

Datatilsynet lagde vægt på karakteren af de oplysninger, som en tildeling af forældremyndighed kan give adgang til, og på at børn bør nyde en særlig beskyttelse af deres personoplysninger. Herudover lagde Datatilsynet vægt på det af Familieretshuset anførte om, at den fejlagtige tildeling af forældremyndighed skete som følge af, at klager anvendte den forkerte ansøgningsblanket samt som følge af fejl begået i Familieretshuset. Datatilsynet fandt imidlertid, at Familieretshuset bør tage højde for, at ansøgere ikke altid anvender den korrekte blanket.

Datatilsynet noterede sig, at Familieretshuset har opdateret de ret-

ningslinjer, der anvendes ved tildeling af forældremyndighed, og at der blandt andet er gennemført awareness i afdelingerne.

Læs hele afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/okt/alvorlig-kritik-af-familieretshusets-behandling-af-personoplysninger

Kritik og påbud til Cryos for ikke at give borger indsigt i antallet af donorbørn undfanget ved borgerens sæddonation

Det danske Datatilsyn traf den 26. november 2021 afgørelse i en sag med journalnummer 2020-31-3894, og udtalte kritik af Cryos International A/S' (»Cryos«) undladelse af at oplyse en borger om antallet af donorbørn undfanget ved sæddonation fra borgeren. Cryos' undladelse af at informere borgeren var ikke i overensstemmelse med reglerne i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 15, og Datatilsynet meddelte endvidere Cryos påbud om at udlevere oplysningerne til borgeren jf. GDPR artikel 58, stk. 2, litra c.

Ved mails af 11. og 12. maj 2020 henvendte en borger sig til Cryos for at få oplyst, hvor mange børn der var undfanget ved hjælp af hans sæd, samt hvor mange af de mødre der havde født, som var enlige. Cryos afviste begge anmodninger, hvorefter borgeren anmodede om indsigt i de personoplysninger, Cryos havde om ham jf. GDPR artikel 15 om den registreredes indsigtsret. Cryos afviste igen anmodningen med henvisning til, at udlevering af de pågældende informationer ville krænke hensynet til andres rettigheder, der vejede tungere end hensynet til borgens indsigtsret jf. GDPR artikel 15, stk. 4.

Datatilsynet tog indledningsvist stilling til hvordan personoplysninger i GDPR artikel 15 skal forstås. Tilsynet fandt med henvisning til GDPR artikel 4, stk. 1, nr. 1, at personoplysninger er enhver form for information om en identificeret eller identificerbar fysisk person. I forlængelse heraf afviste Datatilsynet først, at informationer om mødrenes civilstand udgjorde informationer om borgeren selv. Tilsynet statuerede derimod, at informationer, om hvor mange børn der var blevet undfanget med borgerens sæd, udgjorde personoplysninger om borgeren jf. GDPR artikel 15. På den baggrund udtalte Datatilsynet kritik for Cryos' manglende oplysning af borgeren, hvorefter Datatilsynet udstedte et påbud til Cryos om at udlevere oplysningerne til borgeren, jf. GDPR artikel 58, stk. 2, litra c.

Læs hele afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/nov/kritik-og-paabud-til-cryos-for-manglende-indsigt

Alvorlig kritik af Coop Danmark A/S' behandling af oplysninger på virksomhedens fællesdrev

Det danske Datatilsyn traf den 4. november 2021 afgørelse i sag 2021-441-9356, hvor Datatilsynet udtalte alvorlig kritik af Coop Danmark A/S' (»Coop«) behandling af personoplysninger på virksomhedens fællesdrev, der ikke levede op til kravet om fornødne sikkerhedsforanstaltninger efter artikel 32 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«).

Sagen vedrørte personoplysninger om 477 medarbejdere og eksterne konsulenter, der havde været tilgængelige på Coops fællesdrev. Personoplysningerne var både placeret på fællesdrevet af de registrerede selv, samt af Coop forbindelse med ansættelsen og vedrørte perioden 2013-2017. Coop opdagede bruddet i forbindelse med en scanning af drevet den 11. juni 2021 samt den 24. august 2021.

Efter GDPR artikel 32 skal den dataansvarlige træffe passende tekniske og organisatoriske foranstaltninger for at sikre et vist sikkerhedsniveau. Det var Datatilsynets opfattelse, at der skulle stilles højere krav til den dataansvarlige ved systemer med et stort antal oplysninger om et stort antal brugere.

På denne baggrund fandt Datatilsynet, at Coop ikke havde levet op til kravet om fornødne sikkerhedsforanstaltninger i GDPR artikel 32, hvor Datatilsynet særligt lagde vægt på, at oplysningerne havde været tilgængelige fra 2013 til 2021, og at Coop burde have været opmærksom på, at medarbejdere kunne have placeret personoplysninger på drevet. Datatilsynet udtalte i den forbindelse alvorlig kritik af, at behandlingen af personoplysninger ikke var sket i overensstemmelse med artikel 32.

Læs hele afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/nov/alvorlig-kritik-af-coop-danmark-as%e2%80%99-behandling-af-oplysninger-paa-virksomhedens-faellesdrev-

Den Katolske Kirke får kritik og påbud om behandling af indsigtsanmodning

Det danske Datatilsyn udtalte den 24. november 2021 kritik af Den Katolske Kirke i Danmarks besvarelse af en indsigtsanmodning i sag med journalnummer 2021-31-4650. Derudover meddelte Datatilsynet Den Katolske Kirke et påbud om at foretage en ny vurdering af klagers indsigtsanmodning.

Den 17. februar 2021 anmeldte klager et afslag på indsigtsanmodning til Datatilsynet. Klager var blevet nægtet adgang til indsigt i, hvad to vidner i sagen blev spurgt om, og hvad de havde svaret. Vidnerne blev overordnet spurgt ind til klager og klagers eksmands tidligere ægteskab, med henblik på at få annulleret et ægteskab i Den Katolske Kirke.

Datatilsynet fandt, at der var grundlag for at udtale kritik af, at Den Katolske Kirkes besvarelse af indsigtsanmodningen var sket i strid med reglerne i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016

(»GDPR«) artikel 15. Den Katolske Kirke havde ikke sandsynliggjort, at klagers eksmands religionsfrihed, præsternes tavshedspligt og vidnernes rettigheder, kunne føre til en afvisning om indsigtsanmodning. Endvidere havde Den Katolske Kirke ikke foretaget en konkret afvejning i forhold til de enkelte oplysninger, men generelt afvist at udlevere oplysningerne.

Datatilsynet fandt endvidere grund til at anmelde Den Katolske Kirke et påbud om (1) at tage stilling til hvorvidt betingelserne for at give klager indsigt efter GDPR artikel 15 er opfyldt, og (2) at meddele klager, om anmodningen om indsigt imødekommes eller afslås. Vurderer Den Katolske Kirke, at indsigten skal imødegås skal denne vedlægge en kopi af personoplysningerne sammen med meddelelsen. Vurderer Den Katolske Kirke omvendt, at indsigt ikke kan imødekommes, skal oplysninger herom vedlægges meddelelsen Fristen for efterlevelse af påbuddet var 6 uger.

Læs hele afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/nov/den-katolske-kirke-faar-kritik-og-paabud-om-behandling-af-indsigtsanmodning-

Datatilsynet indstiller Kræftens Bekæmpelse til bøde

Det danske Datatilsyn anmeldte den 29. september 2021 Kræftens Bekæmpelse til politiet og indstillede dem til en bøde på 800.000 kr., fordi de ikke havde truffet passende sikkerhedsforanstaltninger til beskyttelse af borgeres helbredsoplysninger.

Sagen vedrørte fire brud på persondatasikkerheden, der skyldtes, at Kræftens Bekæmpelse havde undladt at implementere sikkerhedsforanstaltninger, som de selv havde vurderet passende efter et lignende brud i 2018. Dette resulterede i, at mindst 1.448 personers oplysninger blev kompromitteret, herunder helbredsoplysninger.

Datatilsynet lagde ved bødeindstillingen blandt andet vægt på, at de sikkerhedsforanstaltninger, som Kræftens Bekæmpelse selv vurderede passende i 2018, ikke blev implementeret, herunder at det var særlig vigtigt for en dataansvarlig at gennemføre tiltag, som de selv havde identificeret i en risikovurdering som nødvendig.

Der blev i forbindelse med bødeudmålingen bemærket, at på trods af Kræftens Bekæmpelses indsats til behandling af kræft, var det væsentligt, at dette arbejdsområde normalt behandler personlige oplysninger, hvilket medfører et ansvar som organisationen skal leve op til. Ved bødeudmålingen blev dog alene taget udgangspunkt i indtægter fra genbrug, arrangementer og salg af merchandise og andre produkter, svarende til 10 procent af den samlede indtægt, hvorved donationer ikke indgik i beregningen af indtægter.

Læs hele nyheden her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/sep/kraeftens-bekaempelse-indstillet-til-boede

Ny vejledende tekst fra Datatilsynet om brug af personoplysninger i testøjemed

Den 27. oktober 2021 udgav Det danske Datatilsyn en vejledende tekst om, hvilke forholdsregler man skal tage, når man bruger personoplysninger ved udvikling og test af IT-systemer. Teksten giver vejledning om, hvornår det kan være velbegrundet at bruge personoplysninger i test- og udviklingsøjemed, og om hvilke rettigheder og pligter man skal have for øje, når man bruger personoplysninger i den forbindelse.

Ved udvikling og drift af IT-systemer anvender man sædvanligvis to slags data: testdata og produktionsdata. Testdata er typisk fiktiv eller anonymiseret data, som bruges til udvikling og test, når IT-systemer (videre)udvikles eller vedligeholdes. Produktionsdata er typisk data fra et system, som allerede er i drift, for eksempel kundeoplysningerne i et kundesystem eller regnskabsoplysningerne i et økonomistyringssystem. Produktionsdata kan således indeholde uanonymiserede personoplysninger. I nogle tilfælde kan det være nødvendigt at bruge produktionsdata (med personoplysninger) i forbindelse med udvikling og test af IT-systemer.

Den vejledende tekst understreger, at der stadig er tale om behandling af personoplysninger, når personoplysninger fra produktionsmiljøet bruges i forbindelse med test, selvom de får karakter af testdata.. Behandlingen skal derfor overholde databeskyttelsesreglerne, og der gælder ikke et lavere beskyttelseshensyn til personoplysningerne, blot fordi de får karakter af testdata.

Jo tættere man som virksomhed eller myndighed kommer på produktionsfasen, des mere velbegrundet kan det være at anvende produktionsdata, herunder personoplysninger, skriver Datatilsynet. I nogle tilfælde vil det endda være forbundet med manglende sikkerhed at sætte et system i produktion uden først at have testet med personoplysninger.

Der gives tre eksempler på, hvornår det efter omstændighederne kan være velbegrundet og nødvendigt at bruge personoplysninger ved udvikling og test af IT-systemer:
1) ved afsluttende tests af integrationer til andre (eksterne) IT-systemer, 2) når det er forbundet med betydelige vanskeligheder at skabe retvisende (anonymiserede) testdata og 3) i forbindelse med fejlsøgning og fejlretning.

Til sidst i den vejledende tekst gennemgås fire områder af rettigheder og pligter, man skal sørge for at have styr på, når man bruger personoplysninger i udviklings- og testøjemed:

1. **Behandlingsgrundlag**: Man skal sikre sig fornøden behandlingshjemmel, før man behandler

personoplysninger i forbindelse med udvikling og test af IT-systemer. Behandlingshjemlen findes primært i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 6. Det vil typisk være afgørende, om test og udvikling af IT-systemet er nødvendigt for, at behandlingen af personoplysninger til det oprindelige formål (eksempelvis, at man kan behandle ordrer i et kunde-/ordresystem) kan ske. Er det nødvendigt, vil behandlingsgrundlaget normalt være det samme. Er det ikke nødvendigt, er behandlingen som oftest uforenelig med det oprindelige formål, og de indsamlede oplysninger kan ikke bruges til test og udvikling af IT-systemer medmindre et nyt behandlingsgrundlag sikres.

2. **Dataminimering**: Man må ikke behandle flere personoplysninger end nødvendigt for at opnå testformålet i forbindelse ved test og udvikling, og man må kun bruge personoplysninger ved udførelse af tests, hvis testene ikke kunne udføres uden brug af personoplysninger.
3. **Sletning**: Det må ikke være muligt at identificere de registrerede personer i længere tid end nødvendigt for de formål, personoplysningerne behandles til. Man skal derfor tage stilling til, hvornår og hvordan personoplysningerne skal anonymiseres og sikre at sletning sker, når testen er afsluttet. Hvis testmiljøet senere bliver til produktionsmiljøet, skal man være særlig opmærksom på at slette alle personoplysninger, som kun bruges til testformålet, inden testmiljøet overgår til produktionsmiljø.
4. **Behandlingssikkerhed**: Når man behandler personoplysninger i testøjemed, skal man foretage en konkret risikovurdering for de registrerede og etablere passende tekniske og organisatoriske sikkerhedsforanstaltninger i overensstemmelse hermed. Man skal navnlig tage hensyn til risici som hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysningerne. I tilfælde, hvor der vurderes at være en høj risiko, skal man skal foretage en konsekvensanalyse.

Hvad angår sikkerhedsforanstaltningerne, er det Datatilsynets opfattelse, at man som udgangspunkt skal etablere de samme foranstaltninger i testmiljøet, som er vurderet passende i produktionsmiljøet. Det gælder især for adgangsstyring, logning, sikker overførsel af data mellem IT-miljøer og sikkerhedsopdateringer af software, servere mv. (patching). Hvilke sikkerhedsforanstaltninger, som er passende, kan dog afhænge af, hvilket netværk testmiljøet kan tilgås fra, og om det kan eller ikke kan tilgås fra internettet. Det nævnes desuden, at pseudonymisering er en særlig relevant foranstaltning i test- og udviklingsmiljøer, da viden om konkrete personer ofte ikke er afgørende for testen.

Læs hele den vejledende tekst her: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/testdata-brug-af-personoplysninger-ved-udvikling-og-test-af-it-systemer

Nye retningslinjer om samspillet mellem anvendelsen af GDPR artikel 3 om territorialt anvendelsesområde og bestemmelserne om internationale overførsler i kapitel V i GDPR

Den 18. november 2021 vedtog Det Europæiske Databeskyttelsesråd (»EDPB«) Retningslinjer 05/2021 om samspillet mellem anvendelsen af artikel 3 og bestemmelserne i kapitel V om internationale overførsler i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«). Formålet med retningslinjerne er at skabe klarhed over samspillet mellem GDPR artikel 3 og kapitel V. De skal gøre det lettere at finde ud af, om en behandlingsaktivitet udgør en international overførsel, og dermed om GDPR kapitel V skal overholdes.

Kapitel V gælder for »overførsler« af personoplysninger til tredjelande eller internationale organisationer. Retningslinjerne fremhæver, at formålet med kapitel V er at sikre, at beskyttelsesniveauet efter GDPR ikke undermineres af, at personoplysninger overføres til tredjelande eller internationale organisationer. Kapitlets bestemmelser supplerer GDPRs territoriale anvendelsesområde som defineret i GDPR art. 3, når personoplysninger overføres til lande uden for EU.

GDPR indeholder ingen definition af, hvad en »overførsel« indebærer. For at skabe klarhed har EDPB i retningslinjerne opstillet tre kumulative kriterier:

1. En dataansvarlig eller databehandler (dataeksportøren) er omfattet af GDPR (jf. GDPR artikel 3) med hensyn til den pågældende behandling,
2. Dataeksportøren transmitterer eller stiller personoplysningerne til rådighed for en anden dataansvarlig, fælles dataansvarlig eller databehandler (dataimportøren) og
3. Dataimportøren er et tredjeland eller en international organisation.

Hvis kriterierne er opfyldt, betragtes behandlingen som en overførsel i kapitel Vs forstand, uanset om dataimportøren allerede er omfattet af GDPR i henhold til artikel 3 i GDPR.

EDPB fremhæver, at dataansvarlige eller databehandlere, der ikke er etableret i EU, godt kan opfylde det første kriterium, hvis de er omfattet af GDPR efter GDPR artikel 3, stk. 2 om udbud af varer/tjenester til eller overvågning af registrerede i EU. Sådanne dataansvarlige og databehandlere skal således overholde

kapitel V, når de overfører personoplysninger til tredjelande eller internationale organisationer.

Angående det andet kriterium fremhæver EDPB en række pointer i retningslinjerne, heriblandt:

- Det andet kriterium anses ikke for at være opfyldt, når indsamling af personoplysninger sker direkte fra den registrerede i EU og på dennes eget initiativ. Der er ikke nogen dataeksportør i sådanne tilfælde, hvorfor indsamling ikke udgør en overførsel. I retningslinjerne gives et eksempel med en forbruger i Italien, som indsætter sine personoplysninger i en formular i forbindelse et onlinekøb af tøj.
- Der er kun tale om en overførsel, når dataimportøren er forskellig fra dataeksportøren. Som eksempel gives, at en ansat hos en databehandler i Polen rejser til et møde i Indien. I Indien tilgår den ansatte personoplysninger fra sin arbejdsgivers databaser for at færdiggøre et notat. I et sådant tilfælde er der ikke tale om en overførsel, da den ansatte er en del af den dataansvarlige virksomhed i Polen. Der sker dermed ingen overførsel til en anden dataansvarlig eller databehandler.
- Juridiske personer, som er en del af den samme koncern, kan udgøre forskellige dataansvarlige eller databehandlere. Der gives et eksempel, hvor det udgør en overførsel, at et irsk datterselskab videregiver personoplysninger om sine ansatte til sit amerikanske moderselskab.

Konsekvensen af, at de tre kriterier er opfyldt, er, at der er er tale om en overførsel, og at bestemmelserne i GDPR kapitel V dermed skal overholdes. Efter GDPR kapitel V kan overførsel kun ske, hvis Kommissionen har truffet afgørelse om tilstrækkeligt beskyttelsesniveau i tredjelandet eller den internationale organisation, jf. GDPR artikel 45, hvis der afgives fornødne garantier, for eksempel Kommissionens Standard Contractual Clauses, jf. GDPR artikel 46, eller hvis en af undtagelsesbestemmelserne i GDPR artikel 49 finder anvendelse.

Når en overførsel foretages på grundlag af GDPR artikel 46, skal det vurderes, om det er nødvendigt at foretage supplerende foranstaltninger. Hvis dataimportøren allerede er omfattet af GDPR, jf. GDPR artikel 3, stk. 2, er det ikke meningen, at man skal duplikere forpligtelserne efter GDPR, men i stedet adressere de risici, som GDPR ikke allerede dækker. Det er for eksempel risici relateret til tredjelandes loves eventuelle strid med GDPR, tredjelandsregeringers (for) vidtgående adgang til personoplysninger og vanskeligheder ved at håndhæve rettigheder over for en enhed uden for EU.

Retningslinjerne understreger, at også i de tilfælde, hvor der er ikke er tale om en overførsel efter kapitel V, kan databehandling indebære risici i et sådant omfang, at der skal træffes foranstaltninger. Det kan for eksempel være tilfældet, når nationale love i tredjelandet er i strid med GDPR, eller når det er vanskeligt håndhæve rettigheder over for en enhed uden for EU. En dataansvarlig skal altid overholde GDPR, uanset hvor behandlingen finder sted. For eksempel kan en dataansvarlig med afsæt i GDPR artikel 32 om behandlingssikkerhed komme frem til, at det vil være ulovligt eller kræve vidtgående sikkerhedsforanstaltninger at foretage en behandling i et tredjeland, selvom der ikke er tale om en overførsel. Databehandleren kan da eksempelvis beslutte, at ansatte ikke må medbringe laptops mv. til særlige tredjelande.

Læs nyheden her: https://edpb.europa.eu/news/news/2021/edpb-adopts-guidelines-interplay-between-art-3-and-chapter-v-gdpr-statement-digital_da

Læs retningslinjerne her: https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf

WhatsApp har modtaget en bøde på 225 millioner euro fra det irske datatilsyn

Det Europæiske Databeskyttelsesråd (»EDPB«) vedtog den 28. juli 2021 en bindende afgørelse rettet mod det irske datatilsyn, i forbindelse med en tvist vedrørende WhatsApp Ireland Ltd. (»WhatsApp«). Det irske datatilsyn skulle ændre sin afgørelse i forhold til overtrædelser af princippet om gennemsigtighed, beregningen af bøden og fristen for at efterkomme afgørelsen.

Det irske datatilsyn havde allerede konstateret overtrædelser af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 12-14 om oplysningspligt ved indsamling af personoplysninger. EDPB fandt i tillæg, at overtrædelsernes alvor gjorde, at der også var sket en overtrædelse af gennemsigtighedsprincippet i GDPR artikel 5, stk. 1, litra a. Det irske datatilsyn, skulle derfor i sin endelige afgørelse medtage en følgeslutning om krænkelse af det fastlagte gennemsigtighedsprincip.

EDPB besluttede endvidere, at en virksomheds omsætning ikke kun er relevant for størrelsen af det maksimale bødebeløb, men også ved beregningen af selve bøden, for at sikre at den er effektiv, forholdsmæssig og har afskrækkende virkning. Derfor skulle moderselskabet Facebook Inc.'s omsætning medregnes ved beregningen af bøden. Desuden præciserede EDPB, at alle overtrædelser i forbindelse med samme eller tilknyttede behandlingsaktiviteter skal tages i betragtning ved beregningen af bødens størrelse. Det er første gang EDPB præciserer fortolkningen af artikel 83, stk. 3 i databeskyttelsesforordningen. Til sidst anmodede EDPB det irske datatilsyn om at ændre fristen i sin afgørelse, for at WhatsApp skulle bringe sine aktivi-

teter i overensstemmelse med reglerne, fra 6 til 3 måneder.

EDPB pålagde det irske datatilsyn at revurdere sin påtænkte administrative bøde i overensstemmelse med EDPBs konklusioner, heriblandt at (1) den relevante omsætning er den globale årlige omsætning for alle komponentselskaberne i virksomheden, (2) den relevante omsætning er den, der svarer til regnskabsåret forud for datoen for den endelige beslutning truffet af den ledende tilsynsmyndighed, (3) den relevante omsætning er relevant for fastsættelse af bøden således at den er effektiv og forholdsmæssig, og (4) bødens størrelse skal afspejle skærpende faktorer. Det irske datatilsyn skulle endvidere kommunikere den endelige beslutning til Det Europæiske Databeskyttelsesråd inden 1 måned efter modtagelse af rådets bindende beslutning.

Det irske datatilsyn har ændret sin nationale afgørelse i overensstemmelse med EDPBs bindende afgørelse.

Læs pressemeddelelsen her: https://edpb.europa.eu/news/news/2021/edpb-requests-irish-sa-amends-whatsapp-decision-clarifications-transparency-and_en

Læs den bindende afgørelse her: https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12021-dispute-arisen_en

Sydkorea anerkendes som et sikkert tredjeland

Den 17. december 2021 godkendte EU-Kommissionen Sydkorea som et sikkert tredjeland i relation til Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«). Det skete ved en udstedelse af en tilstrækkelighedsafgørelse, hvoraf Sydkorea anses for et sikkert tredjeland. Dermed kan man fremover overføre personoplysninger til Sydkorea uden et overførelsesgrundlag.

EU domstolen klargjorde, at det ikke kræver et EU-identisk niveau af beskyttelse, før et land kan anerkendes som et sikkert tredjeland. Ved tilstrækkelighedskonstateringen vurderes det, om systemet i sin helhed understøtter det nødvendige niveau af beskyttelse. Der kigges her især på selve beskyttelsen, implementeringen og håndhævelsen af systemet. Det er ud fra denne vurdering, at Kommissionen har vurderet, at Sydkorea har et tilstrækkeligt beskyttelsesniveau af personoplysninger.

For at sikre et tilstrækkeligt niveau af datasikkerhed, har Sydkorea implementeret en række love, herunder »The Personal Infor mation Protection Act (PIPA)«, »The Act on the Use and Protection of Credit Information« og »The Communications Privacy Protection Act«. Disse tre love sikrer alle individers datasikkerhed, uafhængigt af deres nationalitet. Nærmere gennemgang af lovene, findes i linket til nyheden.

EU-Kommissionens tilstrækkelighedsafgørelse omfatter ikke behandling af personoplysninger for missionere aktiviteter af religiøse organisationer, for nominering af kandidater af politiske partier, eller af behandling af personlige kreditoplysninger i henhold til kreditoplysningsloven af dataansvarlige, der er underlagt tilsyn af finanstilsynet.

EU-Kommissionens afgørelse har den retsvirkning, at der fremover er mulighed for, at overføre personoplysninger til registreringsansvarlige og databehandlere i Sydkorea, uden yderligere tilladelse.

Læs nyheden her: https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf

Frederiksberg Kommune indstilles til bøde

Det danske datatilsyn anmeldte den 16. december 2021 Frederiksberg Kommune til politiet, da Datatilsynet vurderede, at kommunen ikke levede op til et passende sikkerhedsniveau i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«).

Den 1. marts 2021 anmeldte Frederiksberg Kommune et brud på persondatasikkerheden til Datatilsynet. Det fremgik af sagen, at kommunen havde udvidet den kommunale tandplejes selvbetjeningsløsning fra at omfatte bopælsforældres adgang til tandplejens breve, til også at omfatte samværsforældre med fælles myndigheds adgang til breve. Det indebar, at forældre fik oplysninger om bopælsforælderens og barnets adresse, uagtet at disse var registreret med navne- og adressebeskyttelse. Dette ville have stor betydning i sager, hvor barnet var navne- og adressebeskyttet med henblik på, at den anden forælder ikke fik adgang til oplysninger om barnet.

På baggrund af sagens grovhed valgte Datatilsynet, efter en vurdering efter GDPR artikel 83, stk. 2, at politianmelde Frederiksberg Kommune samt indstille, at der nedlagdes påstand om en bøde på 100.000 kr.

Læs nyheden her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/dec/frederiksberg-kommune-indstilles-til-boede

Udtalelse fra EDPB om tilsynsmyndigheds påbud om sletning (ex officio)

Den 14. december 2021 vedtog Det Europæiske Databeskyttelsesråd udtalelse 39/2021 om, hvorvidt artikel 58, stk. 2, litra g i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) kunne udgøre hjemmel for, at en tilsynsmyndighed kunne pålægge ex officio sletning af personoplysninger i en situation, hvor en sådan anmodning ikke blev indgivet af den registrerede. Det Europæiske Databeskyttelsesråd tog stilling til denne problemstilling på baggrund af en anmodning fra det ungarske datatilsyn fremlagt den 6. oktober 2021.

Hver medlemsstats tilsynsmyndighed er ansvarlig for at overvåge anvendelsen af GDPR for at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder i forhold til databehandling og for at lette den frie strøm af personoplysninger inden for Det Europæiske Økonomiske Samarbejde (»EØS«). Tilsynsmyndigheden har efter GDPR artikel 58, stk. 2 en række korrigerende beføjelser til brug for at sikre overholdelsen af GDPR, herunder faktisk stærk håndhævelse, konsekvent og homogen anvendelse af reglerne og ækvivalente sanktioner for overtrædelser. Det ungarske datatilsyn satte derfor spørgsmålstegn ved, om dette giver tilsynsmyndigheden mulighed for at handle uden opfordring fra den registrerede.

Det Europæiske Databeskyttelsesråd tog først stilling til, om GDPR artikel 17 udelukkende pålægger den dataansvarlige en forpligtelse til at slette personoplysninger efter anmodning fra den registrerede. Artikel 17 fastslår på den ene side den registreredes ret til at anmode om sletning af deres personoplysninger og på den anden side den dataansvarliges forpligtelse til at slette disse data, hvor en af de oplistede grunde i artiklen finder anvendelse. Det Europæiske Databeskyttelsesråd undersøgte herefter, om denne forpligtelse er betinget af, at en registreret udøver retten, eller den eksisterer uafhængigt af enhver anmodning fra den registrerede. Det der talte for, at retten eksisterede uafhængigt af anmodning, var, at den dataansvarlige har en forpligtelse til at slette oplysninger, der ikke længere er relevante.

Det Europæiske Databeskyttelsesråd fandt herefter, at GDPR artikel 17 beskyttede både situationer, hvor den registrerede anmoder om sletning af data, samt situationer hvor databehandleren har en selvstændig forpligtelse til at slette data.

På baggrund af ovenstående fandt Det Europæiske Databeskyttelsesråd, at GDPR artikel 58, stk. 2, litra g udgjorde et gyldigt retsgrundlag for, at en tilsynsmyndighed ex officio kan påbyde sletning af ulovligt behandlede personoplysninger i en situation, hvor en sådan anmodning ikke er blevet indgivet af den registrerede.

Læs nyheden her: https://edpb.europa.eu/system/files/2022-01/edpb_opinion_202139_article_582g_gdpr_en.pdf

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



Wiersholm

Rune Opdahl, Anne-Marit Wang Sandvik, og Carl Emil Bull-Berg

Tilsynsmyndigheter mener bruk av Google Analytics er ulovlig

Det østerrikske og franske datatilsynet har vedtatt at bruk av Google Analytics er i strid med GDPR. Det norske Datatilsynet har sagt seg enig i denne konklusjonen. Dette kan bety at norske virksomheter bør revurdere sin bruk av Google Analytics. I tillegg indikerer det franske datatilsynet at flere avgjørelser vil komme; disse vil ikke kun vil være rettet mot Google Analytics, men også mot andre verktøy som overfører personopplysninger til USA.

I kjølvannet av avgjørelsen fra det østerrikske datatilsynet (DSB) anbefaler Datatilsynet at norske virksomheter leter etter europeiske alternativ til Google Analytics. Seksjonssjef i Datatilsynet, Tobias Judin, har uttalt til Digi.no at det «i praksis er vanskelig å se hvordan nettsider lovlig kan bruke Google Analytics».

Etter DSB-avgjørelsen og uttalelsen til Judin, har det franske datatilsynet (CNIL) via en pressemelding kommunisert at også de har kommet til at overføringer av personopplysninger til USA via Google Analytics er i brudd med GDPR. CNIL har ikke tilgjengeliggjort selve avgjørelsen, men pressemeldingen deres inneholder noen interessante uttalelser. CNIL skriver, blant annet, hvordan de har analysert Google Analytics «in cooperation with its European counterparts». Dette gir en klar indikasjon på at CNILs syn om Google Analytics deles av øvrige tilsynsmyndigheter. Dette er også slik Max Schrems (lederen bak organisasjonen som sendte inn de aktuelle klagene) har tolket uttalelsen til CNIL. Han sa følgende om CNILs avgjørelse:

> It's interesting to see that the different European Data Protection Authorities all come to the same conclusion: the use of Google Analytics is illegal. There is a European task force and we assume that this action is coordinated and other authorities will decide similarily.

Uansett skal GDPR praktiseres likt i hele EØS. Det norske Datatilsynet vil derfor se hen til DSBs og CNILs avgjørelser, og avgjørelser fra andre europeiske datatilsyn som i fremtiden kan komme, i behandlingen av sine saker.

Foreløpig har Datatilsynet én sak om Google Analytics til behandling, og flere lignende saker verserer for andre europeiske datatilsyn. Hvis de følger DSB og CNIL, noe som er veldig sannsynlig, kan det i praksis resultere i et europeisk forbud mot Google Analytics.

Datatilsynet fremhever imidlertid at Google Analytics ikke er verst i klassen, ved at det finnes andre analyseverktøy som samler inn mer data. På Datatilsynets nettsider uttaler Judin at ulovlig verktøy må fjernes omgående, og at alvorlige saker vil resultere i gebyrer. Det er derfor veldig interessant at CNIL i pressemeldingen sin nettopp fremhever at etterforskningen deres, som har blitt utført sammen med deres «European counterparts», ikke kun omfatter Google Analytics, men også andre verktøy brukt av nettsider som kan innebære overføringer av personopplysninger til USA. De advarer at korrigerende tiltak kan bli vedtatt mot slike, i nærmeste fremtid.

IP-anonymisering ser ikke ut til å hjelpe

GDPR forbyr som utgangspunkt overføring av personopplysninger ut av EØS. DSB og CNIL mener Goo-

gle Analytics samler inn personopplysninger og at disse overføres til USA. Det europeiske datatilsynet (EDPS) har nylig konkludert tilsvarende i en sak om bruk av Google Analytics på EU-parlamentets nettside.

Google har argumentert for at opplysningene som samles inn via Google Analytics ikke er personopplysninger fordi Google ikke kobler opplysningene de samler inn til enkeltindivider. Verken DSB eller EDPS er enige i dette. Etter deres syn er det «digitale fotavtrykket», bestående av for eksempel cookie-ID, IP-adresse, nettleser og operativsystem, nok til at det er snakk om personopplysninger, selv om identifikatorer som navn ikke samles inn. Avgjørende for DSB og EDPS synes å være at det er mulig å «single ut» en bruker fra en annen, uavhengig om brukerens identitet er kjent. CNIL har ikke redegjort ordentlig for sin begrunnelse, men ser ut til å ha samme tilnærming.

Google tilbyr en funksjon for IP-anonymisering, som gjør at IP-adresse ikke overføres. Det østerrikske nettstedet i saken for DSB hadde ikke implementert denne funksjonen på riktig måte. DSB mente imidlertid at dette uansett neppe ville vært avgjørende fordi IP-adressen kun utgjør en liten del av det digitale fotavtrykket.

Det er ikke gitt at tilsynsmyndighetenes forståelse er riktig, eller at den ikke kan nyanseres. For det første var personen som klaget inn Google til DSB logget inn på sin Google-konto. Det er noe uklart om konklusjonen hadde blitt den samme hvis personen ikke hadde en Google-konto (selv om en slik distinksjon vil være krevende for en nettsideeier å praktisere). For det andre følger det av GDPR at en «online identifier» først er en personopplysning hvis det rimeligvis kan tenkes at brukeren kan bli identifisert, sett hen til teknologien, kostnadene og tiden det vil ta. DSB og EDPS tar nok noe lett på dette kriteriet. Ettersom CNIL ikke har publisert avgjørelsen sin er det ikke klart om de adresserer dette kriteriet i større utstrekning enn DSB og EDPS.

Kryptering fremstår som det eneste virkemiddelet

For å overføre personopplysninger på lovlig vis til USA, må personopplysninger gis tilnærmet samme beskyttelse som i EØS. Dette vil kreve tiltak, fordi amerikansk personvernlovgivning er fragmentert, og fordi amerikanske etterretningslover gir myndighetene vid adgang til data.

Google forsøkte å overbevise DSB om at selskapet har innført egnede sikkerhetstiltak. Selskapet presenterte omfangsrik dokumentasjon på alt fra inngjerding av serverparker og ende-til-ende kryptering, men DSB lot seg ikke overbevise. DSB vurderte det slik at så lenge Google selv har krypteringsnøkkelen, vil amerikanske myndigheter kunne få tak i nøkkelen og derigjennom personopplysningene. DSBs avgjørelse indikerer at det eneste tiltaket som kan være tilstrekkelig er kryptering av opplysningene før overføring til USA, og hvor krypteringsnøkkelen er utilgjengelig for Google. Det er tvilsomt om en slik løsning er særlig praktisk. CNIL har i sin pressemelding kun skrevet at Google har implementert supplerende tiltak, men at disse ikke er tilstrekkelige for å hindre etterretningsmyndigheter i USA fra å få tilgang til opplysningene. Det virker derfor som at de har hatt samme innfallsvinkel som DSB.

Hva bør man gjøre nå

Vi anbefaler at norske virksomheter som bruker Google Analytics om å se etter et europeisk alternativ. Ved fortsatt bruk av Google Analytics anbefaler vi at IP-anonymisering aktiveres (selv om dette ikke uten videre er tilstrekkelig). Dessuten må man sørge for at brukerne gis informasjon, f.eks. i en cookie-policy, om hvilke cookies som benyttes, hvilke opplysninger som behandles, hvem som behandler opplysningene, formålet med behandlingen, hvor lenge opplysningene blir lagret, om data overføres ut av EØS, og i så fall hvilket overføringsgrunnlag som benyttes.

Samtidig bør ikke betydningen av tilsynsmyndigheters avgjørelser overdrives. Når de også fungerer som ombud for individers personvern, vil avgjørelsene ofte ha en slagside. Avgjørelsene kan overprøves av domstolene. Det vil være en fordel med domstolsprøving før alle aktører endrer en langvarig praksis.

Faktaboks

- Skepsisen til overføringer av personopplysninger ut av EØS har økt siden Snowden-avsløringene tilbake i 2013.
- GDPR, som ble innført i 2018, gjør det i utgangspunktet ulovlig å overføre personopplysninger ut av EØS.
- Frem til 2020 kunne likevel europeiske virksomheter overføre personopplysninger ved å inngå en standardavtale (SCC) med selskapet utenfor EØS, eller ved å påse at selskapet (om det var amerikansk) var underlagt sertifiseringsordninger, som Privacy Shield.
- Etter EU-domstolens avgjørelse i Schrems II-saken i 2020 er dette ikke lenger nok. Nå kreves det også en vurdering av lovgivningen i mottakerlandet, særlig i hvilken grad landets myndigheter kan kreve tilgang til opplysningene.
- Hvis lovgivningen ikke er tilstrekkelig, må det innføres tiltak for å kompensere for dette. I følge det Europeiske personvernrådet er det mest egnede tiltaket å kryptere opplysningene før overføring og la krypteringsnøkkelen forbli i Europa.

Rune Opdahl er advokat og partner i Wiersholms team for teknologi og immaterialrett.
Anne-Marit Wang Sandvik er Managing Associate i advokatfirmaet Wiersholm.
Carl Emil Bull-Berg er advokatfullmektig i advokatfirmaet Wiersholm.

Delphi

Olga Sahlén

I denna notis kommer två utvalda nyheter från den svenska tillsynsmyndigheten Integritetsskyddsmyndigheten (”IMY”) samt en dom från förvaltningsrätten presenteras.

IMY utfärdar sanktionsavgift mot Region Uppsala

IMY meddelade den 27 januari 2022 att myndigheten utfärdar administrativa sanktionsavgifter mot Region Uppsala på sammanlagt 1,9 miljoner kronor avseende två personuppgiftsincidenter. Regionen har, vid den ena incidenten, skickat känsliga personuppgifter och personnummer via automatiserade e-postmeddelanden till samtliga Region Uppsalas e-postdomäner. E-postmeddelanden har också skickats manuellt till läkare och forskare inom regionen. Den andra incidenten rör hur Akademiska sjukhuset i Uppsala skickat e-postmeddelanden innehållande patientuppgifter till mottagare i tredjeland samt sjukhusets lagring av patientuppgifter, där journalhandlingarna utöver lagringen i huvudjournalsystemet även lagrats i Outlook.

Uppgifter om hälsa utgör känsliga personuppgifter vilka enligt dataskyddsförordningen (”GDPR”) är förbjudna att behandla, såvida behandlingen inte omfattas av ett angivet undantag i GDPR. Omfattas behandlingen av ett undantag uppställer GDPR krav på att lämpliga tekniska och organisatoriska åtgärder ska vidtas vid behandlingen.

IMY konstaterar att regionen inte har vidtagit lämpliga säkerhetsåtgärder då även informationen i e-postmeddelandena ska skyddas med lämplig säkerhetsåtgärd och inte endast överföringen. Vidare anger IMY att ett e-postsystem såsom Outlook generellt sett utgör en olämplig lagringsplats för känsliga personuppgifter, då personuppgifterna riskerar att exponeras på internet vilket kan resultera i obehörig åtkomst. I denna del granskade IMY enbart säkerheten för behandlade personuppgifter och inte lagligheten i själva tredjelandsöverföringen. Vidare pekar IMY på att Region Uppsala, i båda fallen, behandlat personuppgifter i strid med regionens egna riktlinjer, vilket indikerar brister i de organisatoriska åtgärderna.

Sammantaget visar granskningarna att Region Uppsala inte har vidtagit tillräckliga säkerhetsåtgärder för att skydda känsliga personuppgifter i de e-postmeddelanden som skickats och inte heller vidtagit tillräckliga säkerhetsåtgärder vid lagring av personuppgifter i sjukhusets e-postserver. Behandlingarna har således skett i strid med GDPR.

Grönt ljus att kamerabevaka offentliga platser?

I maj 2017 beviljade Länsstyrelsen i Uppsala kamerabevakning av en bubbelpool i realtid dygnet runt i syfte att upptäcka, begränsa samt förhindra olyckor.

IMY överklagade Länsstyrelsens beslut. Efter att både förvaltningsrätten och kammarrätten avslagit överklagandet tog Högsta förvaltningsdomstolen (”HFD”) upp målet och prövade frågan om förutsättningarna för att bevilja kamerabevakning var uppfyllda.

För kamerabevakning av en plats som allmänheten har tillträde till krävs enligt kamerabevakningslagen tillstånd i vissa fall. Vid tillståndsprövningen sker en intresseavvägning mellan intresset av bevakning å ena sidan och den enskildes intresse av att inte bli bevakad å andra sidan. Tillstånd ska beviljas om bevakningsintresset väger tyngre än den enskildes intresse av att inte bli bevakad. I förarbetena anges att kamerabevakning ska kunna användas i samtliga skeden av ett olycksförlopp. I syfte att förhindra olyckor väger således bevakningsintresset tungt, därmed kan tillstånd för kamerabevakning ges även vid större integritetsintrång.

HFD anger i domen att det inte är en förutsättning att en olycka faktiskt har inträffat just på den plats som ska bevakas för att en förhöjd risk för olyckor ska anses föreligga. Det är tillräckligt att olyckor har inträffat i närheten av platsen för att olycksrisken ska anses som reell. HFD vägde också in i bedömningen att bubbelpoolen var avsides belägen och skyddad från insyn. Det förelåg en förhöjd risk för olyckor vid bubbelpoolen samt fanns ett starkt behov av kamerabevakning för att förebygga olyckor.

Vad gäller den enskildes intresse av att inte bli bevakad konstaterade HFD att integritetsintresset förs-

vagas då de personer som blir föremål för kamerabevakning är desamma som kamerabevakningen syftar till att skydda. Bevakningen ska vidare endast ske i realtid, utan bildinspelning eller ljudupptagning. Sammantaget bedömde HFD integritetsintrånget som förhållandevis litet. Bevakningsintresset vägde tyngre och badhusets kamerabevakning i realtid är i enlighet med kamerabevakningslagen och tillstånd skulle därmed beviljas.

Förvaltningsrätten sätter ned sanktionsavgift mot SL

IMY utfärdade den 21 juni 2021 en administrativ sanktionsavgift mot SL avseende användningen av kroppsburna kameror i samband med biljettkontroll. Syftet med kamerabevakningen var att förebygga och dokumentera hot och våld samt att säkerställa identiteten på resenärer som ålades betala tilläggsavgift. SL överklagade beslutet till förvaltningsrätten (”FR”).

Den 18 februari 2022 slog FR fast att SL behandlat personuppgifter i strid med GDPR.

SL:s användning av kroppsburna kameror för att förebygga och dokumentera hot och våld var visserligen förenlig med GDPR. FR konstaterar däremot att SL inte har haft rätt att använda tekniken för att säkerställa identiteten på resenärer som ska betala tilläggsavgift. Dessutom har SL inte lämnat tillräcklig information, i rätt tid, till de som träffats av kamerabevakningen. IMY bestämde den administrativa sanktionsavgiften till 16 miljoner kronor. FR bestämde sanktionsavgiften till 12 miljoner kronor.

Olga Sahlén er Associate i Advokatfirman Delphi, Stockholm.

Gorrissen Federspiel

Tue Goldschmieding

Domænenavnet »care4pets.dk« skulle ikke overføres til klager

Det danske Klagenævn for Domænenavne traf den 9. november 2021 afgørelse i sag 2021-0213 mellem klager CBD-Care4pets (»Care4pets«) og indklagede INTERFARM AS (»INTERFARM«). Care4pets har siden 2019 drevet virksomhed under navnet »care4pets« med henblik på salg af plejeprodukter til kæledyr. INTERFARM er registrant af domænenavnet »care4pets.dk« og har planer om i fremtiden at udvide sine aktiviteter i hele Skandinavien, herunder Danmark. Sagen drejede sig om, hvorvidt domænenavnet »care4pets.dk« skulle overføres til Care4pets.

Care4pets gjorde gældende, at INTERFARM aldrig havde taget domænet »*www.care4pets.dk*« i brug siden oprettelsen i 2017. Care4pets gjorde endvidere gældende, at Care4pets' forretning var bundet op på navnet, at de havde opnået varemærkeregistrering af ordmærket, og at deres e-mailadresse indeholdt navnet.

Efter en interesseafvejning i medfør af lov nr. 164 af 26. februar 2014 (»den danske domænelov«) § 25, stk. 1 om god domænenavnsskik kom Klagenævnet for Domænenavne frem til, at Care4pets' kommercielle interesse ikke vejede tungere end INTERFARMs interesse i fortsat at kunne disponere over domænenavnet »care4pets.dk«. Klagenævnet lagde blandt andet vægt på, at navnet består af en sammenstilling af to almindelige engelske ord, samt et tal, der almindeligvis tillægges en sproglig betydning. Det måtte endvidere indgå i interesseafvejningen, at andre end sagens parter, som beskæftiger sig med eller er interesserede i plejeprodukter til kæledyr, kan have en naturlig interesse i at råde over domænenavnet.

INTERFARM fandtes ikke i forhold til Care4pets at have handlet i strid med god domænenavnsskik ved at have registreret og opretholdt registreringen af »care4pets.dk«. Care4pets fik derfor ikke medhold i sagen, og INTERFARM kunne beholde registreringen af domænet.

Læs hele afgørelsen her: https://www.domaeneklager.dk/sites/default/files/decision-pdf/2021-0213_care4pets.dk_.pdf

Domænenavnet »smykkekompagniet.dk« skulle overføres til klager

Det danske Klagenævn for Domænenavne traf den 28. oktober 2021 afgørelse i sag 2021-0178 mellem Smykke Kompagniet I/S (»klager«) og ERFA INVENTAR A/S (»indklagede«). Sagen drejede sig om, hvorvidt domænenavnet »smykkekompagniet.dk« skulle overføres til klager.

Klager argumenterede blandt andet for, at indklagede havde købt domænenavnet med henblik på hamstring uden at have til hensigt at benytte domænenavnet, eftersom domænenavnet blev købt mindre end 2 måneder efter klagers virksomhed blev registreret.

Indklagede argumenterede derimod for, at domænenavnet skulle benyttes til en ny forretning med navnet Smykkekompagniet, og påberåbte til støtte herfor, at indklagede foruden at være først til køb af domænenavnet, også havde oprettet en Instagram-profil før klager.

Klagenævnet for Domænenavne foretog en interesseafvejning, herunder en afvejning af, om domænenavnet blev anvendt loyalt og til varetagelse af legitime interesser i medfør af lov nr. 164 af 26. februar 2014 (»den danske domænelov«) § 25, stk. 1, om god domænenavnsskik.

På baggrund af interesseafvejningen fandt Klagenævnet for Domænenavne det ikke godtgjort, at klagers interesse i domænenavnet væsentligt oversteg indklagedes, hvorved der ikke forelå en overtrædelse af domænelovens § 25, stk. 1, om god domænenavnsskik. Klagenævnet for Domænenavne lagde blandt andet vægt på, at indklagede ville benytte domænenavnet til en ny forretning under etablering. Det havde i denne forbindelse ingen betydning, at indklagede endnu ikke havde etableret en hjemmeside på domænenavnet. Indklagede skulle derfor ikke overføre domænenavnet.

Læs hele afgørelsen her: https://www.domaeneklager.dk/sites/default/files/2021-10/2021-0178%2C%20smykkekompagniet.pdf

Domænenavnet »nexta.dk« skulle overføres til klager

Den 28. oktober 2021 traf det danske Klagenævn for Domænenavne afgørelse i sag J.nr.: 2021-0163 mellem klager Nexta ApS og indklagede Medieforeningen 2001 (»Medieforeningen«). Nexta ApS udvikler software, herunder en platform til markedsføringskampagner til brug i e-commerce virksomheder. Nexta

ApS havde registreret domænenavnet »nexta.io« til brug herfor i 2017. Medieforeningen er en forening af medier, der ofte er startups. Foreningen udlejer hosting-servere til sine medlemmer.

Den 14. marts 2020 registrerede Medieforeningen domænenavnet »nexta.dk«. Spørgsmålet i sagen var, om Medieforeningen skulle overføre domænenavnet til Nexta ApS. Den 27. marts 2020 ændrede Nexta ApS selskabsnavn fra Next Advertising ApS til Nexta ApS. Medieforeningen gjorde derfor gældende, at de var først i tid med hensyn til »nexta.dk«.

Klagenævnet for Domænenavne lagde imidlertid til grund, at Nexta ApS »i hvert fald fra maj 2017« havde brugt betegnelsen Nexta i forbindelse med markedsføring og salg i Danmark, og at betegnelsen Nexta i høj grad blev forbundet med netop Nexta ApS på internettet. På den baggrund fandt Klagenævnet for Domænenavne, at Nexta ApS havde opnået beskyttelse efter lov nr. 426 af 3. maj 2017 (»den danske markedsføringslov«) § 22 om beskyttelse af forretningskendetegn forud for Medieforeningens registrering af »nexta.dk«. Klagenævnet fandt dette, selvom Nexta ApS ikke havde gjort noget anbringende vedrørende den danske markedsføringslovs § 22 gældende. Klagenævnet fandt det til gengæld ikke dokumenteret, at Nexta ApS havde stiftet en varemærkeret ved ibrugtagning efter lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) § 3, stk. 1, nr. 3.

Klagenævnet lagde vægt på, at »nexta.dk« var identisk med Nexta ApS' forretningskendetegn og blev anvendt til at viderestille til en hjemmeside, hvorpå der blev udbudt tjenesteydelser af samme eller lignende art, som Nexta ApS udbød. På den baggrund fandt Klagenævnet, at der forelå en nærliggende risiko for forveksling og dermed en overtrædelse af Nexta ApS' rettigheder efter den danske markedsføringslovs § 22.

Medieforeningens anbringende om, at de havde registreret »nexta.dk« på vegne af den frivillige forening Nexta, og at denne forening derfor var den reelle registrant af domænenavnet, blev ikke taget til følge grundet manglende dokumentation.

Da Medieforeningen ikke havde godtgjort at have nogen anerkendelsesværdig interesse i at opretholde registreringen af »nexta.dk«, fandt Klagenævnet for Domænenavne, at Medieforeningen havde overtrådt god domænenavnsskik, jf. af lov nr. 164 af 26. februar 2014 (»den danske domænelov«) § 25, stk. 1, ved at nægte at overdrage registreringen af »nexta.dk« til Nexta ApS. Medieforeningen skulle derfor overføre registreringen af »nexta.dk« til Nexta ApS.

Læs hele afgørelsen her: https://www.domaeneklager.dk/sites/default/files/2021-10/2021-0163%2C%20nexta.dk_.pdf

»Yummi Gummi« var ikke forvekslelig med »Vitayummy«

Sø- og Handelsretten afsagde den 26. november 2021 dom i sagen BS-10861/2021-SHR mellem Nordic Nutriment ApS (»sagsøger«) og Skiin v/Lotte Lindgren (»sagsøgte«). Sagen vedrørte, om sagsøgtes brug af betegnelsen »Yummi Gummi« krænkede sagsøgers rettigheder efter lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) og lov nr. 426 af 3. maj 2017 (»den danske markedsføringslov«).

Sagsøger havde varemærket til varemærket »Vitayummy«, der var kosttilskud i vingummiform. Spørgsmålet i sagen var, om sagsøgtes brug af betegnelsen »Yummi Gummi«, der ligeledes var et kosttilskud i vingummiform, var forvekslelig med sagsøgers varemærke. Sagsøger fremlagde blandt andet eksempler, hvor en kunde og en influencer havde forvekslet produkterne.

Sø- og Handelsretten fandt, at varemærkerne både visuelt, fonetisk og betydningsmæssigt adskilte sig fra hinanden. I den forbindelse lagde retten til grund, at det alene var ordet »Yummy/Yummi«, som varemærkerne havde tilfælles, mens ordet »vita« og »gummi« ikke havde nogen sammenhæng. På denne baggrund fandt Sø og Handelsretten, at der ikke var risiko for forveksling mellem varemærkerne, jf. den danske varemærkelovs § 4, stk. 2, nr. 2 om identiske og lignende varemærker.

Herudover fandt Sø- og Handelsretten det heller ikke godtgjort, at produkterne var markedsmæssigt forvekslelige, idet »Vitayummi« var en række kosttilskud med vitaminer, hvorimod »Yummi Gummi« kun var ét kosttilskud samt en række andre hårprodukter. Der var tillige en prisforskel mellem produkterne. Retten fandt derfor efter en samlet vurdering, at sagsøgte hverken havde overtrådt den danske markedsføringslovs § 22 om anvendelse af kendetegn egnet til at fremkalde forveksling med andre, eller den danske markedsføringslovs § 3 om god markedsføringsskik.

Læs resumé af dommen her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-10861-2021-SHR.2330.aspx

Læs hele dommen her: https://domstol.fe1.tangora.com/media/-300011/files/BS-10861-2021-SHR_Dom.pdf

Varemærket »BLÅ UGLER« krænket af »Små Ugler« og »Blå Ugler«

Den 29. november 2021 afsagde Sø- og Handelsretten dom i sagen BS-28753/2020-SHR mellem United Drinks A/S (»United Drinks«) og Spangsberg Chokolade A/S (»Spangsberg«) mod Spritfabrikken Danmark ApS (»Spritfabrikken«). Det skulle undersøges om »Blå Ugler« var blevet en almindelig beteg-

nelse for en bestemt smag og dermed var degenereret som varemærke. Endvidere omhandlede sagen, om Spritfabrikken havde krænket United Drinks' og Spangsbergs rettigheder til varemærket »BLÅ UGLER«, ved at fremstille, markedsføre og sælge spiritusprodukter under betegnelsen »Små Ugler« og/eller »Blå Ugler«.

Spangsberg havde registreret varemærket BLÅ UGLER for konfekturevarer, og United Drinks havde registreret varemærket BLÅ UGLER for alkoholholdige drikke, efter parterne indgik et samarbejde. United Drinks solgte først alkohol med smag af bolsjet »Blå Ugler«. Spritfabrikken begyndte efterfølgende at sælge shotproduktet »Små Ugler«. De mente ikke at dette krænkede sagsøgernes varemærker, idet betegnelsen »Blå Ugler« ikke opfattedes som et varemærke, men som betegnelsen for en bestemt smag på et bolsje. Sø- og Handelsretten fandt dog ikke, at »Blå Ugler« blev opfattet som en almindelig smagsbetegnelse. Retten lagde vægt på en undersøgelse, hvor ingen af deltagerne svarede »smag« på spørgsmålet om, hvad de forbandt med »Blå Ugler«. Varemærkerne var derfor ikke degenererede og kunne ikke erklæres ugyldige efter lovbekendtgørelse nr. 88 af den 29. januar 2019 (»den danske varemærkelov«) § 28, stk. 1.

Retten fandt, at der var varelighed mellem United Drinks' og Spritfabrikkens produkter og høj grad af lighed mellem de to mærker. Der var derfor forvekslingsrisiko mellem mærkerne og dermed tale om en varemærkekrænkelse. Der var imidlertid ikke varelighed mellem Spangsbergs og Spritfabrikkens produkter, og Sø- og Handelsretten fandt ikke, at Spangsbergs varemærkeret kunne udstrækkes til at også at omfatte shotprodukter. Dog havde Spritfabrikken ved at skrive »med smag af blå ugler« og »er baseret på smagen af blå ugler« på flaskerne, gjort brug af betegnelsen »Blå Ugler« i forbindelse med sit shotprodukt. Sø- og Handelsretten fandt derfor, at der forelå en krænkelse af Spangsbergs og United Drinks' varemærker, jf. den danske varemærkelovs § 4, stk. 2, nr. 1. Desuden gav Spritfabrikkens brug af billeder med bolsjer formet som ugler, indtryk af, at der var forbindelse til Spangsbergs produkter, hvilket var illoyal markedsføring i strid med lov nr. 426 af 3. maj 2017 (»den danske markedsføringslov«) § 3 om god markedsføringsskik.

Spritfabrikken blev forbudt at fremstille, markedsføre og sælge spiritusprodukter under navnene »Små Ugler« og »Blå Ugler«. De blev også forbudt at bruge billeder mv. af blå bolsjer formet som ugler i deres markedsføring. Spritfabrikken skulle ligeledes tilbagekalde og destruere de resterende flasker »Små Ugler«. Endvidere skulle Spritfabrikken betale erstatning til United Drinks skønsmæssigt fastsat til 300.000 kr. samt et rimeligt vederlagt til Spangsberg skønsmæssigt fastsat til 100.000 kr.

Læs resumé af dommen her: https://domstol.fe1.tangora.com/Domsoversigt.16692/-BS-28753-2020-SHR.2331.aspx

Læs dommen her: https://domstol.fe1.tangora.com/media/-300011/files/BS-28753-2020-SHR_-_Dom.pdf

Retten fandt at varemærket »LEASYS« medførte en risiko for forveksling med varemærket »L'EASY«

Sø- og Handelsretten afsagde den 14. oktober 2021 kendelse i sagen BS-11438/2021-SHR mellem 3C RETAIL A/S (»3C Retail«) og Leasys Danmark, Filial af Leasys S.P.A., Italien (»Leasys Danmark«). Sagen vedrørte, om brugen af varemærket »LEASYS« medførte en forvekslingsrisiko med varemærket »L'EASY«. Sø- og Handelsretten fandt, at »LEASYS« kunne forveksles med varemærket »L'EASY«, hvorefter retten nedlagde et forbud overfor Leasys Danmarks brug af varemærket samt et påbud om sikkerhedsstillelse.

3C Retail udbyder en række varer og tjenesteydelser, herunder lån, leasing og udlejningsaftaler. 3C Retail var før registreret i CVR under navnet »L'EASY«, men skiftede i 2014 navn til 3C Retail. 3C Retail har siden 1993 haft registeret ord- og figurvaremærker til »L'EASY«. Leasys Danmark udbyder biludlejning og andre ydelser, og blev registeret i CVR i 2020. Leasys Danmark har siden 2020 haft registreret en række EU-varemærkerettigheder der indeholder »LEASYS«. Den 19. marts 2021 anlagde 3C Retail sag an ved Sø- og Handelsretten om nedlæggelse af forbud mod Leasys Danmarks brug af varemærket »LEASYS«.

Sø- og Handelsretten skulle herefter prøve om betingelserne for nedlæggelse af forbud i § 413 i lovbekendtgørelse nr. 1835 af 15. september 2021 (»den danske retsplejelov«) var opfyldt. Sø- og Handelsretten fandt indledningsvis, at det var sandsynliggjort, at 3C Retail havde rettighederne til varemærket »L'EASY«, jf. den danske retsplejelovs § 413, nr. 1. Sø- og Handelsretten bemærkede endvidere, at »L'EASY« var et velkendt varemærke, jf. § 4, stk. 2, nr. 3 i lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«). På den baggrund fandt Sø- og Handelsretten at »LEASYS« var forvekslelig med L'EASY. Retten tog herefter stilling til, om der var tale om tjenesteydelser, der lignede hinanden, og fandt at ydelserne ikke var identiske. Retten bemærkede dog, at »L'EASY« nød beskyttelse som et velkendt varemærke, hvorfor Leasys Danmarks brug af varemærket »LEASYS« kunne udgøre en utilbørlig brug af varemærket »L'EASY«, da der var tale om lignende ydelser. Leasys Danmarks adfærd nødvendiggjorde derfor, at der blev nedlagt forbud og udstedt påbud om sikkerhedsstillelse over-

for Leasys Danmarks brug af varemærket »LEASYS«, jf. den danske retsplejelovs § 413, nr. 2.

Læs resumé af kendelsen her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-11438-2021-SHR.2324.aspx

Læs hele kendelsen her: https://domstol.fe1.tangora.com/media/-300011/files/Anonymiseret_kendelse_BS-11438-2021-SHR.pdf

Go Strøm politianmeldt for ulovligt telefonsalg

Den danske Forbrugerombudsmand oplyste i en pressemeddelelse af 15. oktober 2021, at elselskabet Go Strøm er blevet politianmeldt af Forbrugerombudsmanden selv for uønsket telefonsalg efter lov nr. 1457 af 17. december 2013 (»den danske forbrugeraftalelov«) § 4 om henvendelse uden forudgående samtykke, og vildledning af forbrugere efter lov nr. 426 af 3. maj 2017 (»den danske markedsføringslov«) § 5, stk. 1 om vildledende markedsføring.

Politianmeldelsen skete på baggrund af adskillige klager fra forbrugere siden selskabets oprettelse i april 2021. Elselskabet havde blandt andet vildledt forbrugerne ved at udgive sig for at ringe fra deres nuværende elselskab og herefter tilmelde forbrugerne en elaftale fra Go Strøm uden forbrugernes viden, hvis forbrugerne oplyste CPR-nr. og kontooplysninger. Forbrugerombudsmanden vurderede, at denne vildledning var så grov, at det kunne være bedrageri, hvis forbrugerne led økonomiske tab ved overførslen til et andet elselskab.

Læs hele pressemeddelelsen her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2021/go-stroem-politianmeldt-for-ulovligt-telefonsalg/

Datingside idømt bøde for vildledning af forbrugere

Den 5. oktober 2021 offentliggjorde den danske Forbrugerombudsmand en pressemeddelelse om, at datingsiden dating.dk er blevet idømt en bøde på 50.000 kr. ved Vestre Landsret for at have overtrådt forbuddet mod vildledning i lov nr. 426 af 3. maj 2017 (»den danske markedsføringslov«) § 5, stk. 1 sammenholdt med § 8 og § 6, stk. 1 sammenholdt med § 8.

Dating.dk havde vildledt om prisen og bindingsperioden for datingabonnementet »+PlusProfil« ved at markedsføre et tilbud på profilen på kun én krone. På bannere på dating.dk stod der for eksempel: »[…] Så find kærligheden på dating.dk for kun 1 kr.« Det fremgik ikke af bannerne, at man ved benyttelse af tilbuddet blev tilmeldt et løbende betalingsabonnement. På den betalingsside, forbrugerne blev ledt hen til, når de klikkede på bannerne, stod det med småt, at der gjaldt en bindingsperiode på tre måneder, og at den samlede mindstepris var 299 kr.

Vestre Landsret fandt, at bannerne og betalingssiden var vildledende og i strid med den danske markedsføringslov. Det kunne ikke føre til et andet resultat, at forbrugeren skulle afkrydse, at vedkommende accepterede betingelser om et løbende abonnement, i forbindelse med udfyldelse af oplysninger om betalingskort.

Ved Byretten i Viborg var dating.dk blevet idømt en bøde på 100.000 kr. Vestre Landsret nedsatte den til 50.000 kr. henset til sagsbehandlingstiden.

Forbrugerombudsmanden udtalte, at dommen slår fast, at det er vildledende, hvis det ikke fremgår tydeligt, at der er en bindingsperiode på et abonnement, selvom forbrugerne accepterer de generelle betingelser for abonnementet. Forbrugere er således ikke bundet af et betalingsabonnement, hvis de ikke har fået tydelige oplysninger om abonnementet.

Læs hele pressemeddelelsen her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2021/datingside-idoemt-boede-for-vildledning-af-forbrugere/

To elselskaber politianmeldt for ulovligt telefonsalg

Den danske Forbrugerombudsmand politianmeldte den 15. november elselskaberne Grow Energy og Elektron for overtrædelser af lov nr. 1457 af 17. december 2013 (»den danske forbrugeraftalelov«) og lov nr. 426 af 3. marts 2017 (»den danske markedsføringslov«) ved uønsket telefonsalg og vildledning af forbrugerne. Virksomheden BigInGreenland blev endvidere politianmeldt for medvirken til Grow Energys telefonsalg.

Grow Energy blev politianmeldt for at have ringet til 12 forbrugere uden forudgående samtykke, jf. den danske forbrugeraftalelovs § 4, stk. 1 om forbuddet mod telefonsalg. Grow Energy blev endvidere anmeldt for at have vildledt 8 af de 12 forbrugere ved at udgive sig for at være forbrugernes elselskaber og give udtryk for, at forbrugerne kunne spare penge ved at skifte elselskab til Grow Energy, jf. §§ 5 og 6 i den danske markedsføringslov om forbuddet mod vildledning af forbrugere. BigInGreenland blev politianmeldt for at have medvirket til 9 ud af de 12 opkald.

Elektron blev politianmeldt for at have ringet til 12 forbrugere uden forudgående samtykke, jf. den danske forbrugeraftalelovs § 4, stk. 1 om forbuddet mod telefonsalg. Elektron blev også politianmeldt for at have vildledt tre af forbrugerne samt anvendt aggressiv markedsføringsstrategi overfor to af forbrugerne ved urigtigt at have oplyst, at forbrugerne havde vundet en konkurrence jf. §§ 5-6 og 9 i den danske markedsføringslov om forbuddet mod vildledning af forbrugere. Elektron har tilkendegivet, at elselskabet ønsker at betale en bøde, hvorefter sagen kan afsluttes.

Læs hele pressemeddelelsen her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/

pressemeddelelser/2021/to-elselskaber-politianmeldt-for-ulovligt-telefonsalg/

Diskotek fik bøde for at rette markedsføring med alkohol mod unge

Den 4. oktober 2021 meddelte den danske Forbrugerombudsmand, at et diskotek havde markedsført tre arrangementer med omtale af alkohol over for unge på sin Facebook-side. Diskoteket blev politianmeldt og accepterede en bøde på 30.000 kr.

Ifølge lov nr. 426 af 3. maj 2017 (»den danske markedsføringslov«) § 11, stk. 2 er det forbudt at rette markedsføring på nettet, som indeholder omtale, billeder af eller henvisninger til alkohol, mod børn og unge under 18 år.

Diskotekets markedsføring af arrangementerne indeholdt blandt andet et billede af en mand med en flaske vodka i hånden, et billede med et skilt med teksten »GREY GOOSE WORLD'S BEST TASTING VODKA« og et billede med flere flasker spiritus på bordene. Facebook-opslagene var markeret med »16+«, hvorfor Forbrugerombudsmanden vurderede, at markedsføringen også rettede sig mod unge mellem 16 og 17 år. På den baggrund og med vægt på, at opslagene indeholdt billeder og omtale af alkohol, vurderede Forbrugerombudsmanden, at opslagene overtrådte den danske markedsføringslovs § 11, stk. 2.

Læs om sagen her: https://www.forbrugerombudsmanden.dk/find-sager/markedsfoeringsloven/sager-efter-markedsfoeringsloven/diskotek-fik-boede-for-at-rette-markedsfoering-med-alkohol-mod-unge/

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

Bird & Bird

Monique Wadsted og Leonard Garg

PMD T 11815-20 2022-01-27
Konkurrerande parkeringsbolag gjorde intrång i Parksters databas

PMÖD B 5557-21 2021-12-21
Brott mot avkodningslagen och intrång i den s.k signalrätten

PMÖD PMÖ 10189-21, 2021-10-06
Inget intrång i upphovsrätt för programvara

Patent- och marknadsdomstolen dom 27 januari 2022

Mål nr: PMT 11815-20 Intrång i databas - dataskrapning var intrång i databas

Patent- och marknadsdomstolen meddelade den 27 januari 2022 dom i mål PMT 11815-20 mellan Parkster AB (Parkster) och Parkamo GmbH (Parkamo) samt Eplik 202001 AB (Eplik).

Svarandebolagen förbjöds vid vite att göra fortsatta utdrag och tillgängliggöranden av kärandens databas och dömdes att solidariskt utge skälig ersättning och ersättning för ytterligare skada om totalt 4 500 000 kr.

Parkster tillhandahöll en app i vilken användaren kan hitta tillgängliga parkeringsplatser och administrera sin parkering. All information i appen hämtade Parkster från sin databas. Informationen hade samlats in under många ur från olika fastighetsägare med vilka Parkster hade avtal. Det uppdagades att ett antal konton från ett fåtal IP-adresser hade registrerats och använts för att hämta information om bl.a. taxor och zoner från Parksters app. Kontona kunde knytas till företrädare för svarandebolagen. Svarandebolagen lanserade en egen app med funktioner liknande Parksters app.

Domstolen konstaterade att svarandebolagen måste ha berett sig tillgång till informationen genom s.k. dataskrapning. Domstolen fann att Parksters databas både var ett resultat av en väsentlig investering genom anskaffning, granskning och presentation av innehållet i Parksters databas, och att databasen innehöll en sammanställning av ett stort antal uppgifter. Domstolen godtog inte svarandebolagens invändningen om att inhämtningen skett genom egen s.k. crowd-sourcing utan fann att svarandebolagen genom dataskrapningen och lanseringen gjort intrång i Parksters ensamrätt enligt 49 § i upphovsrättslagen.

Patent- och marknadsöverdomstolen dom meddelad 21 december 2021

Mål nr: B 5557-21 Brott mot avkodningslagen och intrång i den s.k signalrätten

Flera personer dömdes till fängelsestraff, näringsförbud och sammanlagt drygt 100 miljoner kronor i skälig ersättning enligt lagen om avkodningsutrustning och upphovsrättslagen för bl a drift från Sverige av en cardsharing-verksamhet och

iptv-verksamhet. Cardsharing-verksamheten bestod av förvärv, försäljning, distribution, installation och underhåll av avkodningsutrustning i syfte att göra tv-sändningar från Canal Digital, Com Hem och NENT tillgängliga i tolkningsbar form för runt 6.000 användare. IPTV-verksamheten bestod av återutsändning an TV-sändningar från NENT, C More och Discovery.

Patent- och marknadsöverdomstolen beslut meddelat 6 november 2021

Mål nr: PMÖ 10189-21

Intrångsundersökning - *Inget intrång i upphovsrätt för programvara*

Patent- och marknadsöverdomstolen avslog ansökan om intrångsundersökning hos ett IT-konsultbolag på grund av bristande bevis. Domstolen konstaterade att sökanden inte visat att det *skäligen kunde antas* att svaranden gjort sig skyldig till upphovsrättsintrång vilket är en förutsättning för att intrångsundersökning ska beviljas. Domstolen påpekade att beviskravet omfattar såväl *förekomsten av en rättighet* som att det vidtagits en *intrångsgörande handling*. Bedömningen ska göras översiktligt.

Intrångsundersökningen avsåg en programvara och domstolen konstaterade att den inklusive källkoden åtnjöt upphovsrätt. IT-konsultbolaget hade i uppdrag att utveckla programvaran för den som ansökte om intrångsundersökning. Det fanns enligt domstolen inte tillräckliga bevis för att IT-konsultbolagets införande av upphovsrättsnotiser och anpassningar av hårdvara var tillräckligt för att det kunde skäligen befaras försök till eller genomfört intrång. Inte heller IT-konsultbolagets intäkter gav sådant stöd. Därför meddelades ingen intrångsundersökning.

Monique Wadsted är partner Bird & Birds Intellectual Property-grupp och leder sektorgruppen Swedish Media, Entertainment & Sports i Stockholm. Med mer än 20 års erfarenhet i branschen har hon genom åren jobbat med flera stora uppmärksammade rättsfall.

Leonard Garg arbetar vid sidan av sina studier som trainee i Bird & Bird's Intellectual Property och Dispute Resolution grupp.


simonsen vogtwiig

Hedda Baumann Heier og
Emile Schjønsby-Nolet

Utredning av vederlagsrett til artister og plateselskap

Professor Ole-Andreas Rognstad ved Universitetet i Oslo har på vegne av Kulturdepartementet utredet betydningen av EU-domstolens avgjørelse i C-265/19 (RAAP-dommen) for norsk rett. Avgjørelsen gjelder tolkningen av artikkel 8 (2) i utleie- og utlånsdirektivet (2006/115/EF) som er en bestemmelse (tvangslisens) som gir utøvende kunstnere og produsenter rett til vederlag når verk brukes offentlig, f.eks. som bakgrunnsmusikk i offentlige rom. Avgjørelsen indikerer at også rettighetshavere fra land utenfor EØS-området som ikke har påtatt seg tilsvarende forpliktelser, har krav på vederlag. I sin utredning konkluderer problematiserer professor Rognstad EU-domstolens avgjørelse i en EØS-kontekst og konkluderer med at avgjørelsen ikke kan gis betydning da den vil gripe inn i EFTA-statenes eksterne traktatkompetanse. Utredningen tar til orde for en tolkning som fører til at Norge kan nekte å gi vederlagsrett til rettighetshavere fra land som ikke har tilsluttet seg Romakonvensjonen.

Utredningen kan leses her

Sak om sitatrett er sluppet inn til behandling i Høyesterett

Den 29. november 2021 kunngjorde Høyesteretts ankeutvalg at de tillater at anken i saken mellom Advokatfirmaet Rognstad AS og Verdens Gang AS fremmes for behandling i Høyesterett. Saken gjelder bruk av fotografier fra advokatfirmaets nettside i forbindelse med en nyhetsreportasje i avisen VG. Høyesterett vil kun behandle rettsanvendelsen i spørsmålet om Verdens Gang AS har hjemmel i åndsverksloven («åvl») §§ 29 (sitatregelen) eller 36 (2) (journalistunntaket) til å gjengi fotografiene.

Høyesterett avsier sin dom i varemerkesaken om Stortorvet Gjæstgiveri

14. desember 2021 avsa Høyesterett sin avgjørelse i Stortorvet Gjæstgiveri-saken. Restauranten «Stortorvets Gjæstgiveri» i er et kjent spisested i Oslo med mer eller mindre kontinuerlig drift over flere hundre år. Restauranten er i dag drevet av Olav Thon. I 2015 åpnet Madriku AS «Stortorvet Gjestgiveri» i Hamar.

I 2018 søkte Thon om varemerkebeskyttelse for sin restaurants logo som et kombinert merke. Varemerkesøknaden gikk gjennom senere samme år. Thon tok deretter ut søksmål mot Madriku AS. Saken verserte i de lavere domstolene fra 2019 til 2021 før saken ble anket til Høyesterett. Det sentrale spørsmålet for Høyesterett var om Madriku sin bruk av navnet Stortorvet Gjestgiveri var en krenkelse av varemerketten, eller eventuelt markedsføringsloven regler om etterlikningsvern og forbud mot handlinger i strid med god forretningsskikk i §§ 30 og 25.

Høyesterett vurderer først om registeringen var i samsvar med registeringsvilkårene i varemerkeloven (vml) § 14. Det sentral spørsmålet var om merket hadde nødvendig særpreg. Høyestrett konkluderte med at navnet «Stortorvets Gjæstgiveri» isolert sett var beskrivende og uten særpreg. «Gjæstgiveri» var kun ansett som et synonym for serveringssted, og var derfor beskrivende for tjenestens art, mens «Stortorvet» angir en geografisk plassering. Det neste spørsmålet var om merket likevel kunne vernes i lys av dets grafiske utforming. Retten uttaler at vurderingen er om den utformingen av merket er i stand til å avlede omsetningskretsens oppmerksomhet fra ordenes meningsinnhold. For Stortorvet Gjæstgiveri var heller ikke dette tilfellet.

Som utgangspunkt kunne kjennetegnet derfor ikke registreres. Det neste spørsmålet var om merket likevel hadde oppnådd beskyttelse gjennom innarbeidelse jf. vml § 3 tredje ledd. Vurderingstemaet var om Stortorvet Gjæstgiveri hadde fått en sekundærbetydning som overdøvet den opprinnelige språklige betydningen. Stortorvet Gjæstgiveri har en lang historie i Oslo. Høyesterett mente at den langvarige eksklusive bruken av merket talte for at innarbeidelse blant omsetningskretsen i Oslo. Likevel var innarbeidelsen ikke tilstrekkelig på landsbasis. Det kunne derfor heller ikke sies å foreligge en krenkelse av et innarbeidet varemerke.

Avslutningsvis vurderte Høyesterett forholdet etter markedsføringsloven §§ 25 og 30. En kuriositet er at Høyesterett samme dag hadde avsagt Bank Norwegian-dommen (HR-2021-2479) som også gjelder forholdet mellom varemerketten og markedsføringslovens bestemmelser. I lys av Bank Norwegian-dommen, viser Høyesterett til at det ikke det ikke er nødvendig å ta stilling til om det var tale om etterligning. Restaurantene var uansett i to forskjellige byer, og det var ikke noen elementer i Hamar-restauranten som kunne

indikere en forbindelse til restauranten i Oslo. Det var heller ingen andre holdepunkter for at restauranten på Hamar hadde hatt intensjoner om å snylte på kjennetegnet til Thon.

Resultatet ble at bruken av navnet «Stortorvet Gjestgiveri» på en restaurant i Hamar ikke utgjorde en krenkelse av varemerket til «Stortorvets Gjæstgiveri» i Oslo.

Dommen med saksnummer HR-2021-2480-A kan leses i sin helhet i Lovdatas database.

Oslo tingrett: tolkning av avtale om rettigheter til programvare for hoteller

Den 10. oktober 2021 avsa Oslo tingrett sin avgjørelse i en sak mellom hotellkjeden Baltazar Apartments Tjuvholmen AS (Baltazar) og IT-selskapet Netron AS (Netron).

I 2018 inngikk Netron en avtale med Baltazar der Netron stod for utvikling av et SMS-låssystem, bookingløsning og nettside for Baltazar sitt leilighetshotell i Oslo sentrum. Målet var å lage en «self service»-løsning som skulle integreres opp mot nettsidene booking.com og hotels.com. Baltazar hadde, i dialog med Netron, planer for kommersialisering av softwareløsningen ved å tilby løsningen som hyllevare til andre hoteller. Høsten 2019 viste seg at Netron utviklet en tilsvarende løsning for Wex Hotels AS. Da det i tillegg ble oppdaget en rekke mangler ved leveransen av løsningen, valgte Baltazar å be om å få utlevert kildekoden til løsningen til en ny leverandør. Baltazar fremmet krav om prisavslag noen måneder senere.

Det springende punkt i saken var om Natron hadde overført opphavsretten, eller eventuelt en eksklusiv bruksrett, til programvaren som var utviklet for Baltazar.

Dette måtte avgjøres på bakgrunn av en tolkning av avtalen mellom partene der rettigheter var regulert på følgende måte: «*[p]artene er enige om at de leveranser som Netron AS gjør i henhold til denne avtale er kundens eiendom. Egenutviklede moduler og halvfabrikata som Netron benytter i prosjektet er Netron sin eiendom.*»

Tingretten konstaterte kort at Netron sine ansatte sitt arbeid var overdratt til Netron i kraft av å være arbeidsgiver jf. åndsverksloven § 71. For spørsmålet om Natron hadde overført de økonomiske rettighetene til programvaren til Baltazar, tok tingretten først utgangspunkt i forarbeidene, Prop.104 L (2016–2017), sine generelle drøftelser av spesialitetsprinsippet på side 228. Spesialitetsprinsippet er prinsippet om at uklare avtaler skal tolkes i opphaverens favør. Av denne mer generelle drøftelsen utledet tingretten at tolkningsprinsippet også gjelder for videreoverdragelser, men at «*ved videreoverdragelse fra et selskap som har erverver opphavsretten til åndsverket / dataprogrammet fra sine arbeidstakere jf. åndsverkloven § 71, er det liten grunn til å tillegge prinsippet stor betydning*».

En slik forståelse er ikke helt intuitiv sett opp mot resten av forarbeidene, Prop.104 L (2016–2017). I forarbeidene side 334 fremgår det blant annet at «*der de samme hensyn som begrunner prinsippet for overdragelser fra opprinnelig opphaver gjør seg gjeldende, kan det også gjelde i senere ledd*». Det sentrale etter forarbeidene synes altså å være hvorvidt de samme hensyn (herunder skjevhet i forhandlingsstyrke) gjør seg gjeldende også ved videreoverdragelsen. I den konkrete saken fremsto partene som ganske likeverdige med tanke på forhandlingsstyrke, så tingrettens beslutning om å ikke tillegge spesialitetsprinsippet særlig vekt fremstår likevel riktig, selv om det nok kunne vært begrunnet noe annerledes.

For spørsmålet om overdragelse, slår tingretten fast at avtaleteksten er uklar. I fravær av klar regulering, ser tingretten hen til det den mener er bransjepraksis, nemlig at leverandøren skal beholde opphavsretten for programvare som leveres til kunden (jf. SSA-T punkt 10.3.1). Selv om den alminnelige uklarhetsregelen i avtaleretten tilsier at den som har utformet avtalen (her Netron) skal bære ansvaret for uklarheter, mente tingretten at dette ikke kunne gjelde i den foreliggende saken ettersom Netrons forståelse var i tråd med bransjestandarden. Baltazar hadde ikke sannsynliggjort overføringen av hele opphavsretten eller tildeling av en eksklusiv bruksrett.

Retten avviser videre krav etter markedsføringsloven (§§ 30 og 25) og slår fast at det ikke er grunnlag for å imøtekomme et berikelseskrav/vinningsavståelseskrav. Krav om prisavslag var fremmet for etter at reklamasjonsfristen var gått ut. Netron vant dermed saken fullt ut.

Avgjørelsen med saksnummer TOSL-2020-176499 kan leses i Lovdatas database. Avgjørelsen er rettskraftig.

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

Wikström & PARTNERS
Christina Wikström

Nya it-avtalsvillkor för offentlig sektor

För att underlätta arbetet med upprättande av it-avtal används standardavtalsvillkor för olika it-tjänster. Större organisationer inom privat och offentlig sektor har upprättat egna it-avtalsvillkor och leverantörerna har i stor omfattning förordat användandet av allmänna villkor på från TechSverige (f.d. IT&Telekomföretagen). Avtalsvillkoren från TechSverige som finns för olika it-tjänster med SLA-bilaga och personuppgiftsbiträdesavtal har under de senaste 20 åren använts flitigt i olika sammanhang, trots att regleringarna i avtalsvillkoren är leverantörsvänliga. Inom offentlig sektor har det saknats anpassade it-avtalsvillkor, varför TechSveriges allmänna villkor många gånger nyttjas tillsammans med ett tillägg för att skapa mer balanserade avtalsregleringar.

Enligt förordning (1998:796) om statlig inköpssamordning, ska det finnas ramavtal eller andra gemensamma avtal som effektiviserar upphandlingar för varor och tjänster som myndigheterna upphandlar ofta, i stor omfattning eller som uppgår till stora värden. Samordning av dessa upphandlingar sker genom Statens inköpscentral vid Kammarkollegiet, vilket resulterar i ramavtal som myndigheterna ska använda, om myndigheten inte finner att en annan form av avtal sammantaget är bättre. I de fall en myndighets behov inte kan tillgodoses genom avrop från Statens inköpscentrals ramavtal behöver myndigheten på egen hand upprätta avtalsdokument som ska användas i upphandlingen, alternativt förlita sig på avtalsvillkor som leverantören föreslår.

Det är mot denna bakgrund som eSam, ett samverkansprogram för myndigheter, tagit fram allmänna villkor för en rad olika it-tjänster, d.v.s. för att säkerställa att det finns ett kundvänligt och myndighetsanpassat it-avtalsvillkor i de fall Statens inköpscentrals ramavtal eller andra gemensamt upphandlade ramavtal inte kan användas. eSam är ett medlemsdrivet program mellan 35 myndigheter som samverkar kring framtagande av tillgängliga och rättssäkra digitala lösningar.

It-avtalsarbetet inom eSam har fram till idag resulterat i följande fem it-avtalsvillkor;

- eSam Allmänna villkor för it-konsulttjänster (vers. 200623)
- eSam Allmänna villkor för it-drifttjänster (vers. 210121)
- eSam Allmänna villkor för it-supporttjänster (vers. 210312)
- eSam Allmänna villkor för it-projekt (vers. 211201)
- eSam Allmänna villkor för agila it-projekt (vers. 211201)

Till respektive avtalsvillkor har en kommentar tagits fram för att underlätta användandet och belysa avtalsvillkorens centrala regleringar. Avtalsvillkoren är framtagna i nära samarbete med eSams medlemmar och kan ses som en praktisk tillämpning av eSams vägledningar på området utkontraktering. Avtalsvillkoren är framtagna för att användas tillsammans med ett huvudavtalsdokument, exempelvis ett ramavtal eller ett fristående it-avtal. It-avtalsvillkoren har stora likheter i de allmänjuridiska regleringarna vilket möjliggör att regleringarna kan användas tillsammans i samma avtalsstruktur.

På it-avtalsområdet har det framtagits två vägledningar, ”It-avtal – en vägledning om it-tjänsternas avtal” och ”Programvarulicensiering – en vägledning om licensavtal”. It-avtalsvillkoren och vägledningarna finns publicerat på eSams webbplats; *https://www.esamverka.se/stod-och-vagledningar.html.*

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


SELMER

Ståle L. Hagen og
Vemund Sande

Ny standardavtale fra DFØ: SSA-lille sky

Tidligere i år publiserte det norske Direktoratet for forvaltning og økonomistyring (DFØ) sin nyeste standardavtale; «Den lille skyavtalen» (SSA-lille sky). Med sine 25 sider er denne avtalen en litt forenklet versjon av «Statens standardavtale for tilrettelegging, innføring og forvaltning av skytjenester levert på standardvilkår» (SSA-sky) som er på hele 46 sider. SSA-sky har vi tidligere skrevet om i Lov & Data, og det kan legges til at også SSA-lille sky har flere forslag til reguleringer i bilagsmalen, slik at det reelle innholdet er enda litt mer omfattende enn de 25 sidene med generelle kontraktbestemmelser.

Bruksområde for SSA-lille sky er av DFØ beskrevet som anskaffelser av en eller flere skytjenester som skal kunne tas i bruk uten særlig bistand fra leverandøren. Ambisjonsnivået synes å være at også skytjenesteleverandørene selv skal kunne være part i avtalen, i motsetning til det som har vært utgangspunkt for SSA-SKY og SSA-L («Avtale om løpende tjenestekjøp over internett»), som begge legger opp til at en tredjepart (tjenesteintegrator) inngår avtalen med kunden.

SSA-lille sky opererer med begrepene «Skytjenester» og «Tilleggstjenester», hvor førstnevnte typisk vil være en eller flere standardiserte tjenesteleveranser fra en annen enn leverandøren som inngår avtalen med kunden, og sistnevnte vil være tjenestene leverandøren selv skal levere. Tilleggstjenestene er eksemplifisert som integrasjoner, tilpasninger og datakonvertering. Når tjenestene skal beskrives i kontrakten er det viktig å huske veiledningen fra DFØ om at SSA-lille sky skal benyttes når det ikke vil være behov for veldig mye støtte fra leverandøren for at kunden skal kunne ta i bruk skytjenestene.

Det grunnleggende konseptet i SSA-lille sky er at leverandøren, som kan være en tjenesteintegrator eller skytjenesteleverandøren selv, først skal implementere og deretter levere skytjenester fra en eller flere leverandører til kunden. For å ta det siste først så stiller vi oss tvilende til at skytjenesteleverandørene vil akseptere SSA-lille sky som avtale mellom seg og kunden, selv om de får lov til å inkludere sine egne standardvilkår som vedlegg til avtalen. Vi vil nok derfor ende opp i samme situasjon som med SSA-sky og SSA-L, slik at en tredjepart som er villig til å akseptere ansvar og risiko skytjenesteleverandørene selv ikke godtar blir stående som kundens avtalepart og leverandør. Denne leverandøren vil normalt ikke få full ryggdekning fra skytjenesteleverandøren for garantiene (bl a relatert til bruksrett), ansvaret (bl a for funksjonalitet) eller risikoen (bl a ved mislighold) som ligger i forskjellene mellom SSA-lille sky og skytjenesteleverandørenes standardvilkår, og vil derfor ende opp som en form for selger av forsikring mellom den reelle leverandøren av tjenestene og kunden. Vi får håpe og tro at leverandøren evner å ta seg betalt for dette ansvaret og risikoen, og det blir jo da interessant å stille spørsmål om denne merkostnaden står i forhold til merverdien kunden oppnår med denne strukturen.

Vi skal ikke gjennomgå alle utfordringene vi ser ved å bruke SSA-lille sky, men vi konstaterer at det fremdeles ligger en del uklarhet i forholdet mellom den samlede leveransen som inngår i avtalen og spesialreguleringene som gjelder skytjenestene. Det fremstår for oss som i beste fall uklart hvor langt avtalen går i å frita leverandøren fra ansvaret og risikoen for disse skytjenestene. Det som i alle fall er sikkert, er at ansvaret og risikoen vil være mer omfattende ved bruk av SSA-lille sky enn om skytjenesteleverandørenes standardvilkår legges til grunn alene.

Det kanskje største og mest praktiske avviket mellom SSA-lille sky og skytjenesteleverandørenes standardvilkår er, i likhet med SSA-sky og SSA-L, ansvaret for å levere spesifisert funksjonalitet. SSA avtalene legger til grunn at kundens krav og leverandørens svar på kravene og løsningen spesifiseres i bilag 1 og 2 i avtalen. Disse bilagene inneholder normalt omfattende krav til skytjenestenes funksjonalitet, som er noe skytjenesteleverandørene så godt som aldri aksepterer å inkludere i sine avtaler. Resultatet blir følgelig at leverandøren som signerer SSA'en med kunden bærer ansvaret og risikoen for i hvilken

grad disse funksjonelle kravene oppfylles i de aktuelle skytjenestene.

På samme måte som for SSA-sky, og enda mer for SSA-lille sky som skal benyttes når leverandørens innsats er begrenset, mener vi en mer hensiktsmessig tilnærming hadde vært «bottom up». Med det mener vi at skytjenestene burde leveres på sine standardvilkår, uten innblanding av reguleringer i SSA-lille sky, og at det leverandøren skal bidra med er regulert positivt ved at det konkret spesifiseres i avtalen. Dette ville gitt en langt enklere og mer brukervennlig avtale, og leverandørens ansvar og risiko ville vært tydeligere og bedre avklart. Det er sjelden en god idé å be om at en leverandør tar ansvar og risiko for forhold han selv ikke kontrollerer, men det er det disse SSA'ene legger til grunn.

Vi tillater oss å oppsummere på samme måte som vi gjorde i forbindelse med SSA-sky. Det er positive og negative sider ved å velge standardiserte skytjenester, som for eksempel stordriftsfordeler, effektivitet, fleksibilitet, stabilitet og standardisering. Men at noe er standard betyr også at hver enkelt kunde ikke kan få det «på sin måte» og heller ikke på sine egne betingelser. Det er dessverre ikke en god løsning å forsøke å plassere en tredjepart imellom for å kompensere for disse avvikene. Dette er den mest grunnleggende årsaken til at vi mener SSA-lille sky dessverre ikke fremstår som en hensiktsmessig kontrakt.

Ståle L. Hagen er partner og Vemund Sande er fast advokat i advokatfirmaet Selmer.

Gorrissen Federspiel

Tue Goldschmieding

Europarådet har vedtaget holdning til Digital Operational Resilience Act (DORA) og Markets in Crypto-Assets (MiCA)

Den 24. november 2021 vedtog Europarådet sin holdning til Digital Operational Resilience Act (DORA) og Markets in Crypto-Assets (MiCA), der begge udspringer af EU-Kommissionens digitale strategi.

DORA-forslaget har til formål at styrke den finansielle sektors digitale operationelle modstandskraft i lyset af den igangværende digitalisering af finansielle tjenesteydelser. DORA vil pålægge finansielle virksomheder en række krav om bl.a. risikostyring inden for informations- og kommunikationsteknologi (IKT), test af digital operationel modstandsdygtighed og udveksling af oplysninger om cybertrusler og sårbarheder.

MiCA-forslaget søger at støtte innovation og fair konkurrence ved at skabe en ramme til udstedelse og levering af tjenester relateret til kryptoaktiver, samt at sikre et højt niveau af forbruger- og investorbeskyttelse.

Med vedtagelsen er Europarådet klar til at indlede trepartsforhandlingerne med Europa-Parlamentet. Når der er nået politisk enighed, vil begge institutioner formelt vedtage både DORA og MiCA, hvilket forventes at ske i løbet af efteråret 2022.

https://www.consilium.europa.eu/media/53104/st14066-en21.pdf

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

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

Karnov Lovkommentarer, sømløst integrert i Lovdata Pro.

Skrevet av landets fremste jurister og kvalitetssikret av våre 25 fagredaktører.

KOMMENTARENE

Kommentarene er utstyrt med interne og eksterne henvisninger og med tilrettelegging for rask navigering i loven og til andre rettskilder – herunder internasjonale, og spesielt EU/EØS-relevante, kilder.

Du får også tilgang til den danske EU-Karnoven som inneholder kommentarer til TEU, TEUF i tillegg til noter til utvalgte direktiver og forordninger. Du finner også domsanalyser og utvalgte EU-dommer i EU-Karnoven.

MER INFORMASJON

Har du spørsmål eller ønsker å vite mer, vennligst ta kontakt med oss.

www.karnovgroup.no

KARNOV GROUP

BESTILL I DAG

Er du Lovdatakunde kan du bestille direkte gjennom Lovdata Pro.

https://pro.lovdata.no

LOVDATA PRO

Produksjon: 07 Media AS