Lov & Data

Nr. 146
Juni 2021
Nr. 2/2021

Innhold






Lov&Data

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

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

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

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

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

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

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

Leder

Ny forordning om AI

EU-kommissionen fremlagde den 21. april 2021 et forslag til forordning, der skal regulere kunstig intelligens. Forslaget til forordningen er resultatet af et arbejde, der har været længe undervejs. Tilbage i februar 2020 fremlagde EU-kommissionen en såkaldt hvidbog om en europæisk tilgang til kunstig intelligens baseret på ekspertise og tillid. Udkastet til forordningen bygger videre på disse tanker. Forslaget ligger nu åbent for *feedback* indtil den 7. juli 2021 forud for EU-Kommissionens vedtagelse og senere fremlæggelse for Europa-Parlamentet og Rådet.

EU-kommissionen udtrykker med forslaget store ambitioner om at blive en global leder via fokus på de store potentielle risici, hensyn til sikkerhed og fundamentale rettigheder. Det er derfor i sig selv også illustrativt, at EU-kommissionen ønsker at skabe direkte harmonisering via en forordning frem for et – for medlemslandene - mere fleksibelt instrument i form af et direktiv.

Hvis vi træder et skridt tilbage, så er det væsentligt først at gøre sig klart, at alene definitionen af kunstig intelligens under forordningen bliver central for rækkevidden i lyset af de teknologiske stormskridt, der sker inden for kunstig intelligens. Definitionen angiver software udviklet via teknikker og metoder nærmere oplistet, disse fremgår af Annex I, og som for mål udviklet af mennesker kan generere resultater såsom indhold, forudsigelser, anbefalinger eller beslutninger, der påvirker miljøet de indgår i. De oplistede teknikker i Annex I omfatter:

»(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods.«

Det er svært at nå anden konklusion end at forordningen vil få betydning for voldsomt mange typer af teknologi. Der virker dermed til at være taget hånd om at sikre fremtidig teknologi-udvikling, hvorvidt det vil være forudsigeligt, om en teknologi falder indenfor virker også klart, det

vil det formentlig. Den balanceakt minder om andre reguleringsinitiativer fra EU i disse år, hvor ønsket er fuldstændig sikkerhed for, at forhold i fremtiden vil blive omfattet.

Tilgangen til reguleringen af kunstig intelligens flugter også i øvrigt med det, vi i forvejen kender fra nyere IT/tech og data regulering fra EU fx persondataforordningen og netværks- og sikkerhedsdirektivet. Nøgleordene er proportionalitet og risiko-baseret tilgang.

For kunstig intelligens indebærer det et klassificeringssystem, der udgør udgangspunktet for reguleringen af den pågældende type af omfattet software. Kategorierne er uacceptabel risici, høj risici, begrænsede risici og minimal risici.

Uacceptabel risici er en kategori, der består i et decideret forbud. Artikel 5 oplister direkte de omfattede systemer, der er genstand for forbuddet. Det drejer sig som systemer, som:

- bruger teknikker rettet mod underbevidstheden til at manipulere mennesker;
- udnytter information om mennesker til at målrette mod deres sårbarheder og forvride deres adfærd væsentligt, hver hvor det sandsynligvis vil forårsage fysisk og psykisk skade;
- offentlige myndigheder enten selv eller via andre kan bruge til evaluere eller klassificere troværdighed hos borgere baseret på deres sociale adfærd eller karakteristika, populært kaldet »social score cards« eller lignende, med henblik på negativ behandling af individet eller en gruppe individet tilhører, hvis den negative behandling er urelateret til måden hvorpå dataene oprindeligt var indsamlet;
- bruger realtids biometrisk godkendelse i offentlige rum til retshåndhævelsesformål det vil blandt andet sige ansigtsgenkendelse, men der er væsentlige undtagelser netop her, der tillader brug til kriminalitetsforebyggelse og national sikkerhed.

Det er tydeligt for alene denne kategori, hvordan afgræsningen af systemer bliver interessant at følge i takt med at private samfundsaktører og offentlige myndigheder vil søge at benytte fremskridt og nye muligheder.

Den største og mest komplekse regulering sker af systemer kategoriseret som værende af høj risiko. Disse systemer er underlagt forordningen artikel 6 – 51 specifikt. Optagelsen af systemer i denne kategori har en mere fleksibel natur end for uacceptable systemer og software. Systemer omfattet fremgår af et Annex III til forordningen, og der er indsat en klar hjemmel allerede i Article 7, der tillader revidering af Annex III. Som påpeget ovenfor er det ikke svært at udlede, at det har været væsentligt at fremtidssikre muligheden for at omfatte nye teknologier.

Konkret fremgår det af Annex III, at omfattede områder er: Biometrisk identifikation, styring af kritisk infrastruktur, uddannelse, beskæftigelse, essentielle ydelser såsom velfærdsydelser, kreditvurdering, alarmtjenester, politi- og anklagemyndighedsarbejde, migration/asyl og domstoles retsanvendelse.

Forpligtigelserne rettet mod disse er mange og fortjener selvstændig belysning, det kan her nævnes, at det inkluderer pligter vedrørende data governance, teknisk dokumentation, journaliseringskrav, gennemsigtighed, menneskeligt tilsyn, rigtighed, robusthed og informationssikkerhed.

Ligesom med systemerne som genstand for regulering så søger forordningen også at sikre en bred skare vil være omfattet som ansvarlig for forpligtigelserne. Under fællestitlen operatører kan alle blive omfattet lige fra leverandører, importører, distributører og til brugerne – forstået som enhver naturlig eller juridisk person der bruger systemets funktionalitet til ikke-private formål.

Den nærmere regulering af andre områder såsom fx geografisk udstrækning og specifikke undtagende systemer er ikke uinteressant, men vil for den erfarne praktiker næppe give anledning til større overraskelser.

Sanktionshjemlen er ligeledes på line med eksisterende regulering i GDPR, men overliggeren er hævet for artikel 5 altså systemerne klassificeret som havende en uacceptabel risici, sådan det maksimale bødeniveau nu kan udgøre 6 % af global omsætning eller EUR 30 mio. Og ligeledes ligesom i GDPR er hensigten at skabe et governance setup, der bliver ledet af et »European Artificial Intelligence Board«, som skal have til rolle at føre tilsyn og holde overblik over håndhævelsen i de enkelte medlemslandes nationale myndighed.

Samlet set står vi med et meget spændende udkast til forordning, der indeholder en række nybrud alene i kraft af at genstanden for regulering ikke nemt lader sig afgrænse, men hvor metoderne anvendt til at søge at skabe orden i reguleringen hviler på principper, vi efterhånden kan kalde kendte. Det er ikke svært at forestille sig, at denne forordning i sin endelig form vil blive ganske central og genstand for anseelig opmærksomhed både i det juridiske faglige miljø men også i offentligheden som sådan. Om tilgangen kan indfri det vidtløftige mål om EU som global leder på kunstig intelligens kan kun tiden vise. Her på lederplads må blot opfordres til, at man deltager i lovgivningensprocessen, så den endelige forordning bliver udtryk for det bedste mulige kompromis.

Tue Goldschmieding

Fire nye avgjørelser fra Datatilsynet om kameraovervåkning

Av Fredrik Wiker og Line Helen Haukalid

I løpet av starten av 2021 har Datatilsynet fattet fire vedtak relatert til ulovlig kameraovervåkning og deling av opptak fra kameraovervåkning. I denne artikkelen skal vi se nærmere på hva Datatilsynet har reagert på i sine vedtak og hvordan virksomhetene i lys av disse vedtakene kan sørge for at kameraovervåkningen og deling av opptak skjer i samsvar med personvernregelverket.

Fredrik Wiker

Line Helen Haukalid

Hvilke regler har vi om kameraovervåkning?

Det finnes ikke noe generelt forbud mot kameraovervåkning i norsk rett. Enhver har likevel rett til respekt for sitt privatliv og hjem etter både Grunnloven og straffeloven. GDPR vil dessuten komme til anvendelse der kameraovervåkningen fanger opp personer. I tillegg er det oppstilt egne krav for kameraovervåkning av ansatte i en forskrift til arbeidsmiljøloven.

Retten til privatliv og krav til berettiget interesse

Kameraovervåkning av det offentlige rom eller annens private eiendom vil som en hovedregel kunne utgjøre et brudd på den enkeltes rett til privatliv. I tillegg vil kameraovervåkning, eller deling av slike opptak, kunne involvere behandling av personopplysninger dersom kameraet fanger opp identifiserte eller identifiserbare personer. I slike tilfeller må den som overvåker ha et behandlingsgrunnlag i GDPR artikkel 6 for at behandlingen skal være lovlig. Dersom overvåkingen går ut på å samle inn sensitive personopplysninger, for eksempel ved at stedet man overvåker er uløselig knyttet til sensitive forhold, gjelder enda strengere regler.

Mest aktuelt i denne sammenhengen er *berettiget interesse* etter GDPR artikkel 6 nr. 1 bokstav f. Bestemmelsen gir rettslig grunnlag for å behandle personopplysninger dersom det er nødvendig for å ivareta en berettiget interesse som veier tyngre enn hensynet til den enkeltes personvern.

Tre kumulative vilkår må være oppfylt. Kameraovervåkningen eller behandlingen av kameraopptak må for det første være for et formål knyttet til virksomhetens berettigede interesse. Videre må kameraovervåkingen være et nødvendig tiltak for å ivareta den berettigede interessen. Dette innebærer at det ikke må finnes andre mindre personverninngripende tiltak som kan oppnå det formålet. Til sist må det foretas en *interesseavveining* mellom virksomhetens berettigede interesser på den ene siden og hensynet til individenes rett til personvern på den andre.

Datatilsynet har hittil i år drøftet kravet til berettiget interesse i fire saker om kameraovervåkning. I alle sakene kom Datatilsynet til at det forelå brudd på GDPR.

Deling av opptak fra butikk

14. januar 2021 ble en butikkjede ilagt et gebyr på 400 000 kr fordi en ansatt delte et opptak fra butikkens overvåkningskamera med en privatperson. Opptaket viste et barn som nasket.

Datatilsynet uttalte at selv om butikken hadde interesse i å opp-

klare lovbruddet, kunne denne interessen oppfylles ved å anmelde forholdet til politiet. Datatilsynet stilte derfor spørsmål ved om deling av opptaket var nødvendig for å forfølge butikkens interesse.

Dessuten ble det lagt vekt på at allmennheten har en rimelige forventning om at opptak fra butikker ikke blir delt med andre. En slik deling vil kunne føre til en «offentlig gapestokk». Det var også av skjerpende betydning at de avbildede var barn. Datatilsynet konkluderte derfor med at de avbildedes personvern veide tyngre enn butikkens interesse i å dele opptaket.

Overvåkning av bysentrum

25. mars 2021 ble et selskap ilagt et gebyr på 150 000 kr for kameraovervåking av Rognan sentrum med direkteoverføring til internett. Formålet var å gi innbyggerne et servicetilbud. I tillegg fungerte kameraet som en trygghet for innbyggerne, siden opptak kunne utleveres til politiet.

Selv om kameraet stod for langt unna til å identifisere enkeltpersoner, utgjorde kameraovervåkningen likevel en behandling av personopplysninger, ettersom man kunne kjenne igjen biler, klær og andre karakteristikker.

Datatilsynet la til grunn at det var tvilsomt om kameraovervåkningen hadde noe berettiget formål. I Det europeiske personvernrådets retningslinjer for kameraovervåkning er det riktignok lagt til grunn at beskyttelse mot tyveri, vandalisme og kriminelle handlinger kan utgjøre en berettiget interesse. Dette forutsetter imidlertid at virksomheten påviser at faren er reell, og ikke kun basert på spekulasjon.

Etter Datatilsynets vurdering var det uklart om det forelå noen reell fare for kriminelle handlinger der kameraet var plassert. Datatilsynet vurderte det også slik at kameraovervåkningen kunne ha vært utformet på mindre personverninngripende måter, for eksempel ved å begrense overvåkningen til tider av døgnet hvor kriminelle handlinger typisk skjer. Det var derfor tvilsomt om overvåkningen oppfylte kravet om nødvendighet. Datatilsynet uttalte videre at de overvåkedes personvern uansett gikk klart foran interessen i å tilby et servicetilbud til innbyggerne.

Deling av opptak med arbeidsgiver

9. april 2021 ble en virksomhet ilagt et gebyr på 35 000 kr. Virksomheten hadde gjennom kameraovervåkning fanget opp en person begå hærverk på virksomhetens eiendom. Dette kameraopptaket delte virksomheten med arbeidsgiveren til personen de mente stod bak hærverket.

Datatilsynet la vekt på at delingen med arbeidsgiver var unødvendig for formålet om forebygging og oppklaring av hærverk, blant annet fordi opptakene allerede var oversendt til politiet. Videre ble det vektlagt at slik deling vil oppleves som en personlig belastning for den som er mistenkt for en straffbar handling.

Overvåkning av restaurantlokale

21. april 2021 ble en restaurant ilagt et gebyr på 200 000 kr for kameraovervåkning av bl.a. sitteområder i restauranten.

Datatilsynet vurderte det slik at overvåkningskameraene filmet mer av restaurantens lokaler enn nødvendig, og at det ikke var nødvendig med døgnkontinuerlig kameraovervåkning.

I interesseavveiningen la Datatilsynet vekt på at gjester generelt må sies å ha en berettiget forventning om å ikke bli filmet i restaurantens sitteområder der det foregår sosialt samvær. På områder som brukes til avslapning, rekreasjon og sosialt samvær, må hensynet til personvernet veie tungt. I tillegg la Datatilsynet vekt på de ansattes rett til personvern på jobb. Interesseavveiningen gikk derfor i personvernets favør.

Datatilsynet fant det også skjerpende at virksomheten ikke ga god nok informasjon om overvåkingen, samt at virksomheten ikke hadde gode nok skriftlige rutiner.

Virksomheter må vurdere sin kameraovervåkning

Avgjørelsene sender et tydelig signal om at virksomheter som i dag benytter seg av kameraovervåkning bør foreta en grundig vurdering av om vilkårene i GDPR artikkel 6 nr. 1 bokstav f er oppfylt.

Før man starter med, eller fortsetter å benytte seg av, kameraovervåkning eller utleverer opptak til tredjeparter, bør man stille spørsmål ved om interessene i behandlingen av opptakene er tungtveiende nok. Videre bør man vurdere om disse interessene kan oppnås på mindre personverninngripende måter, for eksempel ved å begrense området som overvåkes eller tidspunktet for kameraovervåkningen. Disse vurderingene må dokumenteres.

I tillegg må virksomheten ha gode og skriftlige rutiner for kameraovervåkningen, herunder om jevnlig sletting av opptak og rutiner for utlevering av opptak til tredjeparter. Virksomheten må også sørge for at de som blir overvåket får tydelig beskjed om dette, både gjennom skilting og i virksomhetens personvernerklæring.

For å sikre at personvernrisikoen reduseres så mye som mulig bør virksomheten også vurdere å gjennomføre en personvernkonsekvensvurdering etter GDPR artikkel 35.

Fredrik Wiker er advokatfullmektig i Wiersholm.

Line Helen Haukalid er fast advokat i Advokatfirmaet Wiersholm.

SSA-SKY 2021 – Ny statens standardavtale for skytjenester

Av Ståle L. Hagen og
Vemund Sande

Ståle L. Hagen

Vemund Sande

Det norske Direktoratet for forvaltning og økonomistyring (DFØ) forvalter porteføljen med Statens Standardavtaler (SSA) for IT-anskaffelser, og i april 2021 publiserte DFØ den offisielle versjonen av «Statens standardavtale for tilrettelegging, innføring og forvaltning av skytjenester levert på standardvilkår», også kalt SSA-SKY. Den offisielle versjonen er endret på flere punkter siden høringsutkastet som ble sendt ut i juli 2020, og den endelige versjonen er også utvidet i omfang siden høringsutkastet.

De senere årene er SSA'ene blitt harmonisert, forenklet og modernisert, stort sett til det bedre hvis man skal tillate seg å mene noe om hva som generelt anses som brukervennlige og balanserte kontrakter. Den nye SSA-SKY går dessverre i motsatt retning, og introduserer et omfang og en kompleksitet som gjør avtalen mindre egnet for de typiske brukerne uten juridisk utdanning eller spesialisering innen IT-kontrakter. I tillegg introduseres flere utradisjonelle reguleringer som etterlater seg uavklarte ansvarsforhold og rom for flere ulike tolkningsalternativer.

For å starte med det helt grunnleggende er SSA-SKY med sine 46 sider så lang at de færreste kunder og leverandører vil forholde seg til innholdet i sin helhet. Kontrakten er faktisk enda lenger, fordi det i bilagsmalen er inntatt reguleringer på enda et par sider om endringshåndtering og avbestilling, som normalt ville inngå i de generelle bestemmelsene. Vår erfaring, selv om vi anbefaler det motsatte, er at kunder og leverandører overlater til advokater og konsulenter å lese gjennom kontraktene når de blir for lange, noe som er uheldig når innholdet også er av betydelig praktisk og operativ betydning for brukerne. Det er godt mulig en og annen innkjøper eller selger, og kanskje til og med en prosjektleder med særlig interesse for kontrakter, drister seg til å sette seg grundig inn i dette dokumentet, men vi tror likevel dette er en kontrakt som er så omfattende og så komplisert at de færreste kunder og leverandører vil sette seg inn i, forstå og bruke kontrakten aktivt.

DFØ kommer også galt ut fra start med sin tilnærming til oppbygging av denne kontrakten. Her tar man mål av seg til å regulere tjenester knyttet til «tilrettelegging, innføring og forvaltning» av standardiserte skytjenester fra en eller flere tredjeparter. Dette kan være skytjenester kunden selv anskaffer direkte fra skytjenesteleverandøren, eller skytjenester som selges gjennom leverandøren slik at denne «primer» (videreselger) skytjenesteleveransen(e) fra en eller flere tredjeparter. Allerede her skaper DFØ problemer for seg selv ved at de gjennom resten av kontrakten må forsøke å sortere hvordan de ulike reguleringene bør være i disse to ulike situasjonene.

Standardiserte skytjenester vil normalt selges basert på skytjenesteleverandørens standard betingelser, og verken kunden eller en eventuell leverandør som «primer» tjenestene vil i særlig grad få aksept for endringer i disse betingelsene. Når kundene presenterer SSA-SKY og forventer at den legges til grunn også for skytjenestene setter det leverandøren som har signert SSA-SKY med kunden i en situasjon hvor han ikke vil få full «ryggdekning» fra leverandørene av skytjenestene. Avvikene mellom SSA-SKY og skytjenesteleverandørenes standard betingelser kan være av en slik art at leverandøren garanterer for mer enn han har anledning til, at de utgjør en kommersiell risiko (som må prises inn i kontrakten) eller de kan være vurdert som mindre betydningsfulle. Man forsøker å kompensere for dette ved at skytjenesteleverandørens standard betingelser tas inn i bilag til SSA-SKY, og

det er en rekke reguleringer som har som formål å sortere hvordan ytelser som leveres av leverandøren selv skal håndteres annerledes enn tjenestene fra skytjenesteleverandøren, men man lykkes bare delvis og presisjonsnivået blir ikke godt nok. Dette er ikke rart da den valgte tilnærmingen gjør dette til en krevende øvelse.

Vi er av den klare oppfatning at en kontrakt som skal regulere tjenester knyttet til «tilrettelegging, innføring og forvaltning» av standardiserte skytjenester fra en eller flere tredjeparter ikke bør ta en «top-down»-tilnærming, slik som DFØ har gjort med SSA-SKY og hvor utgangspunktet er at leverandøren er ansvarlig for «alt» med mindre det eksplisitt er unntatt. Skal det lages en god og brukervennlig kontrakt til dette formålet bør den starte «bottom-up» og regulere positivt hva leverandøren skal være ansvarlig for. På denne måten vil kontrakten bli enklere, tydeligere mht. leverandørens ansvar og mer balansert.

Det er prisverdig at DFØ innser at det er begrensninger i hvilket ansvar leverandøren reelt sett kan og bør ta for tredjeparts skytjenester, men med den valgte oppbyggingen av SSA-SKY blir det fremdeles liggende igjen ansvar hos leverandøren som ikke reelt sett vil kunne mitigeres i betingelsene med skytjenesteleverandørene. Da gjenstår det avvik som enten må prises inn som kommersiell risiko og som gjør tjenesten mer kostbar for kunden, eller som innebærer at leverandøren i verste fall lover mer enn leverandøren kan holde. Sistnevnte situasjon er en effektiv måte for å sortere ut de seriøse leverandørene, ettersom de sjelden vil sette seg i en situasjon hvor det ikke er en forsvarlig balanse mellom ansvar og kontroll.

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-SKY dessverre ikke fremstår som en hensiktsmessig kontrakt.

Ståle L Hagen, partner, Advokatfirmaet Selmer

Vemund Sande, advokat, Advokatfirmaet Selmer

Hvordan skape et supert personvernombud?

Av Kristine Næss og Steinar Østmoe

Ombudsrollen er en av pilarene i forordningen for å sikre godt personvern. Sammen med de andre kravene til behandlingsansvarlige utgjør bruk av personvernombud en av sikkerhetsmekanismene innebygget i forordningen. Sikkerhetsmekanismene var en forutsetning for at man gikk fra forhåndskontroll og konsesjon, til større grad av selvregulering for virksomheter som behandler personopplysninger. Så hvordan kan virksomheten legge til rette for at personvernombudet blir den gode sikkerhetsmekanismen som rollen er ment å være? I denne artikkelen skriver vi om hvordan ledelsen kan legge til rette for å få et godt fungerende personvernombud.

Kristine Næss

Steinar Østmoe

Antallet virksomheter med personvernombud er firedoblet fra 2015 til 2020. I 2020 var det 1 341 registrerte personvernombud i Norge fordelt på 1891 virksomheter. I seg selv skulle dette gi et løft for personvernet. Vår erfaring tilsier imidlertid at mange ikke klarer å utnytte potensiale som ligger i et velfungerende personvernombud. I likhet med andre krav i forordningen er kravene til ombudsrollen formulert som målsetninger eller rettslige standarder som må sees i sammenheng med de overordnede personvernhensynene. For eksempel vil kravet om å «stille til rådighet de ressurser som er nødvendig for å utføre nevnte oppgaver» i artikkel 38 variere fra virksomhet til virksomhet og er avhengig av konteksten. Virksomheter som bare ser på personvernombudet som et felt å krysse av på en sjekkliste, går derfor glipp av mulighetene som ligger i godt personvern, spesielt ved bruk av ny teknologi og store datamengder.

I tillegg risikerer virksomheten gebyrer om de ikke tar ombudsrollen på alvor. Det er sjelden personvernombudets stilling blir gjenstand for tilsynsmyndighetens kontroll. I 2020 ila imidlertid den belgiske tilsynsmyndigheten et av de første gebyrene for brudd på artikkel 38. Virksomheten ble ilagt et gebyr på 50 000 euro, som var ny rekord i Belgia. Avgjørelsen[1] belyser flere viktige momenter som en virksomhet må passe på når de skal ha et personvernombud. I denne artikkelen trekker vi frem noen eksempler fra denne avgjørelsen, og gir våre beste tips til få et supert personvernombud i en virksomhet.

Unngå interessekonflikter

Personvernombudets uavhengighet

Personvernombudets viktigste oppgave er å ivareta personvernet til de registrerte. Hensynet til de regis-

1 n° 18/2020 fra 28. april 2020: *https://autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-18-2020.pdf*

trerte kan fort stå i motsetning til virksomhetens målsetninger. Derfor skal ombudet beskyttes mot mulige interessekonflikter, og ha en uavhengig stilling. Dette innebærer at virksomheten ikke skal gi instruksjoner eller sanksjonere ombudet for måten det ivaretar ombudsoppgavene på. Ombudet skal heller ikke ha tilleggsoppgaver som kan føre til en konflikt mellom de registrerte og virksomhetens interesser. Spenningen mellom hensynet til de registrerte og virksomheten kommer sannsynligvis til å øke etter hvert som store datamengder, inkludert personopplysninger, blir en sentral del av mange virksomheters forretningsmodell og kjerneprosesser. Også i tilfeller der virksomheten i hovedsak behandler personopplysninger til administrasjon av egne ansatte kan den teknologiske utviklingen sette personvernspørsmål på spissen. Vi finner eksempler på dette blant annet hos virksomheter som ønsker å ta i bruk overvåkning av ansattes aktiviteter gjennom arbeidsdagen, blant annet ved hjelp av løsninger som Microsoft Analytics.

Personvernombudet skal ikke ha enkelte typer lederansvar

Personvernforordningen åpner for at ombudsrollen kan kombineres med andre oppgaver og ivaretas av eksterne ressurser. Artikkel 29-gruppen har tidligere uttalt at personvernombudsrollen ikke bør ligge hos personer i virksomheten som beslutter formål og virkemidler for behandlingen av personopplysninger. I samme uttalelse påpeker gruppen at ombudsrollen ikke bør kombineres med rollen som virksomhetens leder, og heller ikke i kombinasjon med rollen som leder for markedsføring-, HR-, IT- og økonomiavdelingene. Dette er roller som typisk har viktige og store mengder personopplysninger under sitt ansvarsområde. I tillegg nevnes det i uttalelsen at ombudsrollen ikke bør ivaretas av en ekstern ressurs som skal forsvare virksomheten i retten i spørsmål knyttet til personvern.

I den belgiske saken fra 2020 var det nettopp interessekonflikten som lå til grunn for tilsynets avgjørelse. Virksomheten hadde i denne saken lagt ombudsrollen til en person som hadde lederansvar for internrevisjon, risikostyring og etterlevelse. Her hevdet virksomheten at det ikke forelå en interessekonflikt, fordi lederansvaret som var kombinert med ombudsrollen, ikke innebar myndighet til å beslutte formål og virkemidler for behandling av personopplysninger. Det belgiske tilsynet var ikke enig. Som leder ville vedkommende ta beslutninger som gjaldt behandling av personopplysninger innenfor *eget ansvarsområde*. Som eksempel nevnte det belgiske tilsynet at internkontrollen kan frembringe funn om ansatte som kan være utslagsgivende for behandlingen av deres personopplysninger. I tillegg la tilsynet vekt på at virksomheten ikke hadde tatt de nødvendige vurderingene før ombudsrollen ble opprettet, og heller ikke iverksatt avhjelpende tiltak. Mer konkret skulle virksomheten ha vurdert mulige interessekonflikter knyttet til alle tre ansvarsområder som vedkommende hadde lederansvaret for. I tillegg skulle virksomheten ha vurdert den samlede effekten på organisasjonen av at ombudsrollen ble ivaretatt av én person som også hadde ansvar for tre andre funksjoner. Videre la tilsynet vekt på at ombudet i praksis ikke ville kunne ivareta ombudsrollen overfor områdene vedkommende hadde lederansvar for: internrevisjon, risikostyring og etterlevelse. Til slutt ble det pekt på risikoen for brudd på ombudets taushetsplikt i artikkel 38 (5) overfor ansatte, som en følge av sammenblanding av rollene.

Den siste utviklingen tilsier dermed at man bør være forsiktig med å kombinere lederansvar og ombudsrollen uten grundige og veldokumenterte vurderinger.

Personvernombudets tilgang på ressurser i virksomheten

Virksomheter med personvernombud er forpliktet til å sikre at rollen kan utføres på en forsvarlig måte, ved å støtte og tilrettelegge for personvernombudet. Dette innebærer at ombudet har tilgang til ressurser som er nødvendige for å ivareta ombudsrollen. Virksomheten må selv vurdere hvilke ressurser som er nødvendige for at personvernombudet kan utføre sine oppgaver på en god måte.

Tilgang til behandlinger og behandlingsaktiviteter i virksomheten er sentralt. Det er en forutsetning for ombudets rådgivning at ombudet har mulighet til å få oversikt over og innsyn i alle behandlinger av personopplysninger i virksomheten. Dette innebærer at personvernombudet må ha tilgang på kontinuerlige prosesser, aktiviteter i daglige drift og prosjektbasert virksomhet. Ombudet må også få tilgang til alle vurderinger knyttet til personvern i virksomheten, herunder personvernkonsekvensvurderinger og behandlingsprotokoll.

Tilgang til «riktige» ressurser i virksomheten

Mange virksomheter kan kvie seg for å sette av større økonomiske midler til heltidsombud og dedikerte støtteressurser. Det er imidlertid en forutsetning at ombudet har tilgang på tilstrekkelige økonomiske og tekniske ressurser. Slik praktisk tilrettelegging er helt nødvendig for å lykkes. Det er også viktig at virksomheten er klar over at det er nødvendig med bidrag fra fagressurser i personvernarbeidet, og at dette krever både planlegging og penger. Dette kan hensyntas allerede i ressurs- og budsjettplanlegging ved å gjøre rom for å prioritere personvernrelatert arbeidsoppgaver i relevante enheter, avdelinger eller fagmiljøer.

Faglig oppdatering

Dybdekunnskap er sentralt for at ombudet kan utføre sine oppgaver på en god måte. Virksomheten bør derfor gjøre det mulig for ombudet å opprettholde en høy faglig standard. Ombudet bør ha anledning til å delta i relevante fagnettverk, og holde seg oppdatert på faglig utvikling gjennom egenstudier, seminarer, fagfellesskap og andre relevante faglige arenaer. På denne måten kan virksomheten se på personvernombudet som sin helt egen personvernekspert, som rådgir og holder oversikt i virksomheten. I tillegg er det nyttig å utveksle erfaringer med andre personvernressurser i andre virksomheter. Foreningen for personvernombudene eller International Association of Privacy Professionals (IAPP) er eksempler på nyttige fagfellesskap.

Formelle rammer

Ved å etablere formelle rammer rundt ombudsrollen kan virksomheten gjøre det enklere å få god nytte av personvernombudet og gjøre det lettere å ivareta kravene i forordningen. Formelle rammer kan også være en god måte å formalisere og dokumentere vurderingene virksomheten har gjort rundt interessekonflikter ved opprettelse av ombudsrollen.

Et formalisert rammeverk er imidlertid ikke nok i seg selv. I den belgiske avgjørelsen hadde virksomheten vedtatt et «charter» som skulle ivareta personvernombudets uavhengighet. Dette i seg selv ble ikke ansett som et tilstrekkelig virkemiddel for å avhjelpe interessekonflikten, siden virksomheten uansett ikke hadde gjort de nødvendige vurderingene.

Omfanget av personvernombudsstillingen

Virksomheten bør etablere klare rammer og oppgaver for personvernombudet. De formelle rammene rundt stillingen bør være proporsjonale, og baseres på en vurdering av virksomhetens behov. Vurderingen bør ta høyde for behandlingens kompleksitet og virksomhetens størrelse. Dette bør komme til uttrykk i de formelle rammene, for eksempel ved fastsettelse av stillingsprosenten. Virksomheten må også vurdere behovet for å opprette et eget team eller egne roller dedikert til å arbeide med personvern og støtte ombudet. Har virksomheten så stor behandlingsaktivitet at de har behov for et personvernombud i 100 % stillingsprosent med dedikerte støtteressurser, eller vil virksomhetens behov for et ombud dekkes av en 50 % stilling?

Personvernombudets plassering i organisasjonen

Enkel tilgang på virksomhetens ledelse

Plassering av ombudet i virksomhetens hierarki er viktig for at ombudsrollen skal ha effekt. Det er en forutsetning at personvernombudet kan kommunisere direkte med relevant ledelse, både for å løfte problemstillinger, bli involvert i relevante diskusjoner og møter, og for å holde ledelsen løpende orientert. En praktisk måte å gjøre dette på er å etablere faste rammer for personvernombudets kommunikasjon med ledelsen. Dette kan for eksempel være regelmessige statusmøter. Et annet virkemiddel er å etablere prosedyrer og rutiner som fastsetter når ledelsen selv skal involvere personvernombudet i spørsmål som gjelder behandling av personopplysninger. Dette forutsetter at ledelsen får opplæring i de rutiner, retningslinjer eller prosedyrer som etableres. Personvernombudet må med andre ord følges opp med aktiv støtte fra virksomhetens øverste ledelse.

Samspill med virksomheten

Videre har ombudet behov for tilgang til og støtte fra relevante fagmiljøer i virksomheten. Her vil særlig IT-, juridisk- og HR-avdeling, i tillegg til fagmiljøer knyttet til informasjonssikkerhet være relevante å trekke på for ombudet. Andre fagmiljøer og avdelinger kan også være relevante, spesielt deler av virksomheten med ansvar for behandling av personopplysninger i sine kjerneprosesser. I offentlig forvaltning kan dette for eksempel være saksbehandling og arkivering. Vår erfaring tilsier også at gode kanaler inn til relevante fagmiljøer kan bidra til å unngå at personvernombudet blir «isolert» fra virksomhetens daglige drift eller linjearbeid.

Å leie inn et eksternt ombud kan bidra til å unngå interessekonflikter, men kan også gjøre det vanskeligere for ombud å orientere og involvere seg i organisasjonen. Dette kan til en viss grad avhjelpes ved at virksomhetens ledelse involverer og gir ombudet tilstrekkelige ressurser til å ivareta rollen.

I avgjørelsen fra det belgiske datatilsynet ble det lagt vekt på at ombudet ikke var tilstrekkelig involvert i de relevante prosessene i virksomheten. Helt konkret viste tilsynet til at virksomheten kun skulle informere ombudet i forbindelse med risikovurdering etter personvernavvik, i stedet for å involvere ombudet fra starten. Det ble blant annet lagt vekt på at ombudet stod oppsatt under «informeres», og ikke «konsulteres» i virksomhetens ansvarsmatriser. Dette viser viktigheten av gode rutiner for involvering av personvernombudet. Spesielt i større og komplekse virksomheter, kan rutiner være et viktig virkemiddel for å sikre at ombudet involveres til riktig tid.

Ombudsrollen må ikke være for sårbar

Vår erfaring er videre at det mange steder bygges mye uformelle og personavhengige strukturer knyttet til ombudsrollen. Dette innebærer en fare for personavhengighet, og gjør virksomheten sårbar for manglende etterlevelse dersom ombudet blir sykt, slutter, eller på andre måter utilgjengelig. Virksomheter kan sikre seg mot denne typen sårbarhet

ved å bygge formaliserte strukturer rundt ombudet, for eksempel ved å ha klare planer for overtakelse av ansvaret dersom ombudet er utilgjengelig. Dette kan særlig være en fordel i større virksomheter, der personvernombudet følger opp og organiserer arbeidet sentralt.

Oppsummert: våre beste tips for å skape et supert personvernombud

Ledelsen kan legge til rette for å få et godt fungerende personvernombud ved å sikre ombudsrollen mot interessekonflikter, tilrettelegge for tilstrekkelig ressurstilgang og gi ombudsrollen det fokuset den trenger i organisasjonen. Dette hviler på at virksomheten gjør de nødvendige vurderingene ved opprettelsen av ombudsrollen, og fra starten ser på personvernombudet som et godt verktøy som kan komme virksomheten til gode. Dette er særlig viktig i en tid med økende fokus på sanksjoner fra tilsynsmyndighetene og en teknologisk utvikling som i stadig større grad setter personvernspørsmål på spissen.

Kristine Helen Lyngholm Næss: Forvaltningsinformatiker og rådgiver innen informasjonssikkerhet og personvern, Sopra Steria.

Steinar Østmoe: Manager og jurist i Sopra Steria.

Illustrasjon: Datatilsynet

Halvor Manshaus

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

Viktig avgjørelse om fair use og programkode: Google vs Oracle

Den føderale høyesterett i USA (SCOTUS) har nylig avsagt dom i en langvarig tvist om opphavsrett mellom Google og Oracle (referanse 18-956). Sentralt i saken sto spørsmålet om rekkevidden av den såkalte fair use-doktrinen. Avgjørelsen trekker opp retningslinjer som kan få stor praktisk betydning ved utvikling av ny programvare delvis basert på eksisterende programkode.

Kort om saksgangen

Saken ble innledet ved søksmål fra Oracle allerede i august 2010, og det ble krevd 8,8 milliarder USD i kompensasjon for inngrep i Oracles programvare. Google fikk medhold i District Court i 2012. Deretter vant Oracle frem i Federal Circuit i 2014, og saken ble sendt tilbake til District Court. Google fikk i 2015 avslag på anke til SCOTUS over avgjørelsen fra Federal Circuit, men vant i 2016 frem i District Court, der en jury ga Google medhold i at det ikke forelå inngrep. Oracle anket saken videre til Federal Circuit, som i 2018 nok en gang konkluderte i Oracles favør. Google anket saken videre i 2019, og endelig dom fra SCOTUS kom 5. april 2021. Saken ble avgjort med dissens 6 – 2, og blir nå hjemvist til underinstansen for avsluttende behandling.

Sakens bakgrunn: Android Inc.

Android Inc ble grunnlagt i 2003. Den opprinnelige planen for virksomheten var å utvikle operativsystem for kameraer. Denne planen ble raskt skrinlagt, ettersom grunnleggerne av Android Inc. så at digitale kameraer på denne tiden ble lagt til side og erstattet av mobiltelefoner med fotofunksjonalitet. Det tok ikke lang tid før det ble besluttet å lage operativsystem til mobiltelefoner i stedet.

Denne type utviklingsarbeid krever tid og ressurser, og uten noe produkt var det vanskelig å generere inntekter. En av de sentrale grunnleggerne, Andy Rubin, har fortalt at han på et tidspunkt måtte gå til investoren Steve Perlman for å få penger til videre drift. Perlman gikk til banken og tok ut USD 10.000 som ble overlevert til Rubin. Driften kunne fortsette, og 11. juli 2005 kjøpte Google opp virksomheten. De ansatte flyttet samme dag over til Googles kontorområde i Mountain View, California.

Dette var begynnelsen på Google's Android operativsystem, som i dag står for en global markedsandel på 70 % i markedet for mobiltelefoner. Android har imidlertid fått en videre anvendelse enn bare mobiler, og brukes i dag som operativsystem på TVer, høyttalere og mye annet. Google kunne i mai 2019 melde om 2,5 milliarder aktive enheter som benyttet Android OS.

Google ønsket å ha et operativsystem som ga en enkel inngang for programmerere over hele verden. På denne måten ville det være enklere å bygge opp tredjeparts programmer og løsninger som kunne brukes i Googles nye Android plattform.

Det var derfor ønskelig å bruke Java som utgangspunkt for deler av den nye Android plattformen. Java er et objektorientert programmeringsspråk utviklet av Sun Microsystems. I motsetning til mange andre programmeringsspråk kompileres ikke Java til maskinkode før det kan kjøres av en datamaskin. I stedet brukes et underliggende program som heter Java Virtual Machine (JVM). Ved å ha JVM installert, vil brukeren kunne kjøre javaprogrammer uavhengig av hva slags operativsystem som benyttes. Java hadde derfor vid utbredelse, og var kjent for svært mange som drev med programmering.

Google forhandlet derfor med Sun om en lisens for bruk av Java. Da disse forhandlingene strandet, kopierte Google i stedet om lag 11 500 linjer med programkode fra Java SE (den aktuelle versjonen av Java). Disse kodelinjene var en del av Javas application programming interface (API). Et API er kort forklart et grensesnitt for å kjøre programmer fra en samarbeidende programvare. Et eksempel på bruk av API er databaser, der det kjøres kommandoer fra et enkelt grensesnitt for å gjøre kjøringer mot en underliggende database. Når brukeren gjør et Google-søk, overføres det opplysninger fra søkestrengen

på nettsiden til databasen hos Google som resulterer i en treffliste. Ved å bruke API fra Java gjorde Google det enkelt for nye programmerere å kommunisere med Android OS. Ved bruk av enkle Java-kommandoer kunne det gjøres operasjoner i det underliggende Android OS.

Den kommersielle koblingen som motiverte bruken av Java i det nye operativsystemet fra Google, kommer klart frem i dommen, der det siteres fra underinstansen:

> *«Google envisioned an Android platform that was free and open, such that software developers could use the tools found there free of charge. Its idea was that more and more developers using its Android platform would develop ever more Android-based applications, all of which would make Google's Android-based smartphones more attractive to ultimate consumers. Consumers would then buy and use ever more of those phones.»*

I avgjørelsen pekes det på at Android ble en kommersiell suksess. Allerede i 2015 ga Android over USD 42 milliarder i inntekter til Google.

Oracle kjøpte opp Sun Microsystems i 2010 og innledet da søksmålet mot Google: Denne saken har altså pågått i over et tiår. Saken var opprinnelig lagt opp bredere, med anførsler knyttet opp mot patentinngrep som senere falt bort. Google skal for øvrig på et tidspunkt ha endret sitt Android OS slik at det ikke lenger benytter den aktuelle koden fra Java API.

Rettslig vurdering

Slik saken var lagt opp, lå det to spørsmål til behandling. Det første spørsmålet var hvorvidt Java API nøt vern som åndsverk. Det andre spørsmålet var om det forelå såkalt «fair use».

Retten viser til at det aktuelle området gjelder IT-programmering som er gjenstand for store og hurtige endringer når det gjelder teknologisk, økonomisk og kommersiell utvikling. Med dette som grunnlag slås det fast at det ikke er ønskelig å besvare flere spørsmål enn strengt nødvendig for å avgjøre tvisten. Det ble dermed lagt til grunn «purely for argument's sake» at det forelå opphavsrettslig vern for Java API. Dermed kunne SCOTUS avgjøre saken på spørsmålet om det forelå fair use uten å konkludere på det første spørsmålet. Avgjørelsen ble avsagt under dissens, der flertallet konkluderte med å frifinne Google under henvisning til at det ble funnet å foreligge fair use.

Fair use-doktrinen bygger på at bruk av et rettighetsbelagt åndsverk ikke utgjør inngrep dersom det foreligger grunnlag for en rimelig eller rettferdig utnyttelse. Doktrinen åpner dermed opp for vederlagsfri utnyttelse av et verk der dette etter en helhetsvurdering fremstår som rimelig. I avgjørelsen beskrives dette slik:

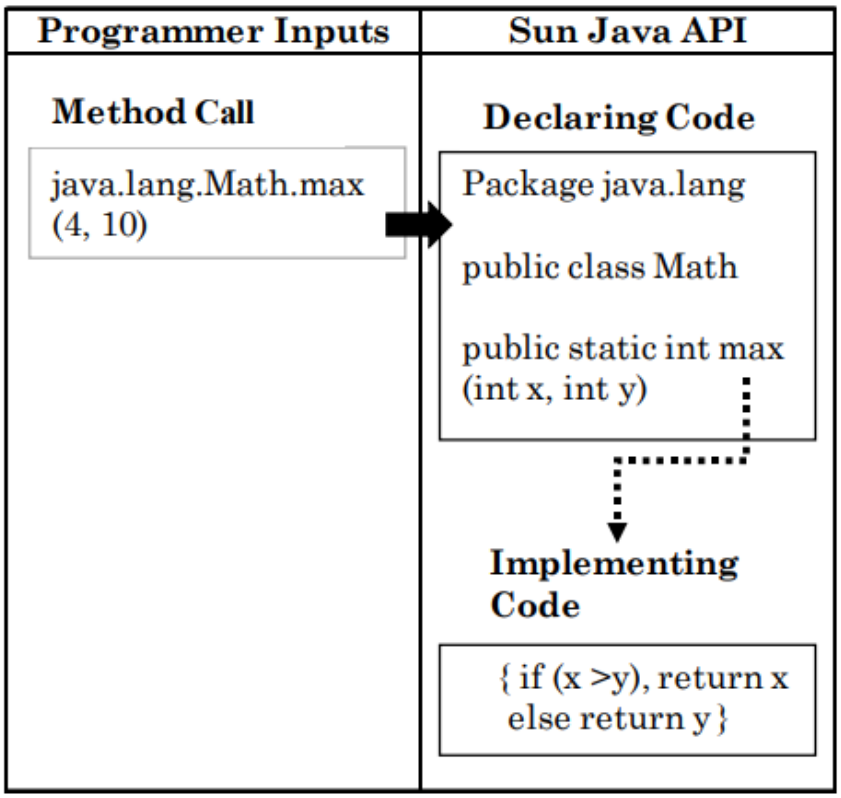
> *«We have described the "fair use" doctrine, originating in the courts, as an "equitable rule of reason" that "permits courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster.»*

USAs Copyright Act, 17 U.S.C. § 107 angir fire sentrale vilkår for vurderingen:

1. *the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;*
2. *the nature of the copyrighted work;*
3. *the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and*
4. *the effect of the use upon the potential market for or value of the copyrighted work.*

I avgjørelsen fremheves at disse vilkårene *«…indicates, rather than dictates, how courts should apply it»*. Det understrekes samtidig at vilkårene ikke utgjør et scorekort som automatisk avgjør saken.

Flertallet valgte å se på vilkår 2 først, *«the nature of the copyrighted work»* – åndsverkets art. I denne analysen gjøres det i avgjørelsen en



distinksjon mellom kode som *deklarerer* og kode som *implementerer*. Denne inndelingen er på linje med bruk av programmeringsparadigmer for å angi den funksjonelle anvendelsen av et program. Deklarativt vil si at koden eller språket beskriver *hva* brukeren vil oppnå, uten å forklare *hvordan* dette skal gjøres. Programmet sier for eksempel at det skal hentes informasjon fra en database om et sett med opplysninger, men uten å forklare hvordan dette skal skje. Implementerende viser til at datamaskinen får en trinnvis beskrivelse av oppgaven som skal utføres.

Illustrasjonen er hentet fra vedlegg B til avgjørelsen og viser sammenhengen mellom de ulike delene av Java API. Brukeren initierer en handling ved å gjøre et metodekall i formatet java.lang.Math.max(4,10). Denne instruksen fra brukeren går til Java API, som i den deklarative koden finner korrekt oppgaveangivelse og hvilken klasse denne tilhører. Den enkelte klasse vil igjen være allokert under en angitt pakke. Alle kodelinjene som angir og benevner metode, klasser og pakker, er deklarativ kode. Den stiplete linjen viser grensesnittet mot den implementerende koden som faktisk instruerer datamaskinen.

I den aktuelle saken hadde Google kopiert tusenvis av kodelinjer med deklarativ koding, mens det retten kaller implementerende kode ble utviklet av Google selv. Det slås deretter fast at den første kodetypen etter sin art er mindre kreativ, og at den typisk vil være bundet opp mot struktur, organisering og oppgaveallokering. Det konkluderes deretter med at denne typen programkode, i den grad det i det hele tatt kan oppstå et åndsverk, ligger lenger unna kjerner av åndsretten enn andre typer dataprogrammer – som for eksempel implementerende kode. Dette brukes deretter som støtteargument for å vise til at anvendelse av fair use i den aktuelle saken vil ha begrensede konsekvenser, ettersom det kun er snakk om programkode i det laveste sjiktet av verkshøydebegrepet.

Det neste punktet er det første på listen, som er knyttet opp mot brukens formål og karakter. I flere tidlige saker har SCOTUS lagt vekt på om bruken er *«transformative»*. I dette ligger det en vurdering av om det er produsert et nytt og eget verk, og om det gjøres en egen kreativ innsats som kommer publikum til gode. Som eksempel vises det i avgjørelsen blant annet til at en parodi nødvendigvis må etterligne originalen for å få frem sitt poeng. Dette er et sentralt trekk i såkalt *appropriation art*, der kunstneren setter tidligere kjente elementer i en ny kontekst og dermed skaper nytt og originalt innhold basert på hel eller delvis kopiering av et verk. Tanken går tilbake til Marcel Duchamp som tok kjente elementer og plasserte i en ny kontekst, såkalte readymades. Verket *Fountain* (1917) var en masseprodusert pissoarskål i porselen som typisk ble brukt på offentlige toaletter. Ved å plassere gjenstanden på en museumsutstilling, ble det skapt debatt om hva kunst egentlig er. Duchamp er også kjent for en reproduksjon av *Mona Lisa* som et billig postkort der hovedpersonen har fått påmalt bart og fippskjegg.

Det finnes flere eksempler på tilsvarende vurderinger i Europeisk rett der parodier kan tillates etter en konkret vurdering av inngrepet opp mot den europeiske menneskerettskonvensjon artikkel 10 om ytringsfrihet, se f. eks. omtale av Deckmyn-saken i LoD-2014-120-30 «Ytringsfrihet og opphavsrett». Poenget i denne kontekst er at det i flere sammenhenger vil være nødvendig å gjenskape originalen for å utøve et nytt og selvstendig uttrykk, og at åndsretten har døren på gløtt når det gjelder å tillate dette.

I avgjørelsen fremheves at Google begrenset bruken av Java API til det som var nødvendig for å lage instruksjoner til mobiltelefoner. I støtteskriv fra diverse amici i saken var denne prosessen beskrevet som en reimplementering. Begrepet er nok benyttet bevisst for å argumentere for at det foreligger en transformasjon eller endring målt opp utgangspunktet. Poenget fra Google og partshjelperne var at Java fremsto som et kjent språk, og at dette kun ble brukt for å kommunisere mot et underliggende implementerende system som Google selv hadde utviklet. Dermed oppsto det en ny og kreativ bruk av det eksisterende API-språket ble det sagt. Retten viser også til tidligere bevisførsel i saken, der det fremkom at det i IT-bransjen skal ha vært vanlig å gjenbruke APIer, og at Sun selv hadde benyttet eksisterende APIer ved utviklingen av Java. Det var også blitt fremhevet at rimelig utnyttelse av funksjonell kode kan gi et enhetlig og konsistent grunnlag for ny og kreativ utvikling. Det var flere innlegg fra tredjeparter i saken, og det ble også påpekt at en for sterk opphavsrett på funksjonelle elementer som i praksis er etablert som industristandarder, vil kunne gi rettighetshaveren en sterkt konkurransebegrensende makt.

Det var da ikke avgjørende at Google hadde et kommersielt motiv bak bruken av API, ettersom retten mente å ha funnet vektige argumenter som talte for at det første vilkåret var innfridd.

Det tredje vilkåret på listen og i drøftelsen er spørsmålet om hvor vesentlige deler av åndsverket som er utnyttet. Googles bruk av 11 500 kodelinjer var hentet fra 37 pakker med Java kode, som inneholdt all koden nødvendig for å fremkalle hundrevis av ulike implementerende handlinger i det underliggende dataprogrammet. Dette høres ut som en omfattende kopiering, men det vises i avgjørelsen til at det totale omfanget av Java API programkode lå på 2,86 millioner linjer. Den aktuelle delen utgjorde således 0,4 % av det totale verket. Det var da naturlig å vurdere om inngrepets omfang skulle vurderes ut ifra den isolerte

konteksten av 11 500 kodelinjer som var benyttet, eller sammenlignes med totalen.

Retten viser til at selv et mindre utdrag kan gjøre inngrep, spesielt der utnyttelsen ligger i kjernen av originalverket. Som eksempel vises det til at det å kopiere en enkelt setning fra en novelle kan være neglisjerbart, men at situasjonen er en annen der den ene setningen faktisk kopierer helt verket. Det siteres deretter fra *El Dinosaurio* av Augusto Monterroso. Verket er anerkjent som verdens korteste historie, og lyder slik:

«Cuando despertó, el dinosaurio todavía estaba allí.»

Da han våknet, var dinosauren der fremdeles.

Det er skrevet flere doktoravhandlinger om dette verket, som kanskje først og fremst overlater det meste til leserens fantasi. Et annet kjent verk som faktisk er kortere lyder

«For sale: Baby shoes, Never Worn.»

Dette skal ha vært utfallet av et veddemål på 1920-tallet da Hemingway ble utfordret av noen kollegaer til å forfatte en novelle på bare seks ord. I følge anekdoten skal de andre uoppfordret ha betalt forfatteren innsatsen på USD 10 hver da de fikk den triste teksten presentert. Anekdoten ble først kjent over 30 år etter Hemingways død, men resulterte i en rekke korte historier i samme genre. Det er usikkert om anekdoten er sann, så det virker rimelig å la Monterroso gå av med seieren.

I dette tilfellet fant retten at Google ikke hadde gått inn i kjernen av åndsverket. Som påpekt ovenfor, hadde retten allerede latt spørsmålet om verkshøyde stå åpent, men gitt en klar indikasjon på at den deklarative koden uansett ville ha ligget lavt i dette terrenget. Retten gjør så en drøftelse av API kodens karakter og fokuserer på funksjonaliteten i språket. Det fremheves at Google ikke søkte kodens estetiske eller kreative karakter, men hadde behov for selve funksjonaliteten. Retten legger vekt på behovet for interoperabilitet mellom ulik programvare, og at den deklarative koden fra Java API var nøkkelen til det hele. Retten konkluderer med at det tredje vilkåret taler i retning av fair use og hengir seg til metafysikken i sin oppsummering av Google arbeidsprosess:

> *«In a sense, the declaring code was the key that it needed to unlock the programmers' creative energies. And it needed those energies to create and to improve its own innovative Android systems.»*

Det fjerde vilkåret på listen fokuserer på markedsvirkningen av inngrepet sett i forhold til originalverket. Det egentlige spørsmålet under denne vurderingen synes å være om inngrepet forårsaker økonomisk skade i hendene på rettighetshaveren. Vurderingen er likevel mer nyansert. Retten påpeker at et parodiverk som påvirker salget av originalen, ikke nødvendigvis innebærer at det foreligger markedspåvirkning i opphavsrettslig forstand. Det må blant annet også legges vekt på hvilken positiv effekt kopiverket medbringer.

Avgjørelsen viser til tidligere bevisførsel, der det fremgår at Sun var svakt posisjonert for en inngang i mobilmarkedet. Den tidligere lederen for Sun hadde selv forklart for underinstansen at Googles Android OS ikke hadde ødelagt muligheter for Sun i dette markedet. Oracle argumenterte mot dette, og retten anerkjenner at Google har tjent enorme summer på sitt nye operativsystem. Likevel konkluderes det i favør av Google også på dette punktet. Retten legger her avgjørende vekt på at åndsverket fra Sun har utviklet seg til et funksjonelt verktøy med bred utstrekning, og at et monopol på dette basert på opphavsrett vil legge sterke bindinger på nettopp innovasjon og nye kreative frembringelser. Alle brukerne av Java API har investert betydelige ressurser i å lære seg språket, og det ville medføre enorme kostnader og ressursbruk å kreve at det utvikles nye parallelle kodespråk. Retten viser her til en tidligere avgjørelse fra 1992 mellom Sega og Accolade som gjaldt omvendt utvikling av programvare (dataspill):

> *«An attempt to monopolize the market by making it impossible for others to compete runs counter to the statutory purpose of promoting creative expression.»*

Retten velger i stor grad å se bort fra den enorme inntjeningen Google har hatt på sitt produkt og fremhever i stedet usikkerheten knyttet til Suns inngang i mobilmarkedet. Dette kan virke som en kursendring når man ser på tidligere avgjørelser knyttet til fair use. Retten understreker derfor at det innenfor inngrep i programvare gjør seg gjeldende særlige hensyn ved at koden etter sin art er funksjonelt utformet:

> *«The fact that computer programs are primarily functional makes it difficult to apply traditional copyright concepts in that technological world.»*

Det understrekes deretter at avgjørelsen ikke skal leses som en endring i vilkårene for fair use. Det pekes på at utfallet er konkret begrunnet i Googles begrensede kopiering for å lage et nytt og *«transformative»* verk, der det ligger implisitt at de deklarative kodelinjene i Java API har hatt et svakere vern enn andre verkskategorier.

Drøftelsen fra flertallet reiser en rekke spennende problemstillinger som det går utenfor rammene av denne spalten å gjennomgå. Vi kan likevel ta oss tid til å gjøre oss kjent med synspunktene til de to dissenterende dommerne. Dissensen fra D0mmerne Clarence Thomas og Samuel Alito tar utgangspunkt i spørsmålet om Java API i det hele tatt har opphavsrettslig vern. Det

påpekes at ved å unnlate å vurdere dette spørsmålet, har flertallet hoppet over en viktig del av sakens problemstilling.

> *«The Court reaches this unlikely result in large part because it bypasses the antecedent question clearly before us: Is the software code at issue here protected by the Copyright Act?»*

Dommer Thomas, som har ført dissensen i pennen, sammenligner metodene som inngår i Java som programmeringsspråk med legaldefinisjoner. Slike definisjoner er en velkjent lovgivningsteknikk. Han viser til at det rettslige begrepet flyktning er tilordnet en definisjon som inneholder mer enn 300 ord. Dermed kan begrepet flyktning brukes i lovteksten, og har dermed en deklarativ funksjon som gjør lovteksten mer kondensert og håndterbar. På denne måten kan lovgiver eller en programmerer ved bruk av riktige metodeangivelser kommunisere kompliserte budskap kortfattet og presist.

Dommer Thomas viser til at Sun hadde gjort Java til open source, og at lisensen her forutsatte at det resulterende programmet skulle være kompatibelt med alle Java plattformer. Utviklere ble oppfordret til å utvikle og forbedre plattformen under den samme åpne lisensen. Dersom man ønsket å beholde den nye koden som en forretningshemmelighet, ville det påløpe en egen lisensavgift. Dissensen fremhever at det rundt 2005 var en rekke aktører som jobbet med å frembringe operativsystem for mobiltelefoner. Grunnet suksessen med Java var det millioner av programmerere som behersket dette kodespråket, og Java var allerede tatt i bruk på de fleste samtidige mobilplattformene. Google skal ha forsøkt å fremforhandle en lisens for Java fire ganger i perioden 2005 – 2006 uten å lykkes. Apple og Microsoft skrev sin egen deklarative kode, mens dommer Thomas fremhever at Google kopierte de aktuelle kodelinjene fra Java API for deretter å fremheve i markedsføringen at det nye Android operativsystemet inneholdt *«Core Java Libraries»*. Det ligger i argumentasjonen her at de to dissenterende dommerne er av den oppfatning at også den deklarative programkoden nyter vern som åndsverk under intern rett. Tilnærmingen er lagt opp ganske bredt, og dommer Thomas anerkjenner at deklarative programmer vil ha et sterkt funksjonelt preg. Samtidig påpeker han at dette ikke gjør arbeidet mindre kreativt:

> *«Computer code occupies a unique space in intellectual property. Copyright law generally protects works of authorship. Patent law generally protects inventions or discoveries. A library of code straddles these two categories. It is highly functional like an invention; yet as a writing, it is also a work of authorship.»*

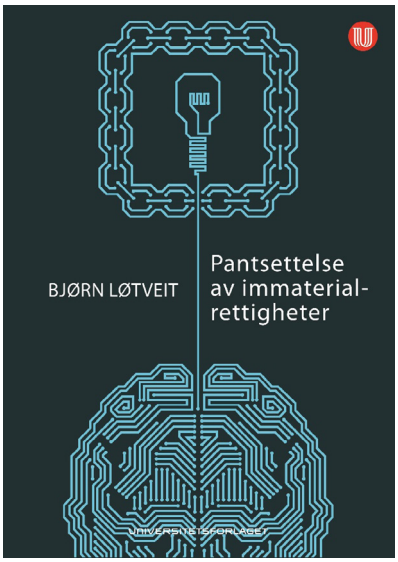
Hans poeng er at valget er gjort ved at dataprogrammer nyter vern som åndsverk i internretten. Definisjonen av dataprogrammer åpner ikke for et skille mellom deklarative og implementerende programmer. Det vises også til lovens definisjon for verkshøyde som ikke avgrenser mot spesielle kategorier av programkode. I stedet tar dommer Thomas utgangspunkt i flertallets uttalelse om at deklarativ og implementerende kode er *«inextricably bound»,* og at deklarativ kode ikke har noen funksjon uten at det eksisterer en programkode som kan implementere kommandoene. Denne gjensidige avhengigheten kan dermed sies å understreke at den ene er likeverdig den andre i forhold til verkshøyde.

Jeg er full ut enig i et helt vesentlig punkt i denne dissensen. Det går på metoden. Ved å ikke ta stilling til hvorvidt den deklaratoriske Java API koden har vern som åndsverk, legger flertallet gjennomgående til grunn i sin analyse at den deklaratoriske koden ligger på et svært lavt nivå i forhold til verkshøyde. Det oppstilles et vannskille mellom deklaratorisk og implementerende kode, uten at det er gjort en forutgående analyse som forteller oss om denne tilnærmingen er riktig. Dersom man nå går tilbake og leser gjennom flertallets drøftelse, mener jeg å se at dommer Thomas har et godt poeng. Det er ikke nødvendigvis slik at resultatet i avgjørelsen er feil, men ved ikke å ta stilling til dette spørsmålet, blir fundamentet for de videre vurderinger unødvendig svakt. Konsekvensen av avgjørelsen blir uansett større enn det flertallet legger opp til i sin avslutning. Ved å antyde at deklaratorisk kode har et i beste fall svakt opphavsrettslig vern, har SCOTUS i realiteten åpnet for nettopp en slik endring eller justering knyttet til fair use for programkode som det uttaler at flertallet ikke tok sikte på. Det blir som dommer Thomas skriver, *«…difficult to imagine any circumstance in which declaring code will remain protected by copyright.»*

Ved å ikke ta stilling til spørsmålet om deklaratorisk kode nyter vern, gjenstår det samtidig større uklarhet enn om dette var blitt konkret avgjort. Denne usikkerheten påvirker en IT-bransje der mange har fremholdt at bruk av deklaratorisk programkode til en viss grad ikke kan anses som inngrep. Det ligger også i fair use-vurderingen at hvert tilfelle må avgjøres konkret og ut i fra det faktum som foreligger. Med den tilnærming som vi ser i denne avgjørelsen, er det nå likevel en større åpning for å anse deklaratorisk programkode som en slags felles infrastruktur som kan benyttes ved frembringelsen av nye dataprogrammer.

Pantsettelse av immaterialrettigheter

Bjørn Løtveit.
Universitetsforlaget – 456 s. Oslo 2021 – ISBN: 9788215040875



Innovasjon er nødvendig for samfunnsutviklingen, men det er også kostbart. Adgangen til å pantsette immaterialrettigheter kan øke kredittilgangen for innovasjons- og teknologibedrifter. Det er på denne måten en sammenheng mellom rimelig kreditt og innovasjon. Denne sammenhengen er utgangspunktet for boken *pantsettelse av immaterialrettigheter*.

Forfatteren går grundig inn på spørsmål knyttet til pantsettelse av et bredt spekter ulike immaterialrettigheter. Ikke bare formelle immaterialrettigheter som patent, – varemerke- og opphavsrettigheter behandles, men også immaterialrettslignende formuesgoder som forretningshemmeligheter, «knowhow» og domenenavn. Særtrekkene ved immaterialrettigheter som formuesgoder drøftes også på et mer overordnet nivå. Selv om boken omhandler et særskilt panterettslig tema, bidrar den også med analyser av verdi for mer allmenne panterettslige og formuerettslige spørsmål.

Boken er basert på Løtveits doktoravhandling fra 2019. Dette var den første vitenskapelige avhandlingen i nordisk rettsteori som behandler reglene om pantsettelse av immaterialrettigheter rettsdogmatisk i monografisk form.

Bjørn Løtveit har master i rettsvitenskap fra 2014, og ph.d. i rettsvitenskap fra 2019. Han jobber som førsteamanuensis ved Det juridiske fakultet, UiT – Norges arktiske universitet.

Personvern og kontroll i arbeidslivet

Marion Holthe Hirst, Signhild Blekastad. Gyldendal – 448 s. Oslo 2021 –- ISBN/EAN: 9788205538368

Boken gir en oversikt over de mest sentrale reglene og problemstillingene som gjelder personvern og de delene av arbeidsretten som gjelder kontroll i arbeidslivet.

Alle virksomheter behandler personopplysninger om sine ansatte for ulike formål og i ulike sammenhenger. Kjennskap til hvilke regler som gjelder for dette, er derfor noe mange har behov for.

Bokens tema er omfattende, noe som medfører at enkelte problemstillinger kun blir overfladisk behandlet. På andre områder går boken mer i dybden, det gjelder særlig temaer som er spesielt aktuelle, eller som ikke tidligere er grundig behandlet i faglitteraturen. Videre er boken utformet slik at den skal være mulig å forstå uten spesielle juridiske forkunnskaper.

Bokens tema er relevant for mange, både for arbeidstakere, arbeidsgivere, advokater, tillitsvalgte, personvernombud og andre som arbeider med juridiske problemstillinger i krysningspunktet personvern og arbeidsrett.

Gorrissen Federspiel

Tue Goldschmieding

Datatilsynet udtaler kritik af Danmarks Statistik for ikke at ajourføre oplysninger

Det danske Datatilsyn ('Datatilsynet') har den 16. februar 2021 ved afgørelse i sag med journalnummer 2020-32-1733 udtalt kritik af Danmarks Statistiks manglende ajourføring af personoplysninger.

En borger klagede den 18. september 2020 til Datatilsynet over Danmarks Statistiks behandling, og manglende sletning, af hans personoplysninger. Klageren havde flere gange henvendt sig til Danmarks Statistik og frabedt sig at blive kontaktet. På trods af flere meddelelser fra Danmarks Statistik om, at klager ikke længere ville blive kontaktet, modtog klager fortsat henvendelser fra Danmarks Statistik.

Datatilsynet fandt, at Danmarks Statistiks behandling af personoplysninger var sket i overensstemmelse med artikel 6, stk. 1, litra e i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'), der tillader behandling af personoplysninger, hvis behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse, eller som henhører under offentlighedens myndighedsudøvelse. Ligeledes var behandlingen sket i overensstemmelse med databeskyttelsesforordningens artikel 17, stk. 3, litra b, der fastslår, at retten til at få slettet personoplysninger ikke gælder, hvis behandlingen er nødvendig for at overholde en retlig forpligtelse, der kræver behandling efter medlemsstaternes nationale ret.

Danmarks Statistik oplyste, at de fører en intern liste over borgere, som ikke ønsker at blive kontaktet med henblik på at deltage i frivillige undersøgelser. Klager blev ved sin første henvendelse ikke registreret korrekt på denne liste. Datatilsynet fandt ikke grundlag for at udtale kritik af den manglende registrering.

Datatilsynet fandt imidlertid anledning til at udtale kritik af, at Danmarks Statistik, ved behandling af oplysninger om klager, ikke havde iagttaget databeskyttelsesforordningens artikel 5, stk. 1, litra d, som netop fastsætter krav om ajourføring ved behandling af personoplysninger. Datatilsynet lagde vægt på, at på trods af at Danmarks Statistik havde meddelt klager, at han ikke længere ville modtage henvendelser, fortsatte klager med at modtage henvendelser.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2021/feb/klage-over-danmarks-statistiks-manglende-ajourfoering-af-personoplysninger

Ny afgørelse om optagelse af telefonsamtaler

Det danske Datatilsyn ('Datatilsynet') har den 10. februar 2020 ved afgørelse i sag med journalnummer 2019-32-0988 udtalt alvorlig kritik af Lægevagten Region Syddanmark ('Lægevagten') for at opbevare optagede telefonsamtaler, som var mere end fem år gamle.

En borger klagede henholdsvis den 11. og 18. august 2020 til Datatilsynet over Lægevagtens behandling af personoplysninger om borgeren. Under sagen kom det frem, at Lægevagten havde optaget og gemt ca. 7,5 millioner samtaler siden januar 2013.

Datatilsynet tog først stilling til borgerens klage om Lægevagtens behandling af borgernes personoplysninger. Det fremgår af artikel 9, stk. 1 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'), at der som udgangspunkt gælder et forbud mod behandling af bl.a. helbredsoplysninger. Er behandlingen nødvendig som følge af eksempelvis sundhedsomsorg og sundhedstjenester, vil den dog være lovlig. Datatilsynet lagde til grund, at formålet med Lægevagtens optagelse af samtalerne var at sikre dokumentation til brug for eventuelle klage- og erstatningssager. Datatilsynet kom frem til, at en sådan behandling udgjorde forvaltning af sundhedsomsorg og sundhedstjenester. Lægevagten havde dermed haft hjemmel til at optage samtalerne.

Datatilsynet tog herefter stilling til Lægevagtens gemte og optagede telefonsamtaler siden januar 2013. Lægevagten anførte, at optagelserne udgjorde en del af borgernes patientjournaler. Efter § 15 i bekendtgørelse nr. 530 af 25. maj 2018 ('Journalføringsbekendtgørelsen') skal patientjournaler opbevares i mindst ti år. Datatilsynet var imidlertid kommet frem til, at formålet med optagelserne var at sikre dokumentation til brug for eventuelle klage- og erstatningssager, og at optagelserne derfor ikke udgjorde en del af borgernes patientjournaler.

Datatilsynet fandt, at opbevaring af lydoptagelser i op til fem år vil være i overensstemmelse med databeskyttelsesforordningen, da behandlingen vil være nødvendig for at opfylde ovennævnte formål i denne periode. Datatilsynet bemærkede, at der gælder en absolut frist på fem år for indgivelse af klager inden for sundhedsvæsenet. Datatilsynet fandt på baggrund heraf grundlag for at udtale alvorlig kritik af Lægevagtens opbevaring af optagede telefonsamtaler, som var mere end fem år gamle, jf. artikel 5, stk. 1, litra e.

Datatilsynet meddelte Lægevagten påbud om at slette alle optagelser af telefonsamtaler, som var mere end fem år gamle.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2021/feb/regionale-laegevagters-optagelse-af-telefonsamtaler

Læs Datatilsynets vejledning om optagelse af telefonsamtaler:
https://datatilsynet.dk/Media/B/F/Optagelse%20af%20telefonsamtaler.pdf

Datatilsynet udgiver vejledning om udmåling af GDPR-bøder

Det danske Datatilsyn ('Datatilsynet') udgav den 29. januar 2021 i samarbejde med Rigspolitiet og Rigsadvokaten en vejledning om beregning af bøder i sager med virksomheders overtrædelse af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') og lov nr. 502 af 23. maj 2018 ('databeskyttelsesloven'). Formålet med vejledningen var at skabe en øget gennemsigtighed i fastsættelsen af størrelsen på bøderne for overtrædelse af databeskyttelsesforordningen.

Bødeniveauet skal afspejle hensynet i databeskyttelsesforordningens artikel 83, stk. 1. Ifølge bestemmelsen skal bøden være et effektivt middel, stå i rimeligt forhold til overtrædelsen og have en afskrækkende virkning. Vejledningens bødeberegningsmodel tager udgangspunkt i et grundbeløb. Datatilsynet fastsætter beløbet efter hvilken rettighed, der er blevet krænket og efter størrelsen af den dataansvarlige virksomhed. Først udregner Datatilsynet det maksimale bødeniveau for den pågældende overtrædelse, hvorefter Datatilsynet fastsætter grundbeløbet til mellem 5 % og 20 % heraf.

Når grundbeløbet er fastsat, op- eller nedjusterer Datatilsynet bødeniveauet alt efter overtrædelsens karakter, omfang, formål, antal af berørte registrerede, omfanget af skaden og varigheden. Der vil eksempelvis ske en nedjustering af bødeniveauet, hvis en overtrædelse sker som led i udbetaling af førtidspension frem for kommerciel markedsføring.

Det er muligt at justere bødeniveauet afhængigt af, om der foreligger skærpende eller formildende omstændigheder. Sådanne omstændigheder omfatter tilregnelsesgrad, tabsbegrænsningsforanstaltninger, tidligere overtrædelser, samarbejdsvillighed og økonomiske fordele.

Endelig oplyser Datatilsynet i vejledningen, at det vil være muligt at justere bødeniveauet efter betalingsevnen. I overensstemmelse med proportionalitetsprincippet, kan Datatilsynet nedjustere bøden, hvis størrelsen bringer virksomhedens økonomiske levedygtighed i fare.

Datatilsynet vil løbende opdatere vejledningen, efterhånden som de, Det Europæiske Databeskyttelsesråd, anklagemyndigheden og domstolene håndterer flere straffesager på området, og som praksis på bødeområdet udvikler sig.

Læs hele vejledningen her:
https://www.datatilsynet.dk/Media/1/9/B%C3%B8devejledning.pdf

Datatilsynet udgiver vejledning om udveksling af oplysninger med politiet

Det danske datatilsyn ('Datatilsynet') offentliggjorde i januar 2021 en vejledning om private aktørers og offentlige myndigheders udveksling af personoplysninger med politiet. Vejledningen er udarbejdet for at undgå, at politiet støder på problemer med at få udleveret personoplysninger til brug for deres efterforskning, da private aktører og offentlige myndigheder kan have en frygt for at overtræde databeskyttelsesreglerne.

Formålet med vejledningen er derfor at illustrere de vide rammer, der gælder ved videregivelse af personoplysninger til politiet ved politiets efterforskning af strafbare forhold i overensstemmelse med Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 6 og 9 og lov nr. 502 af 23. maj 2018 ('den danske databeskyttelseslov') § 8.

Overordnet præciserer den nye vejledning, at der som udgangspunkt kan ske videregivelse af personoplysninger, når politiet anmoder om disse. Det vil eksempelvis være lovligt at udlevere videooptagelser til politiet, hvis politiet skal bruge optagelserne til at efterforske en mulig kriminel handling. Ligeledes kan der ske videregivelse af personoplysninger til politiet, når en person selv retter henvendelse til politiet med henblik på at anmelde et strafbart forhold.

Vejledningen bemærker, at politiet under en igangværende efterforskning ofte ikke kan dele konkrete oplysninger om, hvad politiet skal bruge personoplysningerne til, men at det ikke skal afholde personer fra at videregive personoplysningerne til politiet.

Vejledningen påpeger også, at der i en række tilfælde under indhentelse af personoplysninger gælder krav om retskendelse eller andre krav fastsat i retsplejeloven. Det er politi-

ets ansvar at sikre, at disse krav er overholdt. Hvis en dataansvarlig er i tvivl om, hvorvidt der i en given situation gælder bestemte krav, kan der rettes forespørgsel herom til politiets sagsbehandler. Vejledningen fremhæver, at det må lægges til grund, at politiet alene efterspørger oplysninger om personer, hvor det er berettiget, idet de som offentlig myndighed er underlagt krav om saglighed, lovmæssig forvaltning og det strafferetlige objektivitetsprincip.

For at afklare tvivlsspørgsmål opstiller vejledningen en række eksempler på lovlig udveksling af personoplysninger mellem både private aktører og politiet samt offentlige myndigheder og politiet. Gennemgående i eksemplerne er det afgørende for vurderingen af, om der lovligt kan videregives personoplysninger, at der ikke må være holdepunkter for at antage, at politiet skal bruge oplysningerne til andet end politimæssige opgaver. Der vil ikke være noget til hinder for, at den dataansvarlige vælger at indgå i en nærmere dialog med politiet med henblik på at opnå en afklaring af indholdet af anmodningen om oplysninger.

Læs hele vejledningen her: https://www.datatilsynet.dk/Media/F/2/Udveksling%20af%20personoplysninger%20med%20politiet.pdf

EU-Domstolen har afsagt dom om anvendelse af kommunikationsdata i straffesager

EU-Domstolen afsagde den 2. marts 2021 dom i sag C-746/18 mellem H.K. og Prokuratuur. Sagen angik en straffesag i Estland mod H.K. H.K. blev idømt en frihedsstraf på to år for tyveri, svindel og vold. Den estiske domstol baserede sin domsfældelse på trafik- og lokaliseringsdata, som efterforskningsmyndigheden havde indhentet fra en udbyder af elektroniske kommunikationstjenester.

Trafik- og lokaliseringsdataet gjorde det blandt andet muligt at spore og identificere kilden og bestemmelsesstedet for telekommunikationen. Det præjudicielle spørgsmål i sagen var derfor, om anvendelse af trafik- og lokaliseringsdata i forbindelse med mindre grove og alvorlige straffesager var i strid med artikel 15, stk. 1, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 ('direktiv om databeskyttelse inden for elektronisk kommunikation') sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder ('charteret'). Derudover blev EU-Domstolen bedt om at tage stilling til, hvorvidt det var i strid med disse bestemmelser, at den estiske anklagemyndighed havde kompetence til at give offentlige myndigheder adgang til trafik- og lokaliseringsdataet.

EU-Domstolen påpegede, med henvisning til sin tidligere praksis, at lagringen af dataet skulle være specifik og defineret. Anvendelsen af denne data krævede herefter, at hensynet til den almene interesse var varetaget, og at anvendelsen var proportional.

Under den aktuelle sag fandt EU-Domstolen, at anvendelsen af trafik- og lokaliseringsdata udgjorde et så alvorligt indgreb i de grundlæggende rettigheder, at det faktisk forfulgte formål i den nationale estiske lovgivning ikke var proportionalt. De nationale myndigheder måtte således kun benytte dette trafik- og lokaliseringsdata til at bekæmpe grov kriminalitet og til at forebygge alvorlige trusler mod den offentlige sikkerhed og ikke til at bekæmpe mindre straffesager som den forelagte. Varigheden af perioden for indhentelsen af oplysningerne spillede kun en rolle i det omfang, det skulle begrænses til, hvad der var strengt nødvendigt i efterforskningen.

Endelig vurderede EU-Domstolen, at kompetencen til at give offentlige myndigheder adgang til trafik- og lokaliseringsdata i forbindelse med strafferetlig efterforskning kun kunne gives af en domstol eller anden uafhængig myndighed. I denne sag havde den estiske anklagemyndighed kompetence hertil, og EU-Domstolen fandt det i strid med artikel 15, stk. 1, i direktivet om databeskyttelse inden for elektronisk kommunikation, sammenholdt med charterets artikel 7, 8 og 11 samt artikel 52, stk. 1, idet en anklagemyndighed ikke kunne anses som værende en uafhængig myndighed.

Læs hele dommen her: https://curia.europa.eu/juris/document/document.jsf?text=&docid=238381&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=1604536

Virksomhed idømt en bøde på 100.000 kr.

Byretten i Aarhus ('byretten') har den 12. februar 2021 idømt en virksomhed en bøde på 100.000 kr. for manglende sletning af kundeoplysninger i medfør af artikel 5, stk. 1, litra e i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') om opbevaringsbegrænsning. Sagen er den første danske straffesag mod en virksomhed for en overtrædelse af databeskyttelsesforordningen.

Det danske datatilsyn ('Datatilsynet') foretog i oktober 2018 et tilsyn hos virksomheden. Under tilsynet fandt Datatilsynet, at oplysninger om ca. 800.000 kunder burde have været slettet, da der ikke var en gyldig behandlingshjemmel for disse oplysninger. Oplysningerne lå i et gammelt system, hvor de ikke var blevet slettet, efter virksomheden havde implementeret et andet og nyere system. Datatilsynet indstillede på den baggrund virksomheden til en bøde på 1,5 millioner danske kr. Anklagemyndigheden fulgte Datatilsynets bødeindstilling og nedlagde påstand om en bøde på 1,5 millioner kr.

Under sagen blev det lagt til grund, at omkring 350.000 kundeoplysninger burde have været slettet. Oplysningerne omhandlede navn, adresse, telefonnummer, mailadresse og købshistorik.

Byretten idømte virksomheden en bøde på 100.000 kr., hvilket var en væsentlige mindre bøde, end hvad Anklagemyndigheden havde påstået. Ved afgørelsen lagde byretten især vægt på, at der var tale om en uagtsom overtrædelse af databeskyttelsesforordningen, at der var tale om en førstegangsovertrædelse, at de omhandlede oplysninger alene var almindelige oplysninger, at ingen registrerede havde lidt skade, samt at virksomheden havde bestræbt sig på at overholde databeskyttelsesforordningen i deres andre systemer.

Derudover blev bøden fastsat på baggrund af virksomhedens omsætning og ikke på baggrund af koncernens omsætning, som Datatilsynet havde lagt op til. Anklagemyndigheden har anket dommen.

Læs hele et resume af afgørelsen her: https://domstol.dk/aarhus/aktuelt/2021/2/selskab-idoemt-en-boede-paa-100000-kr/

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

Delphi

Linus Larsén

Reprimand till Spotify för att inte tillvaratagit registrerades rättigheter

I ett beslut från den 24 mars 2021 gav den svenska tillsynsmyndigheten Integritetsskyddsmyndigheten (IMY) en reprimand till musikstreamingtjänsten Spotify AB.[1] Bolaget fick reprimanden för att ha behandlat personuppgifter i strid med artikel 12.4 i GDPR och inte tillvaratagit en registrerads rättigheter på ett fullgott sätt.

Bakgrund

IMY inledde tillsynen mot Spotify mot bakgrund av ett klagomål från en enskild. IMY har under början 2021 meddelat att myndighetens strategi för de närmaste åren kommer vara mer inriktad på att fokusera på sådan tillsyn som bygger på klagomål från enskilda. Den klagande personen var boende i Danmark och ärendet lämnades över till den svenska tillsynsmyndigheten, som ansågs vara ansvarig tillsynsmyndighet enligt artikel 56 i GDPR.

Den klagande parten uppgav att han haft ett konto med betalprenumeration för Spotifys musiktjänster. Personen uppgav sedan att han bett Spotify ta bort hans kortuppgifter vid flera tillfällen. Enligt Spotify har klaganden registrerat sig via PayPal och bolaget behandlade därför inte klagandens kortuppgifter. Istället för kortuppgifter behandlar Spotify istället unika identifierare vid betalning via PayPal. Spotify argumenterade i ärendet för att den rättsliga grunden för behandlingen var ett berättigat intresse då de unika identifierarna som behandlas är nödvändiga för att förhindra missbruk av kostnadsfria provperioder från användare. Den unika identifieraren gav enligt Spotify möjlighet att identifiera ett unikt kreditkort, men innehöll inte uppgifter om kortnummer eller andra kortdetaljer och Spotify hade inte heller möjlighet att få tillgång till dessa detaljer. Baserat på nödvändigheten att behandla uppgifter för ett berättigat intresse, har Spotify nekat den klagande parten att ta bort den unika identifieraren för betalning.

IMY:s bedömning

IMY tolkar den klagandes begäran till Spotify som en invändning mot behandlingen enligt artikel 21.1 i GDPR. För att en behandling ska vara tillåten baserat på ett berättigat intresse efter en sådan invändning, måste avgörande berättigade skäl som väger tyngre än den registrerades intressen visas. I detta fall gjorde IMY bedömningen att sådana skäl finns och att Spotify kunde behandla uppgifterna, med tanke på behovet av att undvika missbruk och att uppgifterna som behandlats har minimerats genom användningen av den unika identifieraren istället för fullständig kortinformation.

IMY tog även ställning om Spotify hade hanterat förfrågan från den registrerade på ett korrekt sätt. Spotify hade i målet angett att begäran hade hanterats inom ramen för kundtjänsten utan inblandning av Spotifys dataskyddsteam och dataskyddsombud, då man inte formellt bedömt det som ett personuppgiftsrelaterat ärende fullt ut. Detta baserade man på att den klagande kunden inte uttryckligen hänvisat till personuppgifter och GDPR. IMY bedömer dock att detta måste stått klart för Spotify utifrån den klagandes begäran, och att Spotify i målet angett att man tolkat begäran som en invändning enligt artikel 21 enligt GDPR gör att omständigheterna talar ännu mer i den riktningen. IMY gjorde i sitt beslut bedömningen att eftersom Spotifys svar på invändningen var negativt för den klagade krävdes en motivering enligt artikel 12.4 i GDPR och en klagohänvisning, något som inte lämnats. Att sådan information framgår av bolagets integritetspolicy var inte tydligt nog. Sammanfattningsvis bedömde IMY att Spotify behandlat personuppgifter i strid med artikel 12.4 i GDPR.

IMY fann vid en samlad bedömning, bland annat baserat på Spotifys förklaring att situationen rörde sig om en engångshändelse inom ramen för många kundtjänstärenden och att kundtjänst fått ytterligare utbildning om personuppgiftsbehandling sedan dess, att det rörde sig om en mindre allvarlig överträdelse av GDPR. Bolaget fick därför en reprimand enligt artikel 58.2 b) i GDPR istället för en sanktionsavgift.

Avslutande kommentarer

Beslutet visar att IMY nu gör allvar av sin strategi att granska klagomål från enskilda i större utsträckning, samt behovet av att ha goda rutiner på plats för att hantera förfrågningar som rör registrerades rättigheter enligt GDPR. Samtidigt är beslutet ett exempel på att det inte alltid är nödvändigt och proportionerligt att utdela en sanktionsavgift, och att åtgärder som ytterligare utbildning om personuppgiftsbehandling för anställda kan utgöra en förmildrande omständighet.

Linus Larsén är senior associate i Advokatfirman Delphi, Stockholm.

1 Integritetsskyddsmyndighetens beslut DI-2020-10541 av den 24 mars 2021.

Gorrissen Federspiel

Tue Goldschmieding

EU-Domstolen har afsagt dom om krav om foranstaltninger mod framing af ophavsretligt beskyttede værker i licensaftale

EU-Domstolen afsagde den 9. marts 2021 dom i sag C-392/19 mellem VG Bild-Kunst og Stiftung Preußischer Kulturbesitz ('SPK'). Sagen angik et præjudicielt spørgsmål fra den tyske forbundsdomstol, Bundesgerichtshof, om fortolkningen af begrebet »overføring til almenheden« i artikel 3, stk. 1 i direktiv 2001/29/EF af 22. maj 2001 om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet ('InfoSoc-direktivet').

I første instans fandt retten i Berlin, at der ikke var tale om »overføring til almenheden« når et værk fra ét websted, hvor det med rettighedshaverens samtykke var frit tilgængeligt, blev indsat på en tredjemands websted ved hjælp af »framing«. Dette fandtes til trods for, at værket blev indsat på en sådan måde, at de beskyttelsesforanstaltninger mod framing, som rettighedshaveren havde iværksat, blev omgået.

Dommen blev efter appel ophævet af den regionale appeldomstol. Dommen blev efterfølgende appelleret til den tyske forbundsdomstol, der forelagde spørgsmålet om fortolkningen af begrebet »overføring til almenheden« i artikel 3, stk. 1 i InfoSoc-direktivet for EU-domstolen.

EU-Domstolen præciserede, at indsættelse af et værk på et websted ved framing, der med tilladelse fra rettighedshaveren er stillet til rådighed for almenheden på et andet websted kan udgøre overføring til almenheden. Det var tilfældet, hvis værket indsættes således, at de beskyttelsesforanstaltninger mod framing, som indehaveren har iværksat eller foranlediget iværksat, omgås.

Læs hele dommen her:
https://curia.europa.eu/juris/document/document.jsf?text=&docid=238661&pageIndex=0&doclang=da&mode=lst&dir=&occ=Hfirst&part=1&cid=1604536

EU-Domstolen giver Kommissionen medhold i appelsag mod VodafoneZiggo

EU-Domstolen afsagde den 25. februar 2021 dom i sag C-689/19 P mellem VodafoneZiggo Group BV ('VodafoneZiggo') og Europa-Kommissionen ('Kommissionen'). Sagen angik en appel af den nationale kendelse (T-660/18), hvori Retten fastslog, at en afgørelse ('den omtvistede retsakt'), der blev truffet af den nederlandske forbruger- og markedsmyndighed ('den nederlandske tilsynsmyndighed'), ikke havde bindende retsvirkninger og var af forberedende karakter. Retten mente derfor ikke, at afgørelsen kunne gøres til genstand for et annullationssøgsmål efter artikel 263 TEUF.

VodafoneZiggo gjorde gældende, at retten begik en retlig fejl ved at fastslå, at den omtvistede retsakt ikke havde bindende retsvirkninger. EU-Domstolen bemærkede dog, at rammedirektivets artikel 19, stk. 2, andet afsnit udtrykkeligt angiver, at en national tilsynsmyndighed kan undlade at følge en henstilling, hvis myndigheden underretter Kommissionen herom og begrunder sin beslutning. EU-Domstolen afviste derfor dette anbringende.

VodafoneZiggo påstod endvidere, at Retten begik en procedurefejl ved ikke at tage stilling til to argumenter, der havde afgørende betydning for vurderingen af sagen. EU-Domstolen afviste, at der forelå procedurefejl i begge tilfælde, da Retten ikke havde tilsidesat sin begrundelsespligt men havde begrundet forkastelsen af begge argumenter tilstrækkeligt.

Afslutningsvist gjorde VodafoneZiggo gældende, at Retten begik en retlig fejl, da den fastslog, at VodafoneZiggos grundlæggende ret til en effektiv domstolsbeskyttelse efter Den Europæiske Unions charter om grundlæggende rettigheders ('chartret') artikel 47 var blevet tilsidesat ved, at selskabets søgsmål blev afvist. EU-Domstolen afviste dette, da chartrets artikel 47 ikke har til formål at ændre den domstolskontrolordning, som var fastlagt i traktaterne. Derudover forpligter rammedirektivets artikel 4 medlemsstaterne til at indføre klagemekanismer, der gør det muligt at påklage afgørelser truffet af de nationale tilsynsmyndigheder, hvilket skaber en ordning, der sikrer en fuldstændig domstolsbeskyttelse.

På den baggrund forkastede EU-Domstolen appellen.

Læs hele dommen her:
https://curia.europa.eu/juris/document/document.jsf?text=&docid=238163&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=1610035

Salling Groups parallelimport og markedsføring af modetørklæder kunne ikke forbydes

Sø- og Handelsretten afsagde den 11. december 2020 dom i sag BS-33029/2020-SHR mellem dagligvarekoncernen Salling Group A/S (»Salling Group«) og Lala Berlin GmbH (»Lala Berlin«), der er producent af luksusmodeartikler. Sagen angik, hvorvidt Lala Berlin kunne forbyde Salling Group at udstille, markedsføre og sælge en række tørklæder og net fra Lala Berlin.

Først tog Sø- og Handelsretten stilling til, hvorvidt Salling Group, som påstået af Lala Berlin, havde solgt varemærkeforfalskninger af Lala Berlins tørklæder. Her fandt Sø- og Handelsretten, at dette ikke var sandsynliggjort og lagde bl.a. vægt på eksterne undersøgelser fra Teknologisk Institut og Antje D. Rauner, der professionelt beskæftiger sig med tekstiler og samarbejdede med Lala Berlin.

Dernæst tog Sø- og Handelsretten stilling til, om produkterne var sat i omsætning inden for EØS med tilladelse fra Lala Berlin, og om der således var sket konsumption af varemærketten efter Forordning (EU) 2017/1001 om EU-varemærker (»varemærkeforordningen«) artikel 15, stk. 1, forud for Salling Groups markedsføring og salg af produkterne. Sø- og Handelsretten lagde vægt på en advokaterklæring udarbejdet for Salling Group forud for dennes parallelimport af produkterne og fandt, at der var sket konsumption således, at Lala Berlin ikke kunne forbyde Salling Group at gøre brug af varemærket.

Slutteligt tog Sø- og Handelsretten stilling til om Lala Berlin havde rimelig grund til at modsætte sig fortsat markedsføring af produkterne, jf. varemærkeforordningens artikel 15, stk. 2. Lala Berlin henviste til, at den fortsatte markedsføring gennem dagligvarebutikker, såsom Bilka og Føtex, kunne skade varemærkets renommé væsentligt. Med henvisning til praksis fra EU-domstolen, udtalte Sø- og Handelsretten, at alvorlig skade på et varemærkes renommé kan ske, hvis forhandleren ved markedsføringen *»ikke har sørget for ikke at placere varemærket i omgivelser, der kan risikere alvorligt at forringe det image, som der er lykkedes indehaveren at skabe omkring sit varemærke.«* Da Salling Groups markedsføring var sket på samme måde, *»som man normalt markedsfører mærkevarer af samme art, og på en måde som må anses for sædvanlig i branchen«* og idet markedsføringen ikke adskilte sig *»væsentligt fra den markedsføring, som nogle af Lala Berlins autoriserede forhandlere«* benyttede, fandt retten, ikke at Lala Berlin kunne modsætte sig fortsat markedsføring af varerne med henvisning til varemærkeforordningens artikel 15, stk. 2.

Læs hele nyheden her:
https://www.domstol.dk/soeoghandelsretten/aktuelt/2020/12/konsumption-mv-ej-forbud/

Læs hele dommen her:
https://domstol.fe1.tangora.com/media/-300011/files/BS-33029-2020-SHR_-_Kendelse.pdf?rev1

Sø- og Handelsretten fandt at rettigheder til Alimakka-tasken ikke var krænket

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 22. december 2020 dom i sagen BS-4318/2020-SHR mellem Núnoo ApS ('Núnoo') og Noella Wholesale ApS m.fl. ('Noella'). Sagen omhandlede, om Noella havde krænket Núnoos rettigheder til 'Alimakka'-tasken ved salg og markedsføring af taskerne 'Caja' og 'Cecilia' efter lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov'), og om Noella havde misligholdt et forlig indgået af parterne.

Det indgåede forlig indebar, at Noella skulle ophøre med salg og markedsføring af Caja og Cecilia-taskerne, og at Noellas restlager af taskerne skulle destrueres. Efterfølgende lancerede Noella nye modeller af taskerne under samme navn. Núnoo rettede på denne baggrund henvendelse til Noella angående misligholdelse af forliget, og Noella ændrede efterfølgende navnene på taskerne til 'Celia' og 'Celina'. Núnoo mente imidlertid, at de nye tasker fortsat krænkede deres rettigheder til Alimakka-tasken, og at forliget derfor var misligholdt.

Alimakka-tasken nyder beskyttelse mod meget nærgående og slaviske efterligninger efter den danske markedsføringslovens § 3 om god markedsføringsskik. Sø- og Handelsretten fandt, at Noellas tasker adskilte sig kvalitets- og designmæssigt fra Alimakka-tasken på en sådan måde, at der ikke forelå en overtrædelse af den danske markedsføringslovens § 3. Dog fandt Sø- og Handelsretten, at Noella havde misligholdt forliget ved at have solgt dele af restlageret af Caja og Cecilia tasker i stedet for at destruere dem som aftalt. Sø- og Handelsretten frifandt derfor Noella for samtlige af Núnoos påstande, undtagen en forbudspåstand om videresalg af restlageret af Caja og Cecilia taskerne i overensstemmelse med forliget.

Læs hele dommen her:
https://domstol.fe1.tangora.com/media/-300011/files/BS-4318-2020-SHR_Dom.pdf

Sø- og Handelsretten har pålagt Telia forbud mod at formidle adgang til en hjemmeside, der krænkede Skechers varemærke- og ophavsrettigheder

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 23. december 2020 kendelse i sag BS-9735/2020-SHR mellem Skechers U.S.A., Inc. II ('Skechers') og Telia Danmark, filial af Telia Nättjänster Norden AB, Sverige ('Telia'). Sagen angik, hvorvidt Sø- og Handelsretten skulle forbyde og påbyde Telia at blokere adgang til hjemmesiden eeltdinida.com, der ifølge Skechers uberettigede benyttede Skechers varemærke og krænkede Skechers ophavsret til en række fotografier på hjemmesiden.

Det var ubestridt, at Skechers varemærke blev uberettiget anvendt på hjemmesiden eeltdindia.com. Imidlertid var parterne uenige, om Skechers havde ophavsret til de fotografier, der fandtes på hjemmesiden. Aktørerne bag hjemmesiden eeltdinida.com var ukendte, og både Skechers og Statsadvokaten for Særlig Økonomisk og International Kriminalitet ('SØIK') måtte opgive at identificere personerne bag hjemmesiden.

Sø- og Handelsretten fandt det imidlertid tilstrækkeligt bevist, at Skechers havde ophavsret til fotografierne på hjemmesiden, og at Telia derfor medvirkede til krænkelsen af Skechers varemærke- og ophavsrettigheder ved at give sine kunder adgang til hjemmesiden eeltdindia.com.

På den baggrund vurderede Sø- og Handelsretten, at betingelserne for et forbud efter lov nr. 938 af 10. september 2019 ('retsplejeloven') § 413, nr. 1 og 2 var opfyldt. Henset til at Skechers forgæves havde forsøgt hjemmesiden lukket på anden vis, og at nedlukningen ikke ville påføre Telia nogle væsentlige omkostninger, fandt Sø- og Handelsretten, at det var proportionalt at meddele Telia forbud mod at give sine kunder adgang til hjemmesiden eeltdindia.com. Telia blev også påbudt at foretage de nødvendige foranstaltninger, der var egnede til at forhindre kundernes adgang til internettjenesten på domænet samt andre domæner, hvoraf det krænkende indhold måtte fremgå.

Læs hele dommen her:
https://domstol.fe1.tangora.com/media/-300011/files/BS-9735-2020-SHR_Kendelse.pdf

Ompakning af lægemiddel var ikke en varemærkekrænkelse men udgjorde illoyal markedsfortrængning

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 9. marts 2021 dom i sag BS-4549/2020-SHR mellem Glenmark Pharmaceuticals Nordic AB ('Glenmark') og Celon Pharma Spółka Akcyjna (S.A.) ('Celon') mod Orifarm A/S ('Orifarm'). Sagen angik spørgsmålet om en varemærkekrænkelse mellem Orifarm som parallelimportør og Celon som indehaver af EU-varemærket, Salmex. Sagen angik også spørgsmålet om god markedsføringskik i forholdet mellem Orifarm som parallelimportør og Glenmark som indehaver af den originale markedsføringstilladelse.

I spørgsmålet om der forelå en varemærkekrænkelse, gjorde Celon for det første gældende, at Celon ikke havde fået en rimelig frist til at reagere på den af Orifarm påkrævede ompakning. Sø- og Handelsretten fastslog, at der foreligger en pligt for en parallelimportør til at underrette varemærkeindehaveren om, at det ompakkede produkt vil blive udbudt til salg. Dette er fastslået i EU-Domstolens dom af 23. april 2002 i C-143/00 (Boehringer I), præmis 61. Sø- og Handelsretten fandt, at Orifarms underretning af 1. november 2019 om, at produktet ville blive udbudt til salg den 18. november 2019, gav Celon en rimelig frist til at reagere.

For det andet gjorde Celon gældende, at ompakningen ville være skadelig for varemærket ved, at tillægsetiketten fremstod skæv og fejlplaceret, at der fremgik polsk tekst på bagsideetiketten, og at piktogrammet i indlægssedlen ikke viste det parallelimporterede produkt. Sø- og Handelsretten fastslog, at en varemærkeindehaver kan modsætte sig markedsføring af et lægemiddelsprodukt, hvis ompakningen kan være skadeligt for varemærket eller varemærkeindehaveren, jf. Domstolens dom af 26. april 2007 i sag C-348/04 (Boehringer II), præmis 40. Det var ikke godtgjort, at de af Celon fremførte grunde var af en sådan karakter, at de kunne skade varemærket.

I spørgsmålet om, hvorvidt der forelå en markedsføringskrænkelse, er det relevant, at Orifarms markedsføringstilladelse gjaldt et andet produkt end det faktisk markedsførte produkt. Tilladelsen var givet til et såkaldt »wide-bottomed-shaped« device, mens det faktiske produkt var et »parrot-shaped« device. På baggrund af dette vurderede Sø- og Handelsretten, at Orifarm havde markedsført produktet uden gyldig markedsføringstilladelse, og Orifarm var dermed erstatningsansvarlig over for Glenmark for illoyal markedsfortrængning.

Læs hele dommen her:
https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-4549-2020-SHR.pdf?rev1

EU-Kommissionens har offentliggjort resultaterne af »greenwashing«-screening af hjemmesider

EU-kommissionen og de nationale forbrugermyndigheder offentliggjorde den 28. januar 2021 deres årlige screening af hjemmesider. Gennemgangen viste, at tæt på halvdelen af de undersøgte online markeder indeholdte »greenwashing«.

»Greenwashing« er en betegnelse for en markedsføringsform, hvorefter en virksomhed ved brug af anprisninger giver forbrugeren et falsk indtryk af, eller vildledende oplysninger om, hvor miljøvenlige virksomhedens produkter er. EU-kommissionen og medlemsstaternes forbrugermyndigheder screener årligt hjemmesider på internettet og internettets onlinemarkeder med henblik på at gøre status på overholdelse af EU's forbrugerlovgivning. Screeningen fokuserer hvert år på ét specifikt område, og i år blev det undersøgt, om hjemmesider benyttede »greenwashing«.

EU-kommissionen og medlemsstaternes forbrugermyndigheder undersøgte 344 tvivlsomme anprisninger. Undersøgelserne viste overordnet, at der i 42 % af tilfældene var grund til at tro, at anprisningen kunne være falsk eller vildledende,

og derfor potentielt kunne udgøre en urimelig handelspraksis. De nationale forbrugermyndigheder skulle efterfølgende tage kontakt til de virksomheder, der havde brugt »greenwashing«. Virksomheder, der markedsfører sig selv eller deres varer som miljøvenlige, skal kunne dokumentere, at virksomheden overholder kravene til brugen af udsagnet. Hvis produktet ikke lever op til de miljømæssige anprisninger, kan der være tale om vildledende oplysninger, der vil udgøre en overtrædelse af forbrugerlovgivningen.

Resultaterne af screeningen vil indgå i en kommende konsekvensanalyse, der skal bruges i forbindelse med et nyt lovgivningsinitiativ inden for EU's forbrugerlovgivning.

Læs pressemeddelelsen her: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_269

Forbrugerombudsmanden har politianmeldt Toleadoo for at have krænket fire danske virksomheders varemærkerettigheder

Den danske forbrugerombudsmand ('Forbrugerombudsmanden') har den 4. februar 2021 politianmeldt den tyske leadvirksomhed, Toleadoo, der sælger kontaktoplysninger på potentielle kunder til virksomheder. Anmeldelsen omhandler uberettiget brug af varemærker og forretningskendetegn tilhørende de fire danske virksomheder, herunder Netto, Rema 1000, BabySam og Power i konkurrencer rettet mod danske forbrugere. Desuden har Forbrugerombudsmanden anmodet de tyske myndigheder om at gribe ind over for konkurrencerne, fordi de efter Forbrugerombudsmandens opfattelse er vildledende og udgør urimelig handelspraksis.

Varemærkerne blev vist i annoncer på Facebook og Snapchat, som ledte videre til hjemmesider med konkurrencer afholdt af Toleadoo. Ifølge Forbrugerombudsmanden gjorde konkurrencerne brug af virksomhedernes varemærker og forretningskendetegn på en sådan måde, at varemærkernes særpræg og renommé blev utilbørligt udnyttet og konkurrencerne var egnet til at fremkalde forveksling med de danske virksomheders forretningskendetegn, jf. lov nr. 88 af 29. januar 2019 ('den danske varemærkelov') § 4, stk. 2 og lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov') § 22.

Derudover er Forbrugerombudsmanden af den opfattelse, at det gennem annoncerne indhentede samtykke til at sende markedsføring ikke kunne anvendes af Toleadoo til lovligt at kontakte forbrugerne. Det ville være i strid med forbuddet mod uanmodet henvendelse, hvis deltagere i konkurrencerne kontaktedes med markedsføring, blot fordi de havde deltaget i en konkurrence.

Læs hele nyheden her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2021/forbrugerombudsmanden-griber-ind-over-for-brug-af-kendte-varemaerker-i-konkurrencer-paa-nettet/

Domænenavnet twitch.dk skulle overdrages til klageren

Det danske klagenævn for domænenavne ('Klagenævnet for Domænenavne') traf den 10. marts 2021 afgørelse i sag 2020-0339, mellem en privatperson ('klager') og Arcanite Media Ltd. ('indklagede'). Klagenævnet for Domænenavne fandt frem til, at domænet 'twitch.dk' skulle overdrages til klager.

Klager gjorde gældende, at indklagede havde registreret og opretholdt registreringen af domænenavnet alene med videresalg eller udlejning for øje i strid med § 25, stk. 2 i lov nr. 164 af 26. februar 2014 ('den danske domænelov'), mens indklagede gjorde gældende, at klageren ikke havde en legitim interesse i domænenavnet.

I relation til første spørgsmål fandt Klagenævnet for Domænenavne ikke, at klager havde godtgjort, at indklagede havde registreret eller opretholdt registreringen af domænenavnet »twitch.dk« alene med videresalg eller udlejning for øje i strid med den danske domænelovs § 25, stk. 2. Det omtvistede domæne indeholdte en hjemmeside med en række »relaterede links« og en kontaktformular til indehaveren af domænet. At indklagede havde indgået i dialog med klager om et muligt køb af domænet, og at indklagede desuden ejede et større antal domænenavne, kunne ikke føre til et andet resultat.

Klagenævnet for Domænenavne behandlede herefter, om indklagede havde overtrådt § 25, stk. 1 i den danske domænelov om god domænenavnsskik. Klager havde redegjort for sin interesse i domænenavnet til hobbybrug. Indklagede havde ikke forholdt sig nærmere til indholdet i klagen, hvilket Klagenævnet for Domænenavne tillagde vægt til fordel for klageren i overensstemmelse med Klagenævnet for Domænenavnes forretningsorden § 11 stk. 3. Klagenævnet for Domænenavne fandt, at indklagede ikke havde nogen legitim interesse i at kunne råde over domænenavnet. Indklagede skulle derfor overføre domænenavnet til klager.

Læs hele afgørelsen her: https://www.domaeneklager.dk/sites/default/files/2021-03/2020-0339%2C%20twitch.dk_.pdf

Domænenavnet kobe.dk skulle overdrages til klageren

Det danske klagenævn for domænenavne ('Klagenævnet for Domænenavne') traf den 8. januar 2021 afgørelse i sag 2020-0248 mellem KOBE ApS ('klager') og Digital Marketing Support ApS ('indklagede'). Klagenævnet for Domænenævnet fandt frem til, at domænet 'kobe.dk' skulle overdrages til klager.

Klager gjorde gældende, at indklagedes brug af domænenavnet stred imod god domænenavnsskik, jf. § 25, stk. 1 i lov nr. 164 af

26. februar 2014 ('den danske domænelov').

Til støtte herfor bemærkede klager, at klager havde en væsentlig interesse i overdragelsen af domænenavnet, da klager drev flere virksomheder under navnet 'KOBE', og at indklagede ikke havde ændret domænenavnets indhold væsentligt siden 2001 eller i øvrigt drev aktiv virksomhed. Domænenavnet havde i en periode været anvendt til at viderestille til domænenavnet 'dansk.net', men domænenavnet anvendes ifølge Klagenævnet for Domænenavnes undersøgelser ikke længere hertil.

På denne baggrund, og da indklagede ikke havde medvirket til sagens oplysning, fandt Klagenævnet for Domænenavne, at indklagede ikke havde nogen legitim interesse i at opretholde registreringen af domænenavnet 'kobe.dk'. Det var derf0r Klagenævnet for Domænenavnes opfattelse, at domænenavnet havde langt større interesse og værdi for klageren end for indklagede. Den interesseafvejning, som anvendelsen af reglen om god domænenavnsskik forudsatte, måtte derfor føre til, at en opretholdelse af indklagedes registrering ville indebære en overtrædelse af god domænenavnsskik, jf. den danske domænelovs § 25, stk. 1.

Læs hele afgørelsen her:
https://www.domaeneklager.dk/sites/default/files/2021-01/2020-0248%20kobe.dk_.pdf

3.1 Domænenavnet 'juridiskbistand.dk' skulle ikke overdrages til klageren

Det danske klagenævn for domænenavne ('Klagenævnet for Domænenavne') traf den 24. februar 2021 afgørelse i sag 2020-0225, mellem JuridiskBistand ApS ('klager') og en privatperson ('indklagede'). Klagenævnet for Domænenavne fandt frem til, at domænet 'juridiskbistand.dk' ikke skulle overføres til klager.

Klager gjorde gældende, at indklagede ikke måtte registrere og opretholde registreringer af domænenavne alene med videresalg eller udlejning for øje, jf. § 25, stk. 2 i lov nr. 164 af 26. februar 2014 ('den danske domænelov'). Til støtte herfor bemærkede klager, at domænenavnet tidligere var blevet tilbudt solgt til en lavere pris for overtagelsen af domænenavnet. Endvidere var indklagede registrant for 13 domænenavne, hvoraf kun et begrænset udvalg var aktive.

Klagenævnet for Domænenavne vurderede først, om der forelå en krænkelse af den danske domænelovs § 25, stk. 2, om registrering og opretholdelse af domænenavne alene med videresalg for øje. Klagenævnet for Domænenavne bemærkede, at indklagede ikke havde haft domænenavnet offentligt til salg og alene havde fremsat sit krav om betaling for overdragelse heraf, efter klageren rettede henvendelse til indklagede. På den baggrund fandt Klagenævnet for Domænenavne det ikke dokumenteret, at indklagede havde registreret eller opretholdt registreringen af domænenavnet alene med henblik på videresalg eller udlejning, hvorfor den danske domænelovs § 25, stk. 2 ikke fandtes overtrådt.

Endvidere fandt Klagenævnet for Domænenavne det ikke godtgjort, at klagerens interesser i det omtvistede domænenavn væsentligt oversteg indklagedes interesser, idet indklagede var uddannet erhvervsjurist og periodisk havde anvendt domænet aktivt til at yde rådgivning, ligesom der var blevet fremlagt en projektplan for domænets fremtidige brug. Klagenævnet for Domænenavne fandt derfor ikke, at der var sket overtrædelse af den danske domænelovs § 25, stk.1, om god domænenavnsskik.

Læs hele afgørelsen her:
https://www.domaeneklager.dk/sites/default/files/2021-03/2020-0225%2C%20juridiskbistand.dk%20-%20anonymiseret.pdf

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


Joel Tholin & Mariam Hussein

”Den andliga odlingens intressen” – det upphovsrättsliga klassikerskyddet inte tillämpligt när ett verk hade återgetts i oförändrat skick

Patent- och marknadsdomstolen meddelade nyligen dom i det uppmärksammade målet mellan Svenska Akademien och Nordiska motståndsrörelsen/Nordfront där det så kallade upphovsrättsliga klassikerskyddet för första gången var föremål för prövning i svensk domstol – drygt 60 år efter skyddets tillkomst.[1]

Bakgrunden till fallet var att Nordiska motståndsrörelsen/Nordfront på sin webbplats hade publicerat flera utdrag ur klassiska litterära diktverk av författare som bland annat Victor Rydberg och Esaias Tegnér. Utdragen hade, enligt Svenska Akademien, återgetts på webbplatsen i anslutning till kränkande material som bland annat utgjorde hets mot folkgrupp. Svenska Akademien väckte talan mot Nordiska motståndsrörelsen/Nordfront och yrkade att återgivningarna av verken skulle förbjudas då återgivningen enligt Akademien stod i strid med det upphovsrättsliga klassikerskyddet.

Rättsliga utgångspunkter

Upphovsrätten till ett skyddat verk gäller enligt svensk rätt från det att verket har skapats till och med 70 år efter upphovsmannens bortgång. Efter skyddstidens utgång får enligt huvudregeln var och en fritt förfoga över verket i ett upphovsrättsligt hänseende, utan exempelvis hänsyn till upphovsmannens ideella rättigheter till ett sådant verk. Det upphovsrättsliga klassikerskyddet, som återfinns i 51 § upphovsrättslagen, utgör emellertid ett undantag från denna huvudregel. Bestämmelsen uppställer vissa hinder mot återgivanden av verk som, efter upphovsmannens bortgång, anses kränka ”den andliga odlingens intressen”. Enligt nämnda bestämmelse får domstol, på talan av myndighet som regeringen utsett, vid vite meddela förbud mot ett sådant återgivande. Svenska Akademien är en av de som har tillerkänts sådan talerätt vad avser klassikerskyddet.

Patent- och marknadsdomstolens bedömning

Domstolen konstaterade inledningsvis att klassikerskyddet inte tillkommer samtliga verk, utan istället tar sikte på ”betydelsefulla litterära och konstnärliga verk” och att syftet var att sådana verk skulle skyddas mot grova förvanskningar. Vidare framhöll domstolen att klassikerskyddet är fristående från, och mer begränsat än, andra ideella rättigheter som den så kallade respekträtten som bland annat innebär att verk inte får göras tillgängligt i ”*sådant sammanhang*” att det skulle anses kränka upphovsmannens anseende.

I förarbetsuttalandena till bestämmelsen om klassikerskydd konstaterades att skyddet omfattning istället tog sikte på *bearbetningar, förändringar* eller *förvanskningar* av verket som sådant. Enligt domstolen fanns det därför inget i förarbetena som tydde på att ett återgivande av ett verk i *oförändrat skick* – med andra ord utan någon bearbetning, förändring eller förvanskning av verket, skulle kunna anses vara i strid med klassikerskyddet. Detta oberoende av vilket sammanhang verket hade återgetts i, och även om sammanhanget ur en allmänkulturell synpunkt skulle kunna framstå som stötande.

Sammanfattningsvis konstaterade domstolen att en återgivning i *oförändrat skick*, så som var för handen i fallet, därför inte ansågs vara en sådan återgivning som kunde anses kränka den ”andliga odlingens intressen” i strid med klassikerskyddet. Att genom en extensiv tolkning utsträcka skyddet, och således skapa ytterligare undantag från huvudregeln att ett verk efter skyddstidens utgång fritt kan utnyttjas, skulle enligt domstolen kunna få yttrande- och tryckfrihetsrättsliga konsekvenser som dels skulle vara svåröverblickbara, och dels i så fall skulle vara en fråga för lagstiftaren. Domstolen lämnade därför Svenska Akademins talan utan bifall.

Joel Tholin, Associate & Mariam Hussein, Associate, Bird & Bird Advokat.

1 Patent- och marknadsdomstolen dom av den 15 april 2021 i mål PMT 17286-19.


Simonsen Vogtwiig

Hedda Baumann Heier og
Emile Schjønsby-Nolet

Ny forskrift til åndsverksloven og lovforslag om gjennomføring av Marrakechtraktaten

Regjeringen la den 26. mars 2021 frem Proposisjon 115 LS (2020-2021). I Proposisjonen ber Regjeringen om Stortingets samtykke til å ratifisere Marrakech-traktaten om visse tillatte former for bruk av verk mv. for blinde eller andre personer med nedsatt synsevne eller leseegenskaper. Traktaten har også materialisert seg som EU-rett, og man har derfor samtidig spurt om godkjenning av EØS-komiteens beslutning om å innlemme Marrakechdirektivet (EU) 2017/1564 i EØS-avtalen. Gjennomføringen vil resultere i enkelte endringer i norsk rett.

Brorparten av gjennomføringene av forpliktelsene er fremlagt i ny forskrift til åndsverksloven, som ble sendt på høring 17. mars 2021. Gjennomføringen gir også enkelte kulturinstitusjoner, som biblioteker, adgang til å behandle persondata under GDPR. Den nye forskriften oppdaterer dessuten henvisninger til åndsverksloven av 2018, og er for øvrig i stor grad en videreføring av gjeldende rett.

Les Prop. 115 LS (2020-2021) på: *https://www.regjeringen.no/no/dokumenter/prop.-115-ls-20202021/id2839963/*

Les høringsnotatet for ny forskrift på: *https://www.regjeringen.no/no/dokumenter/horing-forslag-til-ny-forskrift-til-andsverkloven/id2838698/*

Dom forretningshemmeligheter fra lagmannsretten

Den 12. mars 2021 publiserte Frostating lagmannsrett sin avgjørelse i sak LF-2020-92904. Saken ble behandlet etter de nå opphevede bestemmelsene om forretningshemmeligheter i markedsføringsloven, men domstolen henter tolkningsmomenter fra den nye forretningshemmelighetsloven som trådte i kraft på nyåret. Momentene etter de gamle lovbestemmelsene må derfor antas å ha relevans for gjeldende rett.

Saken stod mellom tunellbransjeaktøren Devico AS og Aziwell AS. En nøkkelperson fra Devico hadde forlatt selskapet og startet sin egen bedrift. Begge selskapene er særlig spesialisert i kjerneboring. Den tidligere Devico-ansatte utviklet en drill for Aziwell i direkte konkurranse med sin tidligere arbeidsgiver. Sakens springende punkt var om utviklingen av «Azidrillen» var i strid med markedsføringsloven § 28, med den rettsvirkning at Devico kunne kreve forbud mot produksjon og salg av Azidrillen i tillegg til erstatning. De to hovedspørsmålene i saken var (i) hva som var omfanget Devico sine «bedriftshemmeligheter» og (ii) om Aziwell «rettsstridig» utnyttet disse.

For vurderingen av hva som faller inn under begrepet «bedriftshemmeligheter», var det på den ene siden klart at de to drillene hadde betydelige likhetstrekk, og var «basert på samme konsept» men var utviklet med «to forskjellige utviklingsløp». Begge bygget på en offentlig kjent teknikk. Kjernen i konflikten var om en bedriftshemmelighet må være knyttet til et konkretisert sluttresultat – i denne konteksten borene slik de fremstår og de konkrete tekniske løsningene i verktøyet – eller om også andre erfaringer og kunnskap som ledsager produktene kan utgjøre «bedrifthemmeligheter». Lagmannsretten kom til at slik akkumulert kunnskap og erfaringer, eller «sum av viten» i prinsippet *kan* utgjøre forretningshemmeligheter, men at det skal en del til. I den foreliggende saken ble summen av viten ble ansett som en bedriftshemmelighet etter en helt konkret vurdering, hvor det ble vektlagt at Devincodrillen var et teknisk krevende produkt med uvanlig stor ressursbruk. Lagmannsretten fastslo at «kunnskap fra flere års prøving og feiling» som kom på toppen av de allment kjente tekniske løsningene, og at kunnskapen ble forsøkt hemmeligholdt. Kunnskapen ble følgelig ansett som en bedriftshemmelighet etter § 28.

I vurderingen av om disse bedriftshemmeligheten har blitt rettstridig utnyttet, uttaler lagmannsretten at vurderingen beror på en avvenning mellom hensynene som begrunner vernet av bedriftshemmeligheter og hensynet til å spre informasjon, herunder innovasjon og karrieremuligheter for arbeidstakere. I denne konkrete vurderingen trakk lagmannsretten for det første frem at det ikke forelå direkte gjenbruk av informasjonen, ettersom løsningene var forskjellige. Likevel var det helt sentralt for Lagmannsretten at Aziwells opplevde en langt mer effektiv utviklingsprosess som følge av kunnskapen til nøkkelmannens tid i Devico. Dette ble ansett for å «overstige» det som anses som

alminnelig fagmannskunnskap. I tillegg var det sentralt at det forelå «subjektiv klanderverdig opptreden». Ved å gå ut av Devico og starte en egen direkte konkurrerende virksomhet, utviste nøkkelmannen «liten lojalitet». Samlet sett ble det derfor ansett å foreligge en «rettstridig utnyttelse».

Lagmannsretten kom derfor til at det forelå rettstridig utnyttelse av bedriftshemmeligheter i strid med markedslovens § 28 og i tillegg brudd på en skriftlig taushetserklæring. Lagmannsretten kom til at det likevel ikke var grunnlag for å ilegge et forbud, men utmålte erstatningen skjønnsmessig til fem millioner kroner.

Les hele avgjørelsen i Lovdatas database med saksnummer LF-2020-92904. I skrivende stund vites det ikke om avgjørelsen er anket til Høyesterett eller om den er rettskraftig.

Dom fra lagmannsretten om kjøp av konkurrenters varemerker som søkeord

Borgating lagmannsrett publiserte 15. april 2021sin avgjørelse i sak LB-2019-36567. Saken stod mellom Bank Norwegian på den ene siden og Brabank ASA, Ikano Bank Ab og Komplett Bank ASA på den andre siden. Google LLC og Hovedorganisasjonen Virke var partshjelpere på hver sin side. Saksforholdet i saken var i korte trekk at Bank Norwegian brukte konkurrentenes kjennetegn som betalte søkeord i søkemotorannonser på nett. Spørsmålet var om dette var i strid med kravet til god forretningsskikk i markedsføringsloven § 25.

Lagmannsretten slo først fast at «god forretningsskikk» er en rettslig standard som vil kunne endre seg dynamisk i takt med næringslivs- og samfunnsutviklingen. Om forholdet mellom generalklausulen i markedsføringsretten og varemerkeretten viste lagmannsretten til Rt. 1998 s. 1315 (Iskrem-dommen) som angir at generalklausulen i markedsføringsloven § 25 supplerer spesialbestemmelsene i markedsføringsloven og immaterialretten. Om generalklausulen skal anvendes i et tilfelle som også reguleres av en spesialbestemmelse, beror på en konkret vurdering der vurderingstemaet primært er *«om det foreligger elementer som ikke fanges opp av vedkommende spesialbestemmelse, og som hensynet til sunn konkurranse tilsier bør gis et vern som går ut over det som følger av spesialbestemmelsen»*, jf. Iskrem-dommen.

I avgjørelsen viser lagmannsretten til EU-domstolens praksis og konkluderer med at Bank Norwegian's annonsepraksis etter varemerkeretten er ansett som et uttrykk for sunn og lojal konkurranse, så sant det ikke foreligger en krenkelse av funksjonene til varemerket. Under henvisning til Iskrem-dommen mener lagmannsretten at det i et slikt tilfelle ville innebære dårlig sammenheng mellom regelverkene dersom den samme praksisen etter markedsføringsretten skulle bli ansett som rettsstridig.

Lagmannsretten var likevel enig med de ankende partene i at bruken av kjennetegnet til en konkurrent som betalt søkeord innebærer bruk av særpreg og renommé og at karakteristikken «snylting» således er treffende. Etter lagmannsrettens syn var dette elementet av snylting likevel ikke sterkt nok til at annonsepraksisen etter sin art alltid vil være i strid med «god forretningsskikk» etter markedsføringsloven § 25. Lagmannsretten utelukket likevel ikke at det etter en bredere vurdering kan tenkes at konkrete annonser kan være uttrykk for illojal konkurranse. Lagmannsretten fant etter en konkret vurdering at det ikke var sannsynliggjort.

Resultatet i avgjørelsen ble at Bank Norwegian vant saken fullt ut. Siden resultatet bød på noe tvil og gikk imot tidligere praksis fra Næringslivets Konkurranseutvalg, fant lagmannsretten at hver av partene måtte ta ansvaret for egne sakskostnader.

Les hele avgjørelsen i Lovdatas database med saksnummer LB-2019-36567. I skrivende stund er avgjørelsen ikke rettskraftig. For ordens skyld gjøres det oppmerksom på at andre advokater hos Simonsen Vogt Wiig representerte Bank Norwegian i saken.

Skrevet av senioradvokat Hedda Baumann Heier og advokatfullmektig Emile Schønsby-Nolet.

Gorrissen Federspiel

Tue Goldschmieding

Udvalg afgiver delbetænkning om gennemførelse af varedirektiv og direktivet om digitalt indhold

Et sagkyndigt udvalg nedsat af justitsminister Nick Hækkerup afgav delbetænkning om digital forbrugerbeskyttelse den 28. januar 2021. Delbetænkningen angår spørgsmålet om, hvordan Europa-Parlamentets og Rådets direktiv (EU) 2019 (771) om aftaler om salg af varer samt Europa-Parlamentets og Rådets direktiv (EU) 2019/770 af 20. maj 2019 om visse aspekter af aftaler om levering af digitalt indhold og digitale tjenester bør implementeres i dansk ret.

Formålet med direktiverne er at skabe klarhed over, hvornår en vare, digitalt indhold eller digitale tjenester har en fejl, og hvad forbrugeren i så fald kan kræve som følge af disse fejl. Implementeringen skal skabe tryghed for forbrugeren, når denne foretager grænseoverskridende e-handel. Implementeringen af direktiverne vil bl.a. medføre, at købelovens forbrugerbeskyttelse også vil gælde i tilfælde, hvor forbrugeren erhverver en digital ydelse ved »betaling« med personoplysninger i stedet for penge. Dette kan eksempelvis være tilfældet, hvor en forbruger afgiver personoplysninger ved oprettelsen af en konto på en streamingtjeneste. Hvis tjenesten ikke leveres som lovet, vil forbrugeren kunne kræve ny levering i overensstemmelse med aftalen eller kræve at ophæve aftalen.

Delbetænkningen indeholder for det første en gennemgang af de nugældende danske regler og direktiverne, og i den forbindelse en række overvejelser om, hvordan direktiverne kan implementeres i Danmark. For det andet indeholder delbetænkningen et konkret udkast til et lovforslag, der bl.a. vil medføre, at de regler, der gælder ved køb af fysiske varer på nettet, også vil gælde for køb af digitalt indhold og digitale tjenester. Det skal implementeres gennem en række ændringer til købeloven, hvor digitalt indhold, digitale tjenester og varer med digitale elementer nu adresseres direkte i lovteksten, og hvor lovens regler om forbrugerkøb vil finde udtrykkeligt anvendelse i forbindelse med køb af digitale tjenester og øvrigt digitalt indhold.

Delbetænkningen er sendt i høring og der forventes lovforslag fremsat i foråret 2021.

Læs hele nyheden her: *https://www.justitsministeriet.dk/pressemeddelelse/udvalg-afgiver-delbetaenkning-om-forbrugerbeskyttelse-i-en-digital-tidsalder/*

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

Nytt fra

LOVDATA

LOVDATA
PRO

Karnov Lovkommentarer – direkte integrert i Lovdata Pro

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

Noen av rettsområdene hvor de mest sentrale lovene blir dekket:

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

Skandinavisk tyngde

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

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

Tilgang krever egen avtale med Karnov Group Norway AS.

pro.lovdata.no

Produksjon: 07 Media AS