Lov & Data

Nr. 147
September 2021
Nr. 3/2021

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

AI Act – rätt sätt att reglera AI?

Artificiell intelligens (AI) spås förändra många delar av samhället i grunden. Redan idag används AI för att ställa medicinska diagnoser, minska energianvändningen, ta fram nya produkter och tjänster, effektivisera industriell produktion och förbättra kundservicen.

AI kan också användas till att förbättra produkters säkerhet och till att säkerställa skyddet för grundläggande rättigheter. Det kan handla om att förhindra olyckor i trafiken eller om att upptäcka och motverka cyberangrepp. Rätt utformade och använda AI-lösningar kan främja en demokratisk utveckling och t.ex. förhindra kränkningar av privatlivet som sker på sociala medier.

Samtidigt är AI-tekniken i sig förenad med risker. Om AI-system som används i självkörande fordon eller sjukvården fallerar kan det leda till sak- eller personskador. Om beslut fattas av bristfälliga AI-system kan individer utsättas för diskriminering eller felaktig hantering av personuppgifter.

I april 2021 presenterade Europeiska kommissionen ett förslag till en ny förordning om artificiell intelligens (ofta omtalad som ”AI Act”), som syftar till att skapa ett enhetligt europeiskt regelverk för att motverka denna typ av risker. Förslaget är mycket omfattande, men i korthet innebär det att ett antal uppräknade AI-tillämpningar, t.ex. vissa former

av realtidövervakning med hjälp av ansiktsigenkänning, förbjuds helt. Andra tillämpningar, t.ex. AI-system för rekrytering eller bedömning av studenter, klassificeras som ”högrisk-AI” och blir föremål för en omfattande och krävande reglering av ett slag som känns igen från dagens produktsäkerhetsreglering. Exempelvis ställs krav på ett riskhanteringssystem för AI-systemets hela livscykel och på hur data som används för maskininlärning väljs ut och hanteras. För vissa AI-användningar införs ett krav på transparens. Det gäller bl.a. system för känsloigenkänning och användningen av s.k. deep fakes. Förslaget innehåller därutöver bestämmelser om kraftfulla sanktioner och en särskild tillsynsordning.

Förslaget genomgår nu en analys och bearbetning i EU:s lagstiftnings-

maskineri. Jag ska här nöja mig med några kommentarer som rör den övergripande regleringsansatsen.

AI är idag inte oreglerat. Produkter som innehåller AI-teknik omfattas av generella och sektorsspecifika produktsäkerhetsregler, allmänna skadeståndsregler på nationell nivå och produktansvarsregler inom EU-rätten. Det finns därutöver regler som syftar till att skydda grundläggande rättigheter, t.ex. EU-regler om diskriminering och behandling av personuppgifter, som är relevanta vid utveckling och användning av AI. Det råder ingen tvekan om att dessa regler kan behöva uppdateras och kompletteras mot bakgrund av AI:s särskilda egenskaper, t.ex. systemens öppna och självlärande funktion och deras ”black-box”-karaktär.

Men frågan är om det är lämplig med en generellt tillämplig reglering för en så bred företeelser som AI. Hur hade det gått om vi på 1960-talet skapat en samlad reglering för att hantera alla typer av risker förknippade med datorprogram eller om vi på 1990-talet tagit fram en samlad reglering för att motverka riskerna med internet?

Till saken hör att AI Act inte skulle ersätta befintliga regleringar utan lägga sig som ett extra lager ovanpå dessa. På EU-nivå pågår för närvarande en översyn av bl.a. produktsäkerhetsregler och produktansvarsregler i ljuset av AI-utvecklingen. När det gäller skyddet för grundläggande rättigheter tycks dataskyddsreglerna och diskrimineringsreglerna kunna hantera många av riskerna, även om det kan krävas tydligare vägledning från tillsynsmyndigheterna och i vissa fall mindre ändringar i lagstiftningen. Enligt min mening är det lämpligare att först och främst genomföra denna översyn av det befintliga regelverket och bl.a. satsa på en modernisering av den sektorspecifika produktsäkerhetsregleringen. Först om detta anses otillräckligt finns de anledning att införa en generell reglering av AI-risker av alla olika slag.

När det gäller de rena förbuden mot vissa AI-system (t.ex. system för manipulation och massövervakning) och när det gäller de transparenskrav som föreslås menar jag vidare att kopplingen till AI i praktiken är svag. Det som föreslås regleras är snarare vissa beteende som inte anses önskvärda i samhället, alldeles oavsett om de möjliggörs med AI-system eller på annat sätt. I vissa fall är dessa beteenden redan i praktiken förbjudna, t.ex. för att den aktuella personuppgiftsbehandlingen strider mot dataskyddslagstiftning, men under alla förhållande kan en eventuell ny reglering ske på ett annat sätt än genom en samlad reglering som tar sikte på AI-system.

Den mycket vida definitionen av AI-system som tillämpas i förslaget gör att de flesta typer av moderna datorprogram kommer att omfattas av förordningen. De negativa konsekvenserna av den breda träffbilden hanteras i viss mån genom att den mest krävande materiella reglering begränsas till vissa uppräknade former av högrisk-AI. Men att på detta sätt svepa in en mängd företeelser och sedan materiellt reglera bara vissa är problematiskt. Dels ges EU-kommissionen, som enligt förslaget får rätt att ändra listan över högrisk-AI, stor makt över AI-utvecklingen, dels kan det uppstå en EU-rättslig spärreffekt mot ny nationell reglering som omfattas av förordningens grundläggande tillämpningsområde, men inte dess huvudsakliga materiella reglering. Den föreslagna regleringsansatsen kan därmed leda både till såväl översom underreglering av AI-system.

En annan potentiell svaghet i förslaget är dessa starka inriktning på tillhandahållare av AI-system samtidigt som den materiella regleringen starkt knyter an till ett AI-systems användning för vissa ändamål. Detta kommer att innebära en utmaning i förhållande till standardsystem för t. ex. maskininlärning som tas i bruk av en användare för ett visst ändamål. Förslaget innehåller visserligen även krav på användare av AI-system, men regleringens syfte kan knappast uppnås om regleringen av tillhandahållare i praktiken inte kan tillämpas. Samtidigt är det många gånger orimligt att se tillhandahållare av standardsystem som tillhandahållare av högrisk-AI-system trots att dessa saknar närmare kännedom om den tilltänkta användningen.

Avslutningsvis finns det anledning att påminna om vad som sagts i inledning: AI har också stor potential att motverka risker. Ett alltför ensidigt fokus på de risker som AI-system onekligen kan föra med sig kan mot denna bakgrund vara kontraproduktivt. Framtida regleringar som syftar till att motverka risker kan också innehålla krav på att välfungerande AI-lösningar faktiskt används.

Daniel Westman

Hvorfor fikk Amazon tidenes største GDPR-gebyr?

Av Ove A. Vanebo

Sommerens største nyhet på personvernfronten er at Amazon er ilagt et overtredelsesgebyr fra Luxembourgs databeskyttelseskommisjon, på rundt 7,8 milliarder norske kroner. Overtredelsesgebyret er forankret i EUs personvernforordning (omtalt som «GDPR» under), som også gjelder i Norge gjennom personopplysningsloven.[1]

Men hvorfor har selskapet fått denne reaksjonen? La meg prøve å gi et svar.

Foreløpig har mediene skrevet lite om bakgrunnen for rekordgebyret.

«Amazon har fått en bot på 746 millioner euro etter å ha brutt EUs regler for databeskyttelse», skrev Finansavisen, men utdypet ikke hvorfor.[2] *Computer-world nevnte kort at «Amazon er ilagt et forelegg på 746 millioner euro for regelbrudd», og at det «er ennå ikke klart hvorfor Amazon skal ha brutt GDPR-reglene».*[3]

Også Digi.no, som vanligvis er oppdatert på teknologinyheter, har kortfattet nevnt at den luxembourgske nasjonale kommisjon for databeskyttelse (CNPD) *«kom til at selskapets praksis ikke var i overensstemmelse med EU-regelverket (GDPR)».*

Uvanlig nok har det vært sped informasjonstilgang om hvorfor Amazon har fått gebyret, mens det vanligvis er en omfattende dekning i ulike medier når gebyrene er store. Hovedgrunnen er at Luxembourgs datatilsyn er underlagt taushetsplikt så lenge saken fremdeles er underlagt forvaltningsbehandling – og dette vil fortsatt gjelde hvis Amazon klager på avgjørelsen.

Heldigvis slipper vi å vente lenge for å få litt innsikt i saken, for allerede nå er det kommet ut spredte opplysninger som belyser saksforholdet. Mye er lite tilgjengelig og kun i fransk språkdrakt. Jeg vil derfor forsøke å samle noen tråder fra
materialet.

Bakgrunnen for saken i media

Bakgrunnen for at saken ble kjent er at Amazon.com, inc. sendte inn en innrapportering til *United States Securities and Exchange Commission*, i medhold av *Securities Exchange Act*

Ove A. Vanebo

av 1934.[4] I redegjørelsens note 4, nevnes kort at selskapet fra tid til annen involvert i saker om krav, saksanlegg/prosesser og rettstvister. Hva gjelder den konkrete saken, nevnes at:

> *«16. juli 2021 traff Luxembourgs nasjonale kommisjon for databeskyttelse ("CNPD") en avgjørelse mot Amazon Europe Core S.à rl, hvor det hevdes at Amazons behandling av personopplysninger ikke var i samsvar med EUs personvernforordning. Avgjørelsen*
> *ilegger et overtredelsesgebyr på € 746 millioner og tilhørende revideringer av praksis. Vi mener CNPDs beslutning er ugrunnet og har tenkt til å imøtegå avgjørelsen kraftig.»*[5]

Så vidt meg bekjent var Bloomberg først ute med et oppslag om

1 Personopplysningsloven § 1.

2 Pernille Frostad og Amund Reigstad/Finansavisen, Amazon brøt regler for databeskyttelse – får bot på over 7,8 milliarder, 30. juli 2021. Lest 20. august 2021: *https://finansavisen.no/nyheter/teknologi/2021/07/30/7712533/amazon-brot-regler-for-databeskyttelse-far-bot-pa-over-7-8-milliarder*

3 Stine Marie Hagen/Computerworld, Har fått rekordstor GDPR-bot, 30. juli 2021. Lest 20. august 2021: *https://www.cw.no/artikkel/gdpr/har-fatt-rekordstor-gdpr-bot*

4 Lest 18. august 2021: *https://www.sec.gov/ix?doc=/Archives/edgar/data/0001018724/000101872421000020/amzn-20210630.htm*

5 Min oversettelse.

saken den 30. juli.[6] I saken avviste Amazon på det sterkeste at det hadde forekommet behandling av personopplysninger i strid med GDPR, eller at det i det minste ikke er et brudd som utleverer personopplysninger: *«Det har ikke vært noe databrudd, og ingen kundedata har blitt synlige for tredjeparter»*. Det påpekes også at: *«Disse fakta [om at data ikke er utleverte] er ikke omstridte. Vi er sterkt uenige med CNDPs avgjørelse.»*

Da opplysningene ble kjent uttalte den franske personvernorganisasjonen *La Quadrature du Net* på sine nettsider[7] at avgjørelsen er en konsekvens av tidligere skritt organisasjonen og 10 000 personer tok i mai 2018, da det ble inngitt en kollektiv klage på Amazons praksis. *La Quadrature du Net* påpekte at bakgrunnen for klagen er det målrettede annonsesystemet som Amazon «påtvinger oss» ikke er basert på frivillig samtykke, noe som er et brudd på GDPR og øvrig personvernlovgivning.

Klagen fra la quadrature du net – hva går den ut på?

Fra 16. april til 27. mai 2018 inviterte *La Quadrature du Net* enhver person som er bosatt i Frankrike til å slutte seg til en kollektiv klage via sitt nettsted. Klagen skulle inngis til tilsynsmyndighetene i samsvar med GDPR art. 77, og *La Quadrature du Net* ba om fullmakt til å klage på personers vegne i henhold til art. 80. 10 065 mennesker som bruker Amazon-tjenester ga organisasjonen fullmakt til å klage på sine vegne.

Klagen er datert 28. mai 2018, og ligger offentlig tilgjengelig på organisasjonens nettsider.[8]

I klagens punkt 2.1 ble det vist til at GDPR krever rettslig grunnlag etter artikkel 6 nr. 1, som inneholder 6 såkalte behandlingsgrunnlag. Tre av grunnlagene ble antatt i prinsippet å kunne være relevante grunnlag: Den registrertes samtykke, oppfyllelse av en kontrakt med den registrerte, og den behandlingsansvarliges eller en tredjeparts berettigede interesser.

For så vidt gjelder samtykke viste *La Quadrature du Net* til at GDPR fortalepunkt 32 tilsier at samtykke forutsetter en aktiv handling: *«Taushet, forhåndsavkryssede bokser eller inaktivitet bør derfor ikke utgjøre et samtykke»*. Dette har også støtte i uttalelser fra EU-kommisjonens tidligere rådgivende organ, Artikkel 29-gruppen.[9]

Samtykket må heller ikke kreves inn i forbindelse med en situasjon

6 Stephanie Bodoni/Bloomberg, Amazon Gets Record $888 Million EU Fine Over Data Violations, 30. juli 2021. Lest 18. august 2021: *https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach*

7 La Quadrature du Net, Amazon fined 746 million euros following our collective legal action, 30. juli 2021 *https://www.laquadrature.net/en/2021/07/30/amazon-fined-746-million-euros-following-our-collective-legal-action/*

8 La Quadrature du Net, Réclamation contre Amazon Europe. Lest 20. august 2021: *https://gafam.laquadrature.net/wp-content/uploads/sites/9/2018/05/amazon.pdf*

9 Artikkel 29-gruppen, Guidelines on consent under Regulation 2016/679 (WP259.01), s. 16: «The GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example 'opt-out boxes').»

der samtykket er nødvendig for i det hele tatt å motta en tjeneste, eller i andre situasjoner der det foreligger et uakseptabelt press for å samtykke (ved f.eks. en negativ konsekvens ved ikke å samtykke). La Quadrature du Net viste i den forbindelse til en sak fra Frankrike fra 2017, der CNIL varslet et pålegg til Whatsapp om å slutte å dele ulike data om sine brukere med Facebook. Begrunnelsen var at overføringene var basert på et samtykke som ikke var frivillig, fordi *«den registrertes avslag på å gi samtykke til overføring av hans data nødvendigvis ville ha betydelige negative konsekvenser, siden han blir tvunget til å slette kontoen sin og ikke vil kunne bruke WhatsApp-applikasjonen»*.[10]

Videre ble det vist til prinsippene om rettferdighet, lovlighet og åpenhet i artikkel 5 nr. 1 bokstav a, og at den registrerte har rett til å trekke sitt samtykke når som helst, jf. GDPR art. 7 nr. 3. I praksis ville retten til å trekke samtykket bli mer illusorisk med løsningen Amazon hadde lagt opp til.

Hva gjelder alternativet om behandling av personopplysninger i medhold av kontraktsoppfyllelse (GDPR art. 6 nr. 1 bokstav b), ble det vist til at ikke enhver opplysningsbehandling nevnt i kontrakten er nødvendig for å «oppfylle» den i henhold til GDPR.[11] Behandlingen må være nødvendig for å oppfylle kontrakten med den registrerte, ved at det er en direkte og objektiv kobling mellom behandlingen av data og formålet med utførelsen av kontrakten. Dette er også lagt til grunn i en uttalelse fra Personvern-rådet etter at klagen ble utformet.[12]

Ulike former for adferdsanalyse og reklameformål kan ifølge La Quadrature du Net neppe forankres i en kontrakt slik Amazon tilsynelatende har lagt til grunn.

Behandlingsgrunnlaget i GDPR art. 6 nr. 1 bokstav f, «berettigede interesser», antas også å være uaktuelt. La Quadrature du Net påpeker at behandlingen Amazon bedriver i
hovedsak vil være regulert av kommunikasjonsverndirektivet.[13] Nevnte direktiv ble endret ved endringsdirektivet *«The Citizen's Rights Directive»*,[14] slik at tilgang til og oppbevaring av informasjon om brukerne neppe kan understøttes av
berettigede interesser, men må forankres i et samtykke.

La Quadrature du Net avslutter klagen ved å kreve følgende to tiltak mot Amazon:

Forbud mot atferdsanalyse og målrettet annonsering som beskrevet, i henhold til GDPR artikkel 58 nr. 2 bokstav f.

Ileggelse av et overtredelsesgebyr som skal være «så stort som mulig», på grunn av «den massive, varige og åpenbart forsettlige karakteren av overtredelsen som har funnet sted», jf. GDPR artikkel 83 nr. 2 og 5.

Oppdateringer som kommenterer saken

I et brev av 2. august ble *La Quadrature du Net* informert av det franske datatilsynet («CNIL») i samsvar med GDPR artikkel 77.[15] I beslutningen fra CNPD, slik den beskrives i brevet fra CNIL, konstateres det brudd på flere ulike forpliktelser.

For det første er CNPD enig med klagerne i at det mangler et rettslig grunnlag etter artikkel 6 nr. 1 for behandlingen av personopplysninger i forbindelse med målrettet reklame.

For det annet påpekes det at Amazon også må sørge for å få behandlingen av personopplysninger i samsvar med åpenhetskravene i artiklene 12, 13 og 14. Disse krever blant annet at det skal oppgis hva formålet med opplysningsbehandlingen er, hvem informasjonen utleveres til, og hva slags rettslig grunnlag Amazon har for behandling av personopplysninger.

For det tredje må Amazon følge opp og svare personene som får informasjon om seg selv brukt i markedsføringsøyemed ved enhver forespørsel om tilgang, retting eller sletting av personopplysninger – i samsvar med artiklene 15 til 17 i GDPR.

Interessant nok, som et fjerde punkt, vises det til at Amazon også må sørge for å få på plass en mekanisme for å ivareta «retten til å protestere» etter GDPR artikkel 21. Litt enkelt sagt innebærer «retten til å protestere» at en protest mot opplysningsbehandlingen vil stanse Amazons adgang til å bruke personopplysningene – med mindre nærmere bestemte grunner taler for fortsatt behandling. Denne retten skal ifølge CNDP gjelde alle aspekter ved den målrettede markedsføringen.

Det fremheves også at Amazon har 6 måneder på seg til å rette opp

10 Commission Nationale de l'Informatique et des Libertés, Décision n° MED-2017- 075 du 27 novembre 2017 mettant en demeure la société WHATSAPP.

11 Artikkel 29-gruppen, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, s. 16-17.

12 Personvernrådet, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, s. 11 og 14.

13 Europaparlaments- og rådsdirektiv 2002/58/EF om behandling av personopplysninger og beskyttelse av privatlivets fred innen området for elektronisk kommunikasjon.

14 Endringsdirektiv 2009/136/EF vedtatt 25. november 2009.

15 Commission Nationale de l'Informatique et des Libertés, Saisine n°18010725 (a rappeler dans toute correspondance), 2. august 2021. Lest 20. august 2021: *https://www.laquadrature.net/wp-content/uploads/sites/8/2021/08/CNIL_CLP211124.pdf*

bruddene på GDPR, dvs. avslutte annonsemålretting eller få frivillig samtykke til det; utover denne perioden må Amazon betale et gebyr på 746 000 euro per dags forsinkelse.

Omtrent samtidig med brevet, offentliggjorde også CNIL selv at Amazon (ved selskapet Amazon Europe Core) får gebyret med grunnlag i klagen fra *La Quadrature du Net*. Både brevet av 2. august og uttalelsen påpeker at CNIL oversendte klagen til CNDP, og at disse tilsynsorganene har samarbeidet tett med saken.[16]

La Quadrature du Net oppdaterte sitt eget oppslag på nettsiden 4. august, som kort oppsummerer saken slik den fremstilles i CNILs brev.[17]

16 Commission Nationale de l'Informatique et des Libertés, L'autorité luxembourgeoise de protection des données a prononcé à l'encontre d'Amazon Europe Core une amende de 746 millions d'euros. Lest 18. august 2021: *https://www.cnil.fr/fr/lautorite-luxembourgeoise-de-protection-des-donnees-prononce-lencontre-damazon-europe-core-une*

17 Se note 7.

Hva nå for amazon (og andre aktører)?

Amazon har som nevnt fått en frist for å oppfylle kravene i GDPR, med forsinkelsesgebyrer om selskapet ikke følger opp. Selskapet har selv avvist at det er skjedd et sikkerhetsbrudd eller at det er utlevert personopplysninger til uvedkommende, og kommer sikkert til å påklage gebyret.

Så lenge alle klagemuligheter ikke er brukt opp, er det som nevnt i samsvar med luxembourgsk lov fremdeles hemmelighold av selve avgjørelsen. Den vil imidlertid senere bli publisert på CNPDs nettsider.

De siste årene har ulike former for markedsføring på internett blitt gradvis vingeklippet gjennom tydelige dommer fra EU-domstolen. I Planet49-saken ble det tydeliggjort at forhåndsavkryssede felter som aksepterer markedsføring på nett er problematisk, og at det er strenge krav til samtykke for cookies o.l.[18] En tilbyder av mobiltjenester fikk i *Orange România*-saken[19] reaksjoner for å legge til grunn at klausul om samtykke til opplysningsinnsamling i tjenestekontrakt, var gyldig samtykke. I juni ble det fremlagt en uttalelse fra generaladvokaten som trolig vil innebære en innstramning av annonsemeldinger i tilknytning til epostkasser.[20]

Det vil ikke overraske meg om Amazon-saken går helt til topps i EUs domstol. Inntil da, får alle personverninteresserte håpe på nye lekkasjer om saken.

Ove A. Vanebo, assosiert partner i Kluge Advokatfirma

18 EU-domstolens sak C-673/17.

19 EU-domstolens sak C-61/19.

20 I forbindelse med EU-domstolens sak C-102/20 (StWL Städtische Werke Lauf ad Pegnitz GmbH).

Ulike vern og mekanismer for beskyttelse av data

Av Silje Strandengen
og Stian Hultin Oddbjørnsen

Silje Strandengen

Stian Hultin Oddbjørnsen

«Eg har masse data, eg har masse gåter», synger Lars Vaular på låten Big Data. Det samme gjelder de fleste virksomheter. Bedrifter blir derfor stadig mer opptatt av sine egne data og hvordan disse kan anvendes for å skape verdifull innsikt og innovasjon. Utvikling av kunstig intelligens og maskinlæring bidrar til å gi potensiell stor merverdi knyttet til bedriftens data. Data er innenfor kunstig intelligens den kritiske komponenten, da dagens kunstig intelligente systemer er avhengig av maskinlæringsteknikker som krever enorme mengder treningsdata. På denne måten er data en så essensiell del av kunstig intelligens, at data i seg selv er et verdifullt gode som bedrifter bør verne om. Det er treffende å slå fast *«an algorithm is, at the end of the day, only as good as its data»*.[1] I forlengelse av dette er det i juridiske og politiske fora stilt spørsmål om mulige *beskyttelsesmekanismer* for data, herunder også eierskap til data.

1 Lehr, David og Paul Ohm. «Playing with the Data: What Legal Scholars Should Learn About Machine Learning. » (2017) s. 677.

Dataens mangfoldighet gjør at det er vanskelig å se for seg ett enkelt rammeverk for regulering og beskyttelse av data.[2] En definisjon av data skal vi ikke begi oss ut på, men artikkelen konsentrerer seg om kommersielle data, og det avgrenses mot enhver form for persondata som reiser helt egne problemstillinger. En lenge pågående tautrekking har handlet om eierskap og beskyttelse av data på den ene siden, og størst mulig tilgang til data på den andre. EU-kommisjonen identifiserte begge disse problemstillingene da de i forbindelse med implementeringen av et digitalt indre marked, fremla arbeidet vedrørende «building a data economy» i mai 2015.[3] Kommisjonen betegner data som *«en katalysator for økonomisk vekst, innovation og digitalisering i alle økonomiske sektorer […] og i samfundet som helhed»*.[4] Arbeidet resulterte likevel ikke i et eget regelverk for data, og i spørsmålet om beskyttelse av – eller eierskap til – data, faller en derfor tilbake på eksisterende lovverk. Det er flere innfallsvinkler og mulige lovverk i forbindelse med rettigheter til data, men sentralt står ulike deler av immaterialretten som potensielt kan gi beskyttelse til bedrifters verdifulle data.

I denne artikkelen vil vi derfor ta for oss spørsmålet om deler av

2 WIPO Conversation on Intellectual Property (IP) and Artificial Intelligence (AI). Revised Issues Paper on Intellectual Property Policy and Artificial Intelligence (2020) s. 10.

3 Se blant annet COM 2015 192 final.

4 COM 2015 192 final s. 15.

immaterialrettens beskyttelse av data, herunder opphavsretten og databasevernet. Vi ser også på vernet for forretningshemmeligheter i sammenheng med databeskyttelse. Enhver immaterialrettslig beskyttelsesmekanisme har egne regelsett og vilkår, og bruk av disse regelsettene på data kan medføre komplekse analyser der loven kan være både uklar og usikker. Den rettslige usikkerheten innebærer at kontraktsreguleringer gjerne spiller den største rollen i praksis, hvor både tilgang og rettigheter til bruk av data reguleres. Derfor vil vi endelig ta for oss kontraktsrettens betydning, herunder hvilke spørsmål som kan oppstå i forbindelse med utarbeidelse av kontrakter om rettigheter til data.

Databasevernets beskyttelse av data

Opphavsrettens databasevern er nok det nærmeste en kommer en direkte regulering av – og beskyttelse for – ikke-personlige data. Vernet gjør seg særlig gjeldende da det ikke er hvert enkelt datapunkt *i seg selv* som nødvendigvis er det mest verdifulle, men heller samlinger av større mengder data. Både generelt innenfor kunstig intelligens, men også Big Data-analyser, er det nettopp algoritmenes mulighet for å analysere store og komplekse datasett, som er det sentrale. Databasevernets beskyttelse for samlinger av data er derfor et naturlig utgangspunkt for spørsmålet om ulike beskyttelsesmekanismer for data.

Databaser er regulert og definert i direktiv 96/9 EF om rettslig vern av databaser (databasedirektivet) som en samling av verk, data eller annet selvstendig materiale som er strukturert systematisk eller metodisk, hvorav innholdet i databasen kan konsulteres individuelt.[5] I tråd med dataenes mangfoldighet, som ble nevnt innledningsvis, kan databasevernet bestå av samlinger av litterære, kunstneriske eller musikalske verk, herunder også annet materiale som tekst, lyd og bilde.[6] Dette er i tråd med EUs nye direktiv 2019/790 om opphavsrett i det digitale indre marked (digitalmarkedsdirektivet) sine eksempler på data som informasjon i digital form, nemlig tekst, lyd og bilde.[7]

Åndsverkloven gir på lik linje med databasedirektivet en enerett til den som fremstiller en database hvor *«innsamling, kontroll eller presentasjon av innholdet innebærer en vesentlig investering».*[8] Det er således tale om et investeringsvern, hvorav bruk av penger, tid, innsats og faglig kompetanse medgått til opprettelsen av databasen kan gi vern, dersom investeringene er vesentlige. Eneretten omfatter videre det å *«råde over hele eller vesentlige deler av databasens innhold ved uttrekk fra eller gjenbruk av databasen».*

I denne forbindelse skal ikke «databasens innhold» forstås dithen at databasevernet gir et rent innholdsvern, i den forstand at de enkelte data i seg selv har vern.[9] Det gis et vern mot uttrekk eller gjenbruk av hele eller vesentlige deler av de data som databasen består av. Databasevernet må på denne bakgrunn anses som en sentral beskyttelsesmekanisme for store datasett eller databaser, herunder data, særlig for bedrifter som benytter seg av teknologi basert på kunstig intelligens og maskinlæring.

Databasevernets relevans i den moderne dataøkonomien har imidlertid vært gjenstand for mang en diskusjon, og databasedirektivet har blitt evaluert to ganger av EU-kommisjonen selv. Den 25. april 2018 fremla EU-kommisjonen sin siste evaluering av databasevernet, og i forlengelse av denne evalueringen ble det også utferdiget en støtterapport til kommisjonens evaluering skrevet av en ekspertgruppe. Evalueringens hovedformål var å vurdere direktivets effektive håndhevelse, relevans og verdi i en stadig mer datadrevet økonomi. Til tross for at flere i teorien har uttalt sin skepsis vedrørende databasevernet og dets anvendelse innenfor den moderne dataøkonomien, konkluderer både kommisjonen og ekspertgruppen med at databasevernet fortsatt er relevant.

Skepsisen har i stor grad sirkulert rundt fire avgjørelser fra EU-domstolen avsagt tilbake i 2004. EU-domstolen presiserte i alle fire dommene rekkevidden av databasevernet, herunder hva som ligger i begrepene innsamling, kontroll og presentasjon av databasens innhold. Dommene omhandler to parallelle sakskompleks om rettighetene til henholdsvis kampprogrammer (Fixtures-dommene), og en database for hesteveddeløp (William Hill).[10] Begrepet investering skal i forbindelse med innsamling av en databases innhold etter databasedirektivet artikkel 7 (1), forstås slik at det omfatter investeringer som vedrører opprettelsen av databasen. Dette omfatter investeringer *«der anvendes til fremskaffelsen af eksisterende materiale og til samlingen heraf i den nævnte database, med omfatter ikke midler, der anvendes til frembringelse af de bestanddele, der udgør en databases indhold».*[11] Den prinsipielle betydningen av dette er at innsamlingsbegrepet må avgrenses mot produksjon og frembringelse av nye data, slik at investeringer som går med til slik produksjon ikke er relevant.

Avgrensningen mot produksjon av data kan ha en bred innvirkning på beskyttelsen av data i den moderne dataøkonomien. Den nye

5 Databasedirektivet artikkel 1 (2).

6 Databasedirektivets fortale punkt 17.

7 Digitalmarkedsdirektivets fortale punkt 8. Direktivet er ikke gjennomført i norsk rett når denne artikkelen skrives.

8 Åndsverkloven § 24 jf. databasedirektivet artikkel 7.

9 Rognstad, Ole-Andreas. «Opphavsrett.» (2019) s. 398.

10 C-46/02 Veikkaus, C-338/02 Svenska Spel, C-444/02 OPAP og C-203/02 William Hill.

11 C-46/02 Veikkaus avsnitt 34.

datateknologien er avhengig av prosesser som innebærer de allerede nevnte fenomenene kunstig intelligens, maskinlæring og Big Data, for ikke å glemme IoT. Det all denne nye teknologien har til felles, sammenholdt med databasevernet, er at det kan være vanskelig å skille mellom generering av data og innsamling av data. I hvilken grad databasevernet faktisk kan verne om data i en slik kontekst, gjenstår derfor å se.

Når det er sagt, er det ingen automatikk i at databasevernet er utelukket som beskyttelsesmekanisme i de tilfeller hvor den som fremstiller en database, også produserer dataen som senere inngår i databasen. Utfordringen er imidlertid å vise til vesentlige investeringer medgått til innsamling, kontroll og presentasjon av databasens innhold, som er uavhengige av eventuelle investeringer medgått til produksjon av dataen som inngår i samlingen. Det er uansett fremholdt i teorien at det kan være vanskelig å oppfylle kravet til vesentlig investering i dagens dataøkonomi, da prosessene med å samle inn, kontrollere og presentere data skjer mer og mer ved hjelp av automatiserte datametoder.

Det er også vårt syn at databasedirektivet, slik det ble lovfestet i 1996, ikke imøtekommer den tekniske utviklingen, samt at direktivet ikke verner om de mulighetene som er forelagt oss i dag vedrørende arbeid med data. I tillegg til ren produksjon av nye data, er det for eksempel usikkert hvorvidt arbeid med å *behandle* data stiller seg til kriteriene innsamling, kontroll og presentasjon. I forkant av maskinlæring vil en eksempelvis gjerne berike, oppdele eller homogenisere dataene i et datasett før algoritmene skal trekke erfaringer fra dataen. Det fremstår høyst usikkert om databasevernet omfatter slike dataaktiviteter.

Opphavsrettslig beskyttelse av data

Slik det ble presisert innledningsvis finnes det så langt ingen særrettigheter til data som sådan, og i et opphavsrettslig perspektiv kan data kun være beskyttet så lenge det foreligger et originalt verk. Lydfiler som utgjør et musikkverk, kan derfor være beskyttet som individuelle digitale data, dersom musikkverket gir uttrykk for original og individuell skapende åndsinnsats.

Det er likevel ikke opphavsrettslig beskyttelse av enkeltstående verk som er det mest sentrale under det overordnede spørsmålet om beskyttelse av data. For i tillegg til databasevernet som en nærstående rettighet etter åndsverkloven § 24, kan en database også beskyttes som et åndsverk. Dette følger uttrykkelig av databasedirektivet, og det ble innenfor norsk rett konstatert av departementet ved implementeringen av data-

basedirektivet.[12] Det opphavsrettslige vernet av databaser går ut på at sammenstillingen av data må være preget av individuell skapende virksomhet.

EU-domstolens sak C-604/10 (Football Dataco I) presiserer kravet om individuell skapende åndsinnsats for sammenstillinger, hvorpå det er utvelgelse, strukturering, sortering og planlegging av databasens materiale som er det avgjørende. Herunder må fremstillere av databaser foreta frie og kreative valg ved utvelgelsen av data, eller ved struktureringen av disse.

Det er to klare konsekvenser som følger av EU-domstolens uttalelser i C-604/10, som kan ha betydning for hvorvidt datasamlinger kan nyte opphavsrettslig vern. For det første foreligger det ikke tilstrekkelig frihet og kreativitet dersom databasen er diktert av tekniske hensyn, regler eller begrensninger.[13] Det skal heller ikke vektlegges om opprettelsen av databasen har nødvendiggjort en betydelig arbeidsmengde eller kunnskap fra opphaverens side, med mindre dette arbeidet eller kunnskapen uttrykker noen form for originalitet ved utvelgelsen eller struktureringen av dataen.[14] Det er på denne bakgrunn ingen andre vilkår enn originalitet ved sammenstillingen av dataen, som kan gi opphavsrettslig beskyttelse.[15]

Det er selve presiseringen av det opphavsrettslige databasevernet som skaper problemer for hvorvidt vernet er egnet til å beskytte data i forbindelse med dagens datadrevne teknologi. Arbeidet med data, særlig store datamengder, vil sjelden innebære slike frie og kreative valg. Det vil snarere tvert imot være tekniske hensyn som ofte vil være styrende, all den tid en database i seg selv er en teknisk innretning som gjerne inngår som en del av større teknologiprosjekter. Graden av tekniske hensyn vil følgelig variere ut ifra formålet med databasen, og hva slags type data det er tale om.

Dette må imidlertid ikke forstås dithen at originalitetskravet har en høyere terskel for databaser enn andre typer verk, men databasen som verkstype *kan* gjøre det vanskeligere å oppfylle originalitetskravet og dets innhold. Økende grad av automatiserte dataprosesser for innsamling og strukturering av data kan samtidig utvaske det opphavsrettslige vernet av databaser i fremtiden, da det kan innebære at det blir umulig å vise til en original skapende åndsinnsats. I motsetning til databasevernet som er et investeringsvern, er åndsverkvernet nemlig avhengig av *menneskelig* skapervilje for å oppfylle originalitetskravet. Maskiner og programvare har per i dag, ikke disse egenskapene.

Data som forretningshemmeligheter

Databasevernet og opphavsrettslig vern av sammenstillinger av data gir mulighet til å kontrollere bruk av bedrifters data, og kan bidra til å oppnå markedsfordeler ved eneretter til egne data. Vernet av forretningshemmeligheter skal på sin side beholde bedriftens kommersielle verdifulle *informasjon* konfidensiell eller hemmelig. Innsatsen som er lagt ned i å generere bedriftens kunnskap og informasjon, kan på denne måten gi konkurransefortrinn ved at utenforstående ikke kan få tilgang til dataen eller informasjonen. I motsetning til både databasevernet og opphavsretten, kan vernet for forretningshemmeligheter gi beskyttelse til individuelle data, og ikke bare samlinger av data. Vernet skiller heller ikke mellom innsamling av data, eller produksjon. Det er således selve *informasjonen* som dataen gir uttrykk for som er gjenstand for beskyttelse, ikke måten dataen er organisert på eller investeringer medgått i fremstillingen av dataen.

Vernet for forretningshemmeligheter er regulert i EUs direktiv 2016/943 om beskyttelse av fortrolig know-how og forretningsopplysninger mot rettsstridig tilegnelse, bruk og formidling. Den nye loven om vern av forretningshemmeligheter (forretningshemmelighetsloven) av 1. januar 2021 gjennomfører direktivet. Lovens formål er å *«sikre innehavere av forretningshemmeligheter vern mot urettmessig tilegnelse, bruk og formidling av hemmeligheten».*[16]

Forretningshemmeligheter er ifølge lovens § 2 opplysninger som er hemmelige, har kommersiell verdi fordi de er hemmelige, eller det er truffet rimelige tiltak for å holde opplysningene hemmelige.[17] For at data skal være beskyttelsesverdig under forretningshemmelighetsloven, må det derfor være data som utgjør hemmelig informasjon. Forretningshemmelighetsdirektivet nevner særskilt *handelsdata*, eksempelvis opplysninger om kunder og leverandører, forretningsplaner, samt markedsundersøkelser- og strategier.[18]

I konteksten av teknologier som maskinlæring og Big Data, kan forretningshemmelighetsvernet potensielt gi beskyttelse til alle opplysninger og data, så lenge dataen oppfyller beskyttelseskravene som vist til ovenfor. Det er likevel krav som kan være vanskelig å oppfylle, for eksempel behovet for at dataene *forblir* hemmelige. Imidlertid kan det tenkes at avtaler kan løse denne problematikken, slik at hemmeligholdelse blir overholdt for verdifulle data, til tross for at dataen for eksempel er overført til en samarbeidspartner.

På lik linje med både opphavsrettsvernet og databasevernet som ble behandlet ovenfor, kan det være

12 Databasedirektivet artikkel 3 (1) og Ot.prp. nr. 85 (1997 – 1998) s. 13.

13 Dommens avsnitt 39 jf. også C-403/08 og C-429/08 Football Association Premier League m.fl. avsnitt 97.

14 C-604/10 Football Dataco I avsnitt 42.

15 Dette følger samtidig av ordlyden i databasedirektivet artikkel 3 (1) og databasedirektivets fortale punkt 15.

16 Forretningshemmelighetsloven § 1.

17 Forretningshemmelighetsloven § 2 (1) bokstav a til c.

18 Forretningshemmelighetsdirektivets fortale punkt 2.

vanskelig å beskytte individuelle data. Under forretningshemmelighetsloven kan det nemlig være vanskelig å bevise at enkelte data har kommersiell verdi fordi de er hemmelige. Imidlertid er det vår oppfatning at data som utgjør eller inngår i større datasett og databaser, oftere vil inneha (større) kommersiell verdi ved hemmelighold.

Vernet for forretningshemmeligheter kan således få en større og større betydning for bedrifter som ønsker å beskytte egne data som en del av sin innovasjonsstrategi. For bedrifter som anvender datadrevet teknologi som kunstig intelligens, vil bedriftens data potensielt ligge til grunn for hele forretningsmodellen. I spørsmålet om beskyttelse av data, herunder kommersialisering av data, vil derfor vernet for forretningshemmeligheter stå helt sentralt nå og i fremtiden.

Imidlertid gir ikke vernet for forretningshemmeligheter innehaver noen form for eneretter til utnyttelse av informasjonen eller dataen. Vernet for forretningshemmeligheter skiller seg således fra de såkalte klassiske immaterialrettighetene som gir håndhevbare eneretter, slik som opphavsretten og databasevernet. Dette bekreftes av forretningshemmelighetsdirektivet hvor det fremgår at direktivet med hensyn til innovasjon ikke er ment å gi *«nogen form for eneret til knowhow eller oplysninger, der er beskyttet som forretningshemmeligheder»*.[19] Det skal derfor være mulig *«at gøre en uafhængig opdagelse af samme knowhow eller oplysninger»*.

Selv om forretningshemmelighetsdirektivet ikke gir beskyttelse i form av eneretter, kan det uansett være fordelaktig i en datasammenheng. Det kan nemlig være bedre egnet å snakke om beskyttelse mot urettmessig tilegnelse av data, enn beskyttelse i form av eneretter som gir adgang til å forby andres utnyttelse av dataen.[20] Dette vil imidlertid være opp til hver enkelt bedrift å vurdere som del av sin immaterialrettslige strategi.

Kontraktsregulering av data

Endelig, uavhengig av beskyttelse av data i kraft av opphavsretten, databasevernet eller vernet for forretningshemmeligheter, kan kontrakter løse mange spørsmål knyttet til rettigheter til data. Immaterialrettslige beskyttelsesmekanismer er gjerne bare et utgangspunkt, og suppleres ikke sjelden av avtale for å sikre gode og nyanserte rettighetsforhold mellom ulike kontraktsparter. Som det ble nevnt innledningsvis, og som artikkelen til nå har belyst, er den immaterialrettslige beskyttelsen av data fortsatt usikker. Dette er nok den største grunnen til betegnelsen «contract is king» når det kommer til regulering av data.[21]

Kontrakter gir fleksibilitet og forutsigbarhet mellom kontraktspartene, men gir ingen rett til håndhevelse utenfor kontraktsforholdet. I motsetning til opphavsretten, som kan påberopes ovenfor *enhver,* vil en kontraktsregulering av rettigheter til data kun gjelde mellom partene. Likevel har gjerne kontraktsretten stor betydning på rettsområder som i liten grad eller mindre grad kan hvile seg på foreliggende rettspraksis.[22]

Kontrakter som regulerer rettigheter til data kan utformes som avtaler om for eksempel tilgang, vedlikehold, forsyning eller lisensavtaler.[23] Alle disse formene for avtaler vil gjerne være dynamiske av karakter, slik at partene enkelt kan gjøre endringer eller justeringer ut ifra partenes behov. Dette anses kanskje som en av de viktigste begrunnelsene for at avtaler gjerne er svaret ved spørsmålet om beskyttelse av bedriftens data. Opphavsrettens vern av databaser har en vernetid på 70 år etter opphavers død, og databasevernet operer med 15 år etter databasen ble fremstilt. Vernet for forretningshemmeligheter løper i utgangspunktet helt frem til informasjonen ikke lenger er hemmelig, da det dermed ikke lenger er tale om en forretningshemmelighet etter direktivet og lovens forstand. Flere av de immaterialrettslige beskyttelsesmekanismene kan derfor anses for å være for statiske, særlig med tanke på dataøkonomiens raske utvikling.

Hovedutfordringen i forhold til en kontraktsfesting av datarettigheter vil være å utarbeide kontrakter som omfatter alle de forskjellige problemene en potensielt kan støte på. I en lisensavtale vil det eksempelvis være nyttig å formulere uttrykkelig hvilke rettigheter som lisensieres, muligheten for viderelisensiering og eventuelle geografiske begrensninger på databruken. Dersom dataen skal inngå i Big Data-analyser bør bedriftene regulere hvem som kan bruke informasjonen som fremkommer av analysene, og ikke bare rettigheter til dataen som inngår i analysen.

Generelt vil også reguleringer knyttet til bruk og utnyttelse av dataen ved avslutning av kontraktsforholdet stå helt sentralt. Da partene i kontrakt har mulighet til å avtalefeste konkret hva som skal skje ved opphør av kontrakten, bør det reguleres hva som skjer med bedriftenes egne data, og muligens de data som er skapt i samarbeid mellom kontraktspartene.

I forlengelse av dette kan det samtidig bemerkes at kontraktene bør inneholde klare definisjoner av hva som utgjør data, herunder vise til samtlige data som er relevant for avtaleforholdet. Det bør samtidig bemerkes særskilt hvilke data som anses som hemmelige, og av den

19 Forretningshemmelighetsdirektivets fortale punkt 16.

20 Drexl, Joseph. «Designing Competitive Markets for Industrial Data: Between Propertisation and Access. » (2017) s. 269.

21 Kemp, Richard, Paul Hinton og Paul Garland. «Legal rights in data. » (2011) s. 149.

22 Bendik og Hansen. «Når juss møter AI». (2019) s. 30.

23 Kemp, Richard, Paul Hinton og Paul Garland. «Legal rights in data. » (2011) s. 150.

grunn anses som forretningshemmeligheter.

Flere kommersielle produkter baserer seg i dag på at en leverandør leverer en plattform eller tjeneste som gjennom maskinlæring på samtlige kunders (rå)data utfører stadig bedre output (metadata) til alle kundene. For en leverandør av slike tjenester er det viktig å sikre seg rettigheter til å bruke kundens rådata for et slikt formål - også utover kontraktens løpetid. For en kunde er det viktig å være klar over at når dennes data er blitt benyttet i maskinlæringen, kan ikke disse nødvendigvis trekkes ut («unlearn») av systemet når kunden ikke lenger selv vil benytte tjenesten. Samtidig vil det for slike tjenester være viktig å sikre seg at kundens rådata ikke deles med øvrige kunder.

Dette lille utsnittet av noen kontraktsspørsmål og scenarioer viser at det er viktig å ha i mente den usikkerheten som er belyst i forhold til bakgrunnsrettens, herunder eksempelvis immaterialrettens, beskyttelse av data, og dermed ha klare og dekkende avtaler som regulerer mulige utfall nå, som fremtidig.

Avslutning

Artikkelen viser at databasevernet, opphavsretten eller vernet for forretningshemmeligheter, kan verne om data i form av databaser og data som er hemmelige og av kommersiell verdi. I tillegg kan opphavsretten verne om individuelle data, dersom dataen kan anses som åndsverk i åndsverklovens forstand. Til tross for at mange i teorien oppstiller spørsmålet om eierskap eller beskyttelse av individuelle data, er det vår oppfatning at det er beskyttelse av store datasett som gjerne vil være det aktuelle for datadreven teknologi, og bedrifter som benytter seg av dette. Databasevernet og vernet for forretningshemmeligheter fremstår derfor som de mest sentrale beskyttelsesmekanismene for data.

Det kan på denne bakgrunn ikke utelukkes at forskjellige aktører som benytter seg av – eller utvikler – ny datadrevet teknologi, vil forsøke å påberope seg ulike former for immaterialrettslig beskyttelse eller vernet for forretningshemmeligheter i hele eller deler av datasettene de besitter. I denne sammenheng kan det bemerkes at databasevernet, som en del av opphavsretten, er formfritt i den forstand at beskyttelse oppstår i det databasen skapes. Rettigheter til en database under opphavsretten kan dermed ikke registreres, slik som for eksempel varemerkerettigheter eller patent.[24]

Det er i denne forbindelse fastslått i juridisk teori at databasevernet fungerer mer som en beskyttelse rettighetshaverne påberoper seg i ettertid, snarere enn noe det *investeres i*, eller inngås lisensavtaler *på grunnlag av*.[25] Det fremgår av de nevnte evalueringene av databasedirektivet at en mulig løsning kan være å transformere databasevernet til en rettighet som erverves ved registrering.[26] Forfatterne av evalueringene presiserer imidlertid at dette på nåværende tidspunkt kun er refleksjoner fra deres side, og derfor noe som må utredes ytterligere for å vurdere eventuelle fordeler ved rettighetsregistrering, samt eventuelle innvendinger.[27] Uavhengig av en slik utvikling, er det på det rene at det er vanskelig på nåværende tidspunkt å si noe sikkert om hvilke insentiver eventuelle rettigheter i relasjon til data faktisk gir.[28] En mulig grunn til dette er at det fremdeles fremstår uvisst hvilken verdi som ligger i data alene, særlig innenfor økosystemet av kunstig intelligens.

Kontraktsretten later derfor til å gi et bedre grunnlag for regulering av eierskap til (eller snarere bruksrett til) – og beskyttelse av – data. Her kan partene utarbeide spesifikke rettighetsreguleringer og forpliktelser etter sine behov. Kontraktsretten gir dermed de ulike aktørene muligheter til å eksperimentere med forskjellige ordninger over tid, og det gis en fleksibilitet for partene til å tilpasse seg ulike omstendigheter i de mange sektorer som etter hvert beveger seg inn i den moderne dataøkonomien.

Silje Strandengen og Stian Hultin Oddbjørnsen, del av CMS Kluge sitt team for teknologi, media og kommunikasjon.

24 Dette skillet trekkes gjerne som opphavsretten på den ene siden, og de industrielle rettighetene på den andre. De mest sentrale av de industrielle rettighetene er patentrettigheter, rettigheter til varemerker og andre kjennetegn, samt designrettigheter.

25 Rognstad, Ole-Andreas. «Opphasvrett.» (2019) s. 392.

26 Derclaye, Estelle m.fl. «Study in support of the evaluation of Directive 96/9EC on the legal protection of databases». (2018) s. 139. Dette er en støtterapport til EU-kommisjonens egne evaluering av databasedirektivet. Rapporten reflekterer på denne måten ikke EU-kommisjonens betraktninger eller refleksjoner, men forfatternes.

27 Derclaye, Estelle m.fl. «Study in support of the evaluation of Directive 96/9EC on the legal protection of databases». (2018) s. 139.

28 Drexl, Joseph. «Designing Competitive Markets for Industrial Data: Between Propertisation and Access. » (2017) s. 273 – 275.

Nye avgjørelser fra Datatilsynet om innsyn i og overvåkning av ansattes epost

Av Emilie Sverdrup og Line Helen Haukalid

Emilie Sverdrup

Line Helen Haukalid

Arbeidsgiver kan ha et stort praktisk behov for tilgang til ansattes epostkasse i ulike situasjoner, for eksempel etter den ansattes fratredelse eller dersom arbeidsgiver mistenker at den ansatte har brutt pliktene sine. Hensynet til den ansattes personvern tilsier imidlertid at innsyn og overvåkning forbeholdes situasjoner der slik tilgang er strengt nødvendig.

Arbeidsgivers rett til å gjøre innsyn i eller overvåke ansattes eller tidligere ansattes e-post er blant annet regulert i forskrift om arbeidsgivers innsyn i epostkasse og annet elektronisk materiale (heretter omtalt som "innsynsforskriften"). Innsynsforskriften gjelder innsyn i og overvåkning av både nåværende og tidligere ansattes epost og filer. Den omfatter ikke bare ansattes
e-post, men også annet elektronisk utstyr som arbeidsgiver har stilt til den ansattes disposisjon til bruk i arbeidet, for eksempel den ansattes mobiltelefon.

I 2021 har Datatilsynet truffet flere avgjørelser relatert til innsyn i og overvåkning av ansattes e-post. Disse avgjørelsene viser viktigheten av å ha et bevisst forhold til innsynsreglene. I denne artikkelen ser vi nærmere på vilkårene for innsyn og overvåkning, samt Datatilsynets praksis rundt dette.

Når kan en virksomhet gjøre innsyn i eller overvåke ansattes epost og filer?

Arbeidsgiver kan kun kreve innsyn i to tilfeller. Det første tilfellet er dersom innsyn er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten. Dette kan typisk være i forbindelse med brått og langvarig fravær, og hvor innsyn er nødvendig for å følge opp den ansattes virksomhetsrelaterte korrespondanse eller for å få tilgang til forretningskritisk informasjon. Et eksempel på et legitimt formål fra Datatilsynets praksis er en akutt situasjon under en ansatts fravær, hvor innsyn er nødvendig for å få oversikt over kommende oppdrag.

Det andre tilfellet er ved begrunnet mistanke om at den ansattes bruk av elektronisk lagret materiale medfører grovt brudd på vedkommendes plikter. Datatilsynet har
uttalt at dette vilkåret normalt vil være oppfylt dersom arbeidsgiver har en begrunnet mistanke om at virksomhetens epost brukes til straffbare forhold, som nedlastning eller videresending av barnepornografi eller ulovlig fildeling, eller til aktiviteter som gir grunnlag for oppsigelse eller avskjed. Eksempel på sistnevnte er at epostkassen mistenkes brukt til trakassering av kollegaer, utsending av spam eller rettstridig deling av virksomhetskritisk informasjon.

Innsynsforskriften skiller mellom innsyn i og overvåkning av arbeidstakers bruk av elektronisk utstyr. Mens innsyn er tillatt i ovennevnte tilfeller, er overvåkning kun tillatt dersom formålet med overvåkingen er å administrere virksomhetens
datanettverk eller å avdekke eller oppklare sikkerhetsbrudd i nettverket.

Innsyn og overvåkning må skje i samsvar med personvernregelverket og arbeidsmiljøloven

Innsyn utgjør en behandling av personopplysninger. Dette betyr at reglene i GDPR kommer til anvendelse. Herunder må den ansatte ha behandlingsgrunnlag for å kunne gjøre innsyn. Aktuelt behandlingsgrunnlag er GDPR artikkel 6 nr. 1 bokstav f berettiget interesse.

Arbeidsgiver sørge for at innsyn gjøres i samsvar med personvernprinsippene i GDPR artikkel 5 og rettighetene i kapittel 3. I praksis betyr dette blant annet at arbeids-

giver må ivareta den ansattes rett til informasjon og rett til å protestere på innsynet. Innsynet må videre begrenses til det som er strengt nødvendig for å oppnå formålet. For eksempel kan man ikke kreve innsyn i hele den ansattes arbeidsområde for å ivareta daglig drift dersom det er tilstrekkelig med innsyn i enkeltfiler. Resultatet fra inn-synet må også slettes så snart formålet er oppnådd.

I tillegg oppstiller innsynsforskriften og arbeidsmiljøloven nærmere prosedyrer som virksomheten må følge både i forkant, underveis og i etterkant av et innsyn eller overvåkning. Det er videre viktig å være oppmerksom på at innsyn utgjør et kontrolltiltak etter arbeidsmiljøloven, noe som utløser særlige prosedyrer.

Innsyn og overvåkning ved avsluttet arbeidsforhold

Når en ansatt slutter skal epostkassen avsluttes slik at det ikke lenger er mulig å sende eller motta eposter, med mindre virksomheten har et særskilt behov for å holde epostkontoen åpen i en kort periode etter opphøret. Innholdet i epostkassen skal slettes.

I juli 2021 ila Datatilsynet et overtredelsesgebyr på 150 000 kr for innsyn i og manglende avslutning av en epostkasse. Innsynet ble gjort i en ansatts oppsigelsestid. Etter opphør av arbeidsforholdet fortsatte arbeidsgiver å logge seg inn i vedkommendes epostkasse daglig i en periode på seks uker.

Bakgrunnen for innsynet var behovet for å ivareta den daglige driften av virksomheten og kontakt med kunder. Datatilsynet uttalte at dette er legitime formål som kan begrunne innsyn. Begrunnelsen for at det likevel ble konstatert regelbrudd var at virksomheten kunne valgt mindre inngripende tiltak for å ivareta daglig drift og kundekontakt ved avslutning av et arbeidsforhold. Formålet kan for eksempel oppnås ved å sende informasjon om ny kontaktperson før en ansatt slutter. Dersom man har et særlig behov for å holde epostkassen åpen, kan man legge inn en fraværsmelding med informasjon om at den ansatte har sluttet og hvem som er ny kontaktperson. Datatilsynet la dermed til grunn at innsyn ikke var nødvendig, og at virksomheten dermed ikke hadde rettslig grunnlag for innsynet.

Datatilsynet bemerket også at overtakelse av epostkassen etter endt arbeidsforhold grenset til overvåkning. Ettersom overvåkningen ikke var begrunnet i nettverksadministrasjon eller for å avdekke eller oppklare sikkerhetsbrudd i nettverket, konkluderte Datatilsynet med at virksomheten heller ikke hadde rettslig grunnlag for over-våkningen.

Datatilsynet karakteriserte overtredelsen som alvorlig. I skjerpende retning ble det lagt vekt på at virksomheten, i tillegg til å mangle rettslig grunnlag, ikke hadde informert om innsynet, samt at virksomheten hadde fortsatt overvåkningen av epostkassen til tross for den tidligere ansattes protest.

Automatisk videresending av epost

I to saker fra tidligere i år ila Datatilsynet overtredelsesgebyrer på 200 000 kr og 250 000 kr for ulovlig automatisk videresending av epost. Sakene gjaldt henholdsvis videresending av en tidligere ansatts

epost etter avsluttet arbeidsforhold og
videresending i forbindelse med sykefravær og ferie. I begge sakene begrunnet virksomhetene videresendingene med at dette var nødvendig for å ivareta daglig drift.

Datatilsynet la til grunn at automatisk videresending av epost er å anse som kontinuerlig overvåking av arbeidstakers epostkasse. Overvåkning er, som nevnt, kun tillatt dersom formålet er administrere virksomhetens datanettverk eller å avdekke eller oppklare sikkerhetsbrudd i nettverket. En virksomhet kan derfor ikke aktivere automatisk videresending av en ansatts eller tidligere ansatts eposter under henvisning til daglig drift.

Hva må virksomheten være klar over i forbindelse med innsyn og overvåkning?

De nevnte sakene viser for det første viktigheten av å være klar over skillet mellom innsyn og overvåking. Disse aktivitetene er underlagt ulike vilkår i innsynsforskriften og må derfor vurderes hver for seg. Mens innsyn er tillatt der det er nødvendig for å ivareta den daglige driften eller ved mistanke om grovt brudd på vedkommendes plikter, må formålet med overvåkning være nettverksadministrasjon eller avdekking/oppklaring av sikkerhetsbrudd i nettverket.

For det andre viser praksis viktigheten av at arbeidsgiver informerer den ansatte om innsyn og overvåkning, samt følger prosedyrereglene i innsynsforskriften. Innsyn og overvåkning er svært personverninn-gripende tiltak, og det stilles derfor strenge krav til informasjon. I flere av sakene har Datatilsynet vurdert det som skjerpende at den ansatte ikke på forhånd ble varslet om innsynet eller overvåkningen.

For det tredje viser praksis viktigheten av å ha dokumenterte rutiner for innsyn. Slike rutiner skal blant annet gjøre virksomheten
bevisst på sine forpliktelser etter personvernregelverket og dermed bidra til etterlevelse. I saker hvor dokumenterte rutiner ikke har vært på plass, har Datatilsynet pålagt virksomheten å etablere slike.

Emilie Sverdrup er advokatfullmektig i Advokatfirmaet Wiersholm.

Line Helen Haukalid er fast advokat i Advokatfirmaet Wiersholm.

Halvor Manshaus, *leder IP/Media-gruppen i Advokatfirmaet Schjødt AS, Oslo og fast spaltist i Lov&Data.*
Inge Kristian Brodersen og Hugo Otterlei, *partnere i Advokatfirmaet Schjødt AS, Oslo, med spesialisering innen IT.*

Heving av erp-kontrakt – kommentar til eidsivating lagmannsretts avgjørelse i tvisten mellom felleskjøpet og infor

Hvert år gjennomføres det en rekke omfattende og komplekse leveranser av informasjonsteknologi i Norge, og det er ikke uvanlig at det oppstår uenigheter mellom partene både før, under og etter et slikt prosjekt. Likevel er det relativt få rettssaker relatert til slike leveranser ved de ordinære domstoler. Tradisjonelt har vi sett at et flertall av slike IT-tvister finner sin løsning gjennom forhandlinger, eventuelt gjennom konfidensiell voldgift. I de siste årene har det likevel kommet frem enkelte profilerte saker med samlede krav på flere hundre millioner norske kroner som har havnet i rettsapparatet.

I en større tvist mellom leverandøren IBM AS og kunden Statens vegvesen, den såkalte «Grindgut-saken», nedkom Oslo tingrett med sin avgjørelse 31. januar 2020 (ref. nr. TOSLO-2016-51424). Saken hadde da gått over flere uker for tingretten, og er nå anket inn for lagmannsretten.

Den 13. juli 2021 avsa Eidsivating lagmannsrett dom i ankesaken mellom kunden Felleskjøpet Agri SA ("FK") og leverandøren Infor (Steinhausen) II GMBH ("Infor") (ref. nr. LE-2018-76187-3[1]). Infor ble frifunnet for FKs krav på erstatning og tilkjent erstatning på over 84 MNOK, samt sakskostnader for både lagmannsretten og tingretten på til sammen ca. 50 MNOK. Lagmannsretten reverserte fullstendig tingrettens avgjørelse fra 9. februar 2018 (TNERO-2016-101703[2]), der tingretten hadde konkludert med at Infor hadde utvist grov uaktsomhet eller forsett. Tingretten tilkjente FK 288 MNOK i erstatning med tillegg av sakskostnader.

Begge disse sakene tok utgangspunkt i norske standardmaler som regelmessig brukes ved inngåelse av IT-kontrakter. Videre var det et avgjørende spørsmål domstolene måtte ta stilling til i disse sakene: Kundens adgang til å heve kontrakten, herunder forståelsen av standardkontraktenes vilkår og regulering av hevingsadgangen. Status etter tingrettens dom i Grindgut-saken og lagmannsrettens dom i Infor-saken er at leverandørene har vunnet frem med sine anførsler knyttet til heving av prosjektavtalen. Ingen av sakene er imidlertid rettskraftige i det dette skrives. Hvorvidt disse to sakene kan tas til inntekt for en økende konfliktvilje og rettsliggjøring i norsk IT-sektor, er det nok for tidlig å si.

Uansett er avgjørelsene av interesse for alle som befatter seg med tolkning av IT-kontrakter, og avgjørelsene vil kunne ha dirkete rettskildemessig betydning ved tolkningen og anvendelsen av de aktuelle standardavtalene. I det følgende vil vi fokusere på den siste saken, som altså gjaldt tvisten mellom FK og Infor og se nærmere på noe av det som kan hentes ut fra lagmannsrettens avgjørelse.

1 Lovdata: *https://lovdata.no/LESIV/avgjorelse/le-2018-76187-3*
2 Lovdata PRO: *https://lovdata.no/pro/TRSIV/avgjorelse/tnero-2016-101703*

Anskaffelsen, kontrakten og prosjektets gjennomføring

Lagmannsretten oppsummerer i dommen bakgrunnen for tvistesaken. I 2013 startet Felleskjøpet en prosess for å anskaffe et nytt forretningssystem, på engelsk ofte omtalt som "Enterprise Resource Planning" og forkortet til "ERP". FK utarbeidet en beskrivelse av funksjonelle og tekniske krav det nye systemet måtte ivareta. En egen prosjektgruppe hos FK laget deretter en omfattende kravspesifikasjon og et tilbudsgrunnlag som lå til grunn for innhenting av tilbud fra utvalgte leverandører. Etter konkurranse mellom flere leverandører ble tilslutt Infor valgt, og kontrakt ble inngått 3. april 2014.

Kontrakten var basert på en av statens standardavtalemaler for IT-anskaffelser, som på den tiden var benevnt "Avtale om levering av standardsystem og tilpasning" og forkortet til "SSA-T". I henhold til kontrakten var det overordnede formålet med prosjektet å skifte ut det daværende og egenutviklede systemet "FK-Meny" med et nytt ERP-system som skulle effektivisere forretningsdriften og øke lønnsomheten. Det nye ERP-systemet skulle blant annet håndtere økonomi- og regnskapssystemer, prosesser som produksjon og salg av korn og kraftfor, salgstransaksjoner og øvrig handelsvirksomhet. Leveranseomfanget ble delt inn i tre hovedsystemer og hovedfaser: "Økonomi" i fase 1, "Handel" i fase 2, og "Tonn" i fase 3, hvor hovedsystemet for Økonomi beskrives som en "bærebjelke" i ERP-systemet (jf. tingrettsdommen s. 3).

Fra vår side kan det her bemerkes at denne situasjonen er nokså typisk for ERP-prosjekter. Utgangspunktet vil altså ofte være at kunden sitter på en eller flere løsninger som til sammen utgjør et eksisterende forretningssystem. Hele eller deler av dette vil kunne være egenutviklet, og man ser ofte en blandingsløsning der ulike komponenter er satt sammen over tid. Kunden vil i tillegg ha egne prosedyrer og rutiner for hvordan informasjon skal legges inn i systemet og struktureres, samt hvordan rapporter, fakturering, regnskap og andre nødvendige handlinger skal hentes ut igjen fra systemet. Inngangen på ERP-prosjektet vil dermed kunne være et forprosjekt der kunde og leverandør må samarbeide om å kartlegge og beskrive det hvordan det nye systemet skal implementeres, med hensyn til struktur, arbeidsflyt, rapportering osv. Profesjonelle kunder vil i forkant av en anbudsrunde ofte ha gjort en egen kartlegging og beskrivelse. Det gjøres så en vurdering opp mot leverandørens ERP-produkt for å se hva som eventuelt må gjøres av tilpasninger og endringer for å møte kundens behov. Der kunden ønsker å beholde eksisterende rutiner og systemer vil det normalt måtte gjøres mer arbeid for å tilpasse leverandørens system. Dette innebærer ikke bare større kostnader i prosjektet, men vil normalt også innebære at senere oppdateringer eller tilpasninger i systemet vil kunne bli mer omfattende ettersom dette må tilpasses spesielt for denne kunden. Det er vår erfaring at det også vil være vanlig at det underveis i prosjektet vil dukke opp ytterligere spørsmål knyttet til overgangen fra kundens eksisterende system og over til den nye ERP-løsningen som skal tilpasses og installeres. For eksempel vil det kunne være utfordringer knyttet til migrering av data eller deler av den gamle løsningen, behov for endringer av rutiner eller en av partene kan se nye muligheter for effektivisering underveis dersom det gjøres justeringer i leveransen. Slike spørsmål må partene avklare seg i mellom, og det vil deretter bli utstedt endringsordre underveis i prosjektperioden. Som en overordnet betraktning kan det legges til grunn at det i et ERP-prosjekt vil være flere endringsordre enn i enklere kontraktsleveranser der det kun leveres ett enkelt system eller en standardløsning uten tilpasninger.

I dette prosjektet hadde hver hovedfase 6 milepæler for spesifikke del-faser. "Milepæl 3" ("M3") for Økonomi og Handel, som gjaldt utvikling- og installasjon (også kalt byggefasen eller gjennomføringsfasen), står sentralt i selve tvistesaken. M3 skulle etter opprinnelig fremdriftsplan ha vært godkjent 27. februar 2015 for Handel og 24. april 2015 for Økonomi. Begge fristene ble flyttet til 17. april 2015 gjennom avtalt endringsordre. Infor gjorde deretter leveringsforsøk som ikke ble akseptert av FK, og fristene ble flyttet på nytt gjennom ytterligere endringsordre, denne gang til 30. juni 2015. FK aksepterte heller ikke leveransen som ble forsøkt gjort opp mot denne siste fristen.

Den 6. juli 2015 ga FK melding til Infor om at forsinkelsen av M3 innebar mislighold av kontrakten og at dagbøter påløp. Etter dette fulgte en periode med intensiv korrespondanse mellom partene og replanleggingsaktiviteter, helt frem til november 2015. Infor anførte blant annet at det i juli 2015 ble oppnådd enighet om at FK frafalt dagbotskravet, i en såkalt "juli-avtale".

Den 17. november 2015 varslet Infor at prosjektaktiviteter ville bli stanset (pauset) med virkning fra 20. november 2015. To dager etter skrev FK i brev at stansing av prosjektet utgjorde et forsettlig mislighold som eksponerte Infor for ubegrenset erstatningsansvar. FK krevde at Infor trakk tilbake beslutningen om stans. Den 2. desember 2015 varslet FK blant annet at man ville vurdere å heve avtalen dersom Infor ikke gjenopptok arbeidet innen 15. desember. Den 10. desember ble det avholdt et heldagsmøte mellom partene, hvor Infor foreslo både operasjonelle (i saken også kalt strukturelle) og kommersielle endringer. I et brev dagen etter ga FK uttrykk å være positive til forslaget til de operasjo-

nelle endringene, men ikke de kommersielle.

10. desember 2015 ble det avholdt et heldagsmøte mellom Infor og Felleskjøpet. I en presentasjon fra Infor til møtet fremgikk det at prosjektet var 10-12 måneder forsinket. Sett i sammenheng med øvrige uttalelser i dommen, tolker vi dette dit hen at Infor informerte FK om at M3 ville nås om 10-12 måneder.

Den 18. desember 2015 sendte FK varsel til Infor om heving av kontrakten. Vi hitsetter fra varselet:

> *"FKA erklærer herved at FKA, med virkning fra 4. januar 2016, hever avtalen om standardsystem og tilpasning inngått 3. april 2014 (Avtalen), med mindre Infor innen 29. desember 2015 skriftlig:*
>
> *i. bekrefter at pausen avbrytes. FKA anser kun pausen som avbrutt dersom Infor fullt ut gjenopptar arbeidet i prosjektet innen kl. 10.00 den 4. januar 2016. Dette innebærer også at prosjektets medlemmer som arbeidet i FKAs lokaler forut for prosjektpausen skal gjenoppta arbeidet og møte opp i FKAs lokaler innen dette tidspunkt, og*
>
> *ii. aksepterer uten forbehold følgende forutsetninger, som alle reflekterer Infors nåværende forpliktelser under Avtalen:*
>
> - *Leveransen skal leveres med samme omfang (scope) som avtalt, med mindre det er grunnlag for endringsordre,*
> - *Leveransen skal leveres til samme pris som avtalt, med mindre det er grunnlag for endringsordre,*
> - *Infor er ansvarlig for fremdrift, når partene er enige om en revidert fremdriftsplan,*
> - *Infor bekrefter at de for fremtiden forholder seg til Avtalens begrensning av Infors rett til stansing inntatt i pkt. 12.3 i Avtalen.*
>
> *Dersom ikke Infor, innen fristene angitt over, avbryter prosjektpausen og gir FKA de bekreftelser som kreves i dette brevet, vil heving inntre automatisk og uten ytterligere erklæring fra FKA. "*

I varselet ble det altså fremmet krav om at stansen opphørte, samt krav om bekreftelser fra Infor. I motsatt fall ville heving ifølge FK inntre automatisk og uten ytterligere erklæring.

Infor sendte brev den 29. desember 2015 hvor Infor bestred at det forelå vesentlig mislighold fra Infors side. Infor anførte at det var FK som var ansvarlig for forsinkelsene. I tillegg anførte Infor blant annet at Infor hadde til hensikt å oppfylle avtalen, og at Infor ikke hadde krevet vesentlige endringer til avtalen. Infor foreslo å gjenoppta diskusjoner om replanlegging tidlig januar 2016. I brev av 31. desember 2015 fra FKs advokat fremgår det at FK aksepterer at Infor i brevet av 29. desember har bekreftet å stå ved avtalen. Det fremgår av dommen at lagmannsretten mente Infor med dette oppfylte det ene av to krav i

hevingsvarselet; kravet om bekreftelser. Det andre kravet, det vil si full gjenopptagelse av alle prosjektaktiviteter, anså lagmannsretten derimot ikke for å være oppfylt på dette tidspunktet.

Nyttårsaften 2015 foreslo FK en utsettelse av hevingen til 18. januar 2016, denne gang betinget av at partene gjennomførte en intens arbeidsperiode hvoretter FK ville avgjøre hvorvidt de ville heve eller ikke. Det fremgikk ikke av FKs brev av 31. desember at FK forutsatte at Infor skulle gjenoppta alle prosjektaktivitetene i den foreslåtte to-ukers arbeidsperioden, og noen ny frist for Infor til å gjenoppta konsulentaktivitetene ble heller ikke satt. Lagmannsretten skriver at ettersom poenget med den felles arbeidsperioden nettopp var å vurdere grunnlaget for den videre prosessen, ville det etter lagmannsrettens syn ha vært naturlig for FK å si klart ifra dersom det var forventet at Infor straks skulle gjenoppta konsulentaktivitetene. Lagmannsretten la derfor til grunn at kravet i hevingsvarselet av 18. desember om å gjenoppta konsulentaktivitetene ikke lenger var virksomt, og at et slikt krav i tilfelle måtte blitt varslet på nytt med ny frist, for å kunne gi grunnlag for heving av avtalen.

Det som i stedet skjedde, var at FK den 3. februar 2016 sendte hevingserklæring til Infor med referanse til både stansen og forsinkelse.

Ettersom Felleskjøpet ikke ga nytt varsel om at alle prosjektaktivitetene skulle gjenopptas før hevingen fant sted 3. februar 2016, fant lagmannsretten at FKs heving den 3. februar på grunnlag av stansen 17. november 2015 var urettmessig. Retten kom også til at stansen i seg selv ikke utgjorde et vesentlig mislighold av avtalen som ga FK rett til å heve, dersom avtalens fremgangsmåte for heving hadde blitt fulgt.

Det er verdt å merke seg at de to rettsinstansene har vurdert både "juli-avtalen", rettsvirkningene av pausen i prosjektet og FKs fremgangsmåte ved heving forskjellig, se neste punkt.

Tingretten vs. Lagmannsretten

I saksforberedelsene til ankeforhandlingen ble det fra Infors side fremsatt begjæringer om bevistilgang til en omfattende mengde dokumenter. Begjæringene ble tatt delvis til følge, og fremlagte saksdokumenter økte fra ca. 3.600 sider i tingretten til ca. 13.000 sider for lagmannsretten. Ankeforhandlingen må sies å ha vært omfattende da den gikk over 27 rettsdager og 35 vitner (inkludert 6 sakkyndige) avga forklaring.

Materielt synes det særlig å være på fire punkter at vurderingene fra lagmannsretten skiller lag med tingretten, nemlig i vurderingen av (1) den såkalte *"juli-avtalen"*, (2) stansen i prosjektet fra 17. oktober 2015, (3) FKs fremgangsmåte ved heving av kontrakten og (4) spørsmålet om forsinkelse som hevingsgrunnlag.

(1) "Juli-avtalen":

Etter en gjennomgang av fremlagt dokumentasjon på e-postkorrespondanse mellom partene i dagene etter FKs melding om forsinkelse og dagbøter den 6. juli 2015, legger lagmannsretten til grunn (s. 19) at partene den 17. juli 2015 hadde oppnådd enighet om at (1) det skulle fastsettes ny leveringsdato for M3, (2) at leveringsdato den 30. juni 2015 ikke lenger gjaldt, og (3) at det ikke påløp dagbøter.

Dette er i skarp kontrast til tingretten som resonnerer seg frem til følgende konklusjon (s. 14): *"Retten finner etter dette at det ikke ble inngått noen «juli-avtale» som har avgjørende betydning for vurderingen av Infors mislighold."* Tingrettens standpunkt har hatt stor betydning for blant annet dens vurdering av spørsmålet om faktisk forsinkelse, se nedenfor.

(2) Stansen:

Lagmannsretten finner ikke holdepunkter for at den ensidige stansen i seg selv utgjorde et vesentlig mislighold. Retten mener det er forhold ved saken som tilsier en "skjerpet hevingsterskel", og viser blant annet til et sakkyndig vitne som uttalte at innføring av stans i et prosjekt ute av kontroll er en "relativt vanlig og anerkjent fremgangsmåte". Retten legger videre vekt på at Infor arbeidet med re-planlegging (ca. 7000 timer) i stansperioden, og kommer til at stansen slik sett ikke innebærer en tilbakeholdelse av Infors ytelser i strid med SSA-T punkt 12.3, der det fremgår at Infor ikke *"kan holde tilbake ytelser som følge av Kundens mislighold, med mindre misligholdet er vesentlig, og Kunden skriftlig har erkjent misligholdet […]"*

Tingretten er derimot på sin side klar på at kriteriene i SSA-T punkt 12.3 ikke var oppfylt: *"Det er på det rene at vilkårene for en eventuell tilbakeholdelse fra Infors side ikke var oppfylt, verken materielt med vesentlig mislighold, eller formelt med skriftlig erkjennelse, og retten går ikke nærmere inn på dette, utover å bemerke at bestemmelsen styrker rettens oppfatning av Infors mislighold og alvorlighetsgraden av dette. At Infor, ved stansingen eventuelt feilbedømte sin rettslige posisjon med hensyn til berettigelsen av stansingen, er noe Infor selv må bære risikoen for. Basert på ovennevnte, at Infors mislighold i beste fall var grovt uaktsomt, faller også Avtalens ansvarsbegrensning bort, jf. Avtalen punkt 11.5.6 siste ledd […]"*

For det andre finner lagmannsretten heller ikke holdepunkter for FKs anførsel om at Infor brukte stansen for å tvinge gjennom forbedrede kommersielle vilkår, eller for at Infor ville stanse prosjektet dersom FK ikke ville betale mer enn det som fulgte av kontrakten. Lagmannsretten baserer seg blant annet på skriftlige uttalelser fra Infors advokat om at endring av kommersielle vilkår ikke var et krav for å fortsette prosjektaktivitetene. Lagmannsretten skriver også at en slik handling ville vært uklokt i et strategisk perspektiv – prosjektet skulle være et referanseprosjekt for Infor i det nordiske markedet.

Tingretten går ikke i særlig grad inn på Infors beveggrunner for stansen, og konstaterer at *"uavhengig av […] årsaken til prosjektpausen, finner retten at denne ikke hadde hjemmel i Avtalen eller i nærmere enighet eller forståelse mellom partene."*

(3) FKs fremgangsmåte ved heving av kontrakten

Etter lagmannsrettens syn, var ikke FKs fremgangsmåte ved heving i samsvar med kontrakten på flere punkter. SSA-T punkt 11.5.4 bestemmer at *"Dersom det foreligger vesentlig mislighold, kan Kunden etter å ha gitt Leverandøren skriftlig varsel og rimelig frist til å bringe forholdet i orden, heve hele eller deler av avtalen med øyeblikkelig virkning."*

FKs varsel om heving av 18. desember 2015 inneholdt en passus om at heving ville inntre automatisk og uten ytterligere erklæring dersom nærmere angitte "forhold" ikke ble bragt "i orden" innen fristen. At det skal skje automatisk, er etter lagmannsrettens syn ikke i samsvar med kontraktsbestemmelsen: FK måtte foreta en ny vurdering om hevingsvilkårene forelå etter at fristen for retting var utløpt.

FKs e-post av 31. desember 2015 med forslag om å utsette tidspunkt for automatisk heving til 18. januar 2016, var betinget av gjennomføring av intensiv arbeidsperiode og et utfall som FK aksepterte. Lagmannsretten påpeker at slike "betingede krav" heller ikke er en fremgangsmåte i samsvar med kontrakten, og heller ikke at det ville vært et "vesentlig mislighold" dersom Infor ikke hadde oppfylt FKs krav om gjennomføring av intensiv arbeidsperiode. Lagmannsretten konkluderer gjennomgangen med å fastslå at FKs heving den 3. februar 2016 på grunnlag av stansen 17. november var urettmessig.

Som nevnt over kom lagmannsretten også til at hvis stansen hadde utgjort hevingsgrunn, måtte FK uansett ha gitt et nytt varsel om heving, med referanse til stansen.

Tingretten gikk på sin side ikke inn i en konkret vurdering av om FKs fremgangsmåte for heving var i samsvar med SSA-T punkt 11.5.4.

(4) Spørsmålet om forsinkelse som hevingsgrunnlag

Når det gjelder spørsmålet om det forelå faktisk (også kalt "aktuell") forsinkelse, påpeker lagmannsretten utgangspunktet om at en fastsatt leveringstid må være oversittet for at det skal foreligge faktisk forsinkelse. Retten legger som nevnt til grunn at partene var enige om å utsette leveringsdato for M3 (ref. "juli-avtalen"), men uten å fastsette noen leveringstid. Dermed forelå det således ingen faktisk forsinkelse med hensyn til M3 som kunne gi FK rett til å heve.

I tillegg fastholdt FK kontrakten etter utløpt maksimal dagbotperiode ca. 8. oktober 2015, og hadde dermed etter lagmannsrettens vurdering forspilt sjansen til å heve for faktisk forsinkelse selv om siste avtalte frist (30. juni 2015) skulle ha blitt lagt til grunn for M3.

Når det gjelder "antesipert" forsinkelse, viser lagmannsretten til at Infor hadde varslet 10-12 måneder forsinkelse allerede 10. desember 2015, og at FK likevel krevde gjenopptakelse av prosjektaktivitetene. Lamgannsretten kommer etter dette til at heller ikke "antesipert forsinkelse" kunne føre frem som grunnlag for heving av kontrakten.

Lagmannsretten går etter dette ikke nærmere inn på spørsmålet om faktisk og antesipert forsinkelse inngikk i hevingsgrunnlaget.

Tingretten legger liten eller ingen vekt på "juli-avtalen" og skriver (s. 9) at *"Det er leveringen av Milepæl 3, M3 som etter rettens skjønn er avgjørende i diskusjonen om forsinkelse. […] Det er ubestridt at leveringen av M3 ble forsinket. Det er også på det rene at Felleskjøpet aldri aksepterte levering av M3. […] Det ble ikke avtalt en ny omforent leveringsdato, og det ble aldri akseptert en levering av M3."* Tingretten fastslår også at (s. 7): *"Ut fra en alminnelig tolking av ordlyden i hevingserklæringen finner retten, alene basert på hevingserklæringen, det sannsynliggjort at hevingen var basert på prosjektets samlede forsinkelse, med den ensidige pausen som en utløsende faktor."*

"Take aways" fra lagmannsrettens dom – vår vurdering

Dommen illustrerer blant annet at dersom en part skal heve kontrakten, må det være et direkte samsvar mellom hevingsvarsel og den etterfølgende hevingserklæring. Dersom man hever på et grunnlag som ikke er varslet, vil hevingen kunne underkjennes fordi feil fremgangsmåte er fulgt. I tillegg kan det ikke varsles automatisk heving under henvisning til gitte vilkår eller kriterier. Det må etter den «rimelige tiden» vurderes om forholdet er «brakt i orden» slik SSA-T punkt 11.5.4 foreskriver.

Som kunde må man etter dette også vokte seg for å gi utrykk for at det skal fastsettes en ny leveringsdato, uten samtidig å klart formidle at opprinnelig leveringsdato gjelder inntil annet blir skriftlig avtalt. Hvis kunden unnlater dette, kan en domstol slik som lagmannsretten gjorde, komme til å konkludere at det ikke lenger finnes noen konkretisert eller formelt fastsatt leveringsfrist å oversitte.

Dommen viser også at det er strenge krav til fremgangsmåten for en heving. Prosedyren i SSA-T punkt 11.5.4 (heving) må følges. Det skal ikke bare gis en rimelig frist for å "bringe forholdet i orden", det må i tillegg gjøres en ny og konkret vurdering av om hevningsvilkårene foreligger ved utløpet av denne rimelige fristen. Det skal med andre ord være en realitet i vurderingen.

Videre illustrerer dommen at hevingsterskelen er skjerpet i denne type kontraktsforhold, når en har kommet langt i leveranseforløpet. Lagmannsretten begrunnet den skjerpede hevingsterskelen med at (i) leveransen gjaldt et omfattende

IT-system som skulle tilpasses kundens virksomhet, (ii) i slike leveranser er det ikke uvanlig med forsinkelser, og hvor det også kan oppstå behov for re-planlegging underveis, og (iii) Infor hadde dessuten over tid nedlagt betydelig innsats i prosjektet. Når lagmannsretten viser til at leveransen skulle tilpasses kundens virksomhet, er det trolig fordi slike tilpassede leveranser ikke kan anvendes av andre. Leverandøren som rammes av heving risikerer altså å sitte med en uferdig og skreddersydd leveranse som ikke kan brukes videre. Heving medfører dessuten at kundens virksomhet må ta fatt på en ofte kostbar og tidkrevende snuoperasjon, hvor en ny anskaffelse og et nytt prosjekt må gjennomføres. Lagmannsretten uttaler følgende om terskelen for at en kunde kan sies å ha rimelig grunn for å si seg løst fra kontrakten: "Det vil normalt ikke være i noen av partenes interesse at hevning skjer i andre tilfeller av mislighold enn der hvor leverandøren ikke kan eller vil avhjelpe."

Lagmannsretten bemerker også at dersom FKs syn om at aktuell forsinkelse løper fra 30. juni 201 skulle legges til grunn, så ville FK ha forspilt sin mulighet til å heve avtalen ved at FK fastholdt avtalen, og lot Infor fortsette arbeidet også etter utløpet av dagbotsperioden og frem til stansen ble iverksatt 20. november 2015. Lagmannsretten viser til Nortvedt m.fl. "NS 8407 Kommentarutgave (2013) side 682:

> *"Dersom byggherren vil påberope seg en forsinkelse som hevingsgrunn, må han i utgangspunktet heve når forsinkelsen foreligger (…). Han kan ikke la totalentreprenøren fortsette arbeidene og beholde forsinkelsen som et mulig hevingsgrunnlag som kan påberopes når som helst".*

Dette innebærer ikke nødvendigvis at en kunde for å beholde hevingsretten etter utløpet av en dagbotsperiode umiddelbart må ta stilling til om kontrakten skal heves eller ikke. Det er heller ikke nødvendig å tolke lagmannsrettens avgjørelse dit hen, ved at det er gjort en konkret vurdering ut i fra forholdene i denne konkrete saken. FKs endelige heving fant sted meget senere enn ved utløpet av dagbotsperioden.

FK fastholdt dessuten kontrakten på tross av opplysninger fra Infor i et heldagsmøte 10. desember 2015 opplyst om at M3 ville la vente på seg i ytterligere ti til tolv måneder. Da er en nærliggende konklusjon at en eventuell hevingsrett med referanse til forsinkelse, må begrunnes i at M3 blir forsinket også ut over de ti til tolv månedene. I det minste ga dette oppfordring til FK om i denne perioden å klargjøre eventuelle synspunkter på forventet leveringsdato. Vi oppfatter at dette er bakgrunnen for at lagmannsretten kom til at slik utsettelse av M3 ikke kunne gi grunnlag for heving på grunn av antesipert forsinkelse. Retten viser til at det ikke kan ha kommet som en overraskelse for FK at Infor i presentasjonen 26. januar 2016, etter gjennomføringen av januarmøtene, opplyste at forventet leveringstid for M3 ville være om ti måneder.

I relasjon til spørsmålet om stansen utgjorde et vesentlig mislighold av avtalen, la lagmannsretten til grunn at FKs evaluering av prosessen og leveransene fra Infor i to-ukers arbeidsperioden forut for hevingen, ikke ga grunnlag for heving av avtalen, og under enhver omstendighet ikke uten at Infor ble gitt varsel om forhold som etter FKs mening utgjør vesentlig mislighold, og med rimelig frist for å bringe forholdet i orden. Lagmannsretten skriver om kravet til varsel: *"Kunden må i varselet angi hva misligholdet består i og hva som forventes for å avhjelpe dette. Kunden må altså beskrive «forholdet» og hva som kreves for å «bringe forholdet i orden»".*

I andre tilsvarende saker vil det nok uansett være slik at dersom en leverandør fremlegger en ny operativ fremdriftsplan, og kunden velger å videreføre prosjektet på basis av denne, vil hevingsrett med referanse til forsinkelse være avskåret inntil det oppstår forsinkelse også i forhold til den nye operative planen, med mindre det er tatt forbehold om dette. Andre misligholdsbeføyelser vil derimot typisk være i behold, forutsatt at kunden tydelig fastholder at å følge den operative fremdriftsplanen, ikke er slik å forstå at kunden har innrømmet forlengelse av fristene i den avtalte fremdriftsplanen.

Artikler

Jens Erik Paulsen.
"AI, Trustworthiness, and the Digital Dirty Harry Problem" i *Nordic Journal of Studies in Policing,* vol. 8, no. 2, 2021, pp. 1–19.

Artificial Intelligence (AI) has been a game changer on many fronts. For the police it offers new ways of carrying out investigation, surveillance, crime prevention and order maintenance. Questions have been raised about the trustworthiness of some innovative AI-driven applications. Under which circumstances and to what extent should the police be permitted to use emergent technology, i.e. use 'dirty' means in order to reach good ends? In this article, this problem is illustrated by a discussion of two emergent technologies, and possible criteria and test regimes for establishing trustworthiness are suggested towards the end of the article.

https://www.idunn.no/njsp/2021/02/ai_trustworthiness_and_the_digital_dirty_harry_problem

Marte Eidsand Kjørven,
Alf Petter Høgberg & Geir Woxholth.
«BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtale-loven § 35 (3) og ny finansavtalelov § 4-30 (4)» i *Lov og Rett* 06/2021 (Volum 60) s. 335-366.

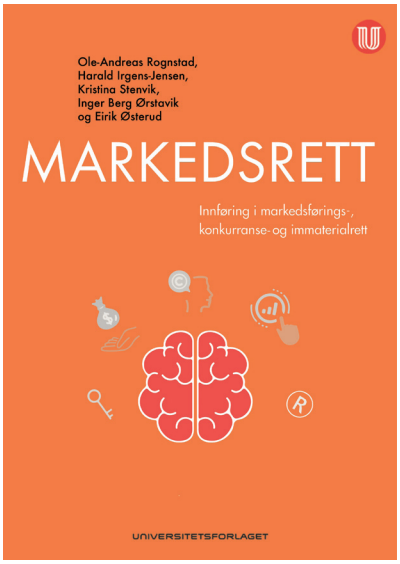
Artikkelen tar for seg hvilke krav som må stilles for å aktivere det strenge forsettsansvaret for BankID-opplysninger på avveie etter gjeldende og kommende finansavtalelov.

https://www.idunn.no/lor/2021/06/bankid-opplysninger_paa_avveie_om_vilkaarene_for_aktivering

Litteratur

Markedsrett, *Innføring i markedsførings-, konkurranse- og immaterialrett*

Rognstad, Ole-Andreas m.fl. Universitetsforlaget – 430 s. Oslo 2021 - ISBN 978-82-15-04328-9



Markedsretten omfatter i praksis tre hovedrettsområder: konkurranseretten, reglene om illojal konkurranse og immaterialretten. I denne boken knytter forfatterne de ulike rettsområdene sammen på en pedagogisk måte og viser hvordan markedsretten gjør seg gjeldende.

På hvilke måter kan en bedrift som har lagt ned store ressurser i produktutvikling og markedsføring, skjerme sine investeringer? I hvilken grad kan bedriften forhindre konkurrerende virksomheter fra å selge og markedsføre de samme eller liknende produkter uten å bære tilsvarende kostnader? Hvordan kan bedriften beskytte eget navn og produktnavn og andre kjennetegn slik at kundene kjenner igjen produktene til bedriften? Boken omhandler regler som har betydning for denne type problemstillinger. Den har også en rekke praktiske eksempler og oppgaver og kan brukes som inngangsport til en større fordypning i markedsrettens fagområder.

Gorrissen Federspiel

Tue Goldschmieding

3.1 Ændring af lov om TV-overvågning

Den 1. juli 2020 trådte lov nr. 802 af 9. juni 2020 om ændring af lov om tv-overvågning i kraft. Formålet med ændringsloven var at følge op på regeringens trygheds- og sikkerhedspakke, og derfor giver ændringsloven en øget mulighed for adgangen til tv-overvågning. Trygheds- og sikkerhedspakken blev præsenteret som en reaktion på sprængninger rettet mod Skattestyrelsen og en lokalpolitistation i København i starten af 2019.

Størstedelen af ændringslovens bestemmelser trådte i kraft den 1. juli 2020. Justitsministeren var dog bemyndiget til at bestemme ikrafttrædelsesdatoen for lovens § 2 e, der omhandler registrering af overvågning i politiets register over tv-overvågningskameraer. Justitsministeren har ved bekendtgørelse nr. 1060 af 28. maj 2021 om ikrafttræden af § 1, nr. 10 i lov om ændring af lov om tv-overvågning fastsat ikrafttrædelsestidspunktet for ændringslovens § 2 e til den 1. juli 2021.

Bestemmelsen gør det obligatorisk for private og offentlige myndigheder, der foretager tv-overvågning af gade, vej, plads eller lignende område, at registrere sig i politiets register over tv-overvågningskameraer (POLCAM). Formålet med bestemmelsen er at gøre det lettere for politiet at få adgang til overvågningsmateriale i forbindelse med politiets efterforskning af strafbare forhold. Ændringerne skal således bidrage til at skabe tryghed og sikkerhed i offentligheden.

Læs ændringsloven her: https://www.retsinformation.dk/eli/lta/2020/802

Læs bekendtgørelsen her: https://www.retsinformation.dk/eli/lta/2021/1060

3.2 Datatilsynet udtalte kritik som følge af utilstrækkelig kryptering i selvbetjeningsløsning hos politiet

Det danske Datatilsyn har den 7. april 2021 ved afgørelse i sag med journalnummer 2020-432-0049 udtalt kritik af det danske Rigspolitis selvbetjeningsløsning til brug for ansøgninger om våbentilladelser.

Rigspolitiets selvbetjeningsløsning indeholdt en webansøgningsformular og en mailafsendelsesfunktion. Ved udfyldning af webansøgningsformularen, der indeholdte ansøgerens personoplysninger, bemærkede Datatilsynet, at der opstod forbindelse mellem politiets server og ansøgerens browser, og at forbindelsen var krypteret med TLS 1.0 kryptering. Datatilsynets anbefaling for kryptering er TLS 1.2. Rigspolitiet oplyste, at den eksisterende ansøgningsproces ikke understøtter et højere niveau af kryptering end TLS 1.0.

På baggrund af dette fandt Datatilsynet grundlag for at udtale kritik af Rigspolitiet behandling af personoplysninger. Datatilsynet var af den opfattelse, at den valgte kryptering indeholdte kendte sårbarheder, og at den derfor ikke var egnet til brug af behandling af personoplysninger på et tilstrækkelig højt sikkerhedsniveau, som kræves efter artikel 32, stk. 1 af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ("databeskyttelsesforordningen").

Læs afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/apr/utilstraekkelig-kryptering-i-selvbetjeningsloesning-hos-politiet

3.3 Datatilsynet udtalte alvorlig kritik af en ukrypteret mail med personoplysninger sendt fra Justitsministeriet

Det danske Datatilsyn ("Datatilsynet") har den 19. maj 2021 ved afgørelse i sag med journalnummer 2020-442-6885 udtalt alvorlig kritik af Justitsministeriet for at sende en ukrypteret e-mail med personoplysninger.

Justitsministeriet sendte den 27. marts 2019 en e-mail til Advokatsamfundet. E-mailen indeholdte 35 personers navne, personnummer og tilsendte rykkerskrivelser om oversendelse til inddrivelse af bøder fra SKAT. Justitsministeriet kunne ikke bevise, at e-mailen var krypteret, og Datatilsynet måtte derfor antage, at e-mailen ikke var blevet sendt krypteret.

Ifølge Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ("databeskyttelsesforordningen") artikel 32, stk. 1, har den dataansvarlige pligt til at sikre passende tekniske og organisatoriske foranstaltninger til at imødegå de risici, der er forbundet med databehandlingen. Den dataansvarlige skal også bevise, at denne pligt er opfyldt, jf. databeskyttelsesforordningens artikel 24. Datatilsynet fandt ikke, at Justitsministeriet hav-

de godtgjort, at forpligtelsen var opfyldt, jf. artikel 32, stk. 1, jf. artikel 24 i databeskyttelsesforordningen.

Datatilsynet fandt også, at Justitsministeriet havde handlet i strid med artikel 33, stk. 1 i databeskyttelsesforordningen, der pålægger databehandlere at give Datatilsynet meddelelse om afbrud inden 72 timer efter bruddet. Justitsministeriet blev bekendt med bruddet den 18. november 2019, men anmeldte først forholdet til Datatilsynet den 28. februar 2020.

Endelig kritiserede Datatilsynet, at Justitsministeriet havde undladt at underrette de registrerede om bruddet. Dette medførte, ifølge Datatilsynet, en forhøjet risiko for personernes rettigheder, jf. artikel 34, stk. 1.

Datatilsynet udtalte derfor alvorlig kritik af Justitsministeriet for brud på databeskyttelsesforordningens artikel 32, stk. 1, jf. artikel 24, 33, stk. 1, og 34, stk. 1. Datatilsynet påbød også Justitsministeriet at underrette alle registrerede om bruddet, jf. artikel 58, stk. 2, litra e i databeskyttelsesforordningen.

Læs afgørelsen her:
https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/maj/ukrypteret-mail-med-personoplysninger-sendt-fra-justitsministeriet

3.4 Datatilsynet udtalte alvorlig kritik af Club Matas A/S" behandling af personoplysninger

Det danske datatilsyn ("Datatilsynet") har den 20. april 2021 i sag med journalnummer 2018-41-0012 udtalt alvorlig kritik af Club Matas A/S ("Club Matas") og tilhørende underklubbers behandling af persondata. Datatilsynets afgørelse blev truffet på baggrund af et tilsynsbesøg, der blev afholdt den 4. oktober 2018.

Ifølge Club Matas' "Vilkår og betingelser for Club Matas" af september 2020, behandlede denne medlemmer af club matas' personoplysninger efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ("databeskyttelsesforordningens") artikel 6, stk. 1, litra a og f.

Datatilsynet tog først stilling til, om Club Matas' behandling af personoplysninger var baseret på samtykke fra de registrerede efter databeskyttelsesforordningens artikel 6, stk. 1, litra a. Det blev derfor vurderet, om de registrerede havde givet et gyldigt samtykke i overensstemmelse med definitionen af samtykke i databeskyttelsesforordningen. Et samtykke bliver defineret som "enhver, frivillig, specifik, informeret og utvetydig viljeserklæring", jf. databeskyttelsesforordningens artikel 4, nr. 11.

Datatilsynet fandt, at udformningen af samtykketeksten ikke opfyldte betingelsen om frivillighed. Datatilsynet lagde vægt på, at samtykket ikke var opdelt, og medlemmerne derfor ikke kunne foretage et reelt og frit valg af samtykke til de enkelte behandlingsformål. Endvidere var det Datatilsynets opfattelse, at Club Matas' samtykkeløsning ikke var beskrevet tilstrækkeligt klart. Slutteligt konkluderede Datatilsynet, at samtykkeløsningen ikke var tilstrækkeligt informeret. Datatilsynet mente ikke, at det tydeligt fremgik af samtykketeksten, at vigtige informationer om behandling af personoplysninger fremgik af "Vilkår og betingelser for Club Matas". Derudover var Club Matas' vilkår om personoplysninger beskrevet sammen med Club Matas' generelle vilkår. Det var derfor uklart, hvilke informationer, der angik behandling af personoplysninger.

Datatilsynet fandt dermed grundlag for at udtale alvorlig kritik af Club Matas' samtykkeløsning, der hverken sikrede et tilstrækkeligt frivilligt, specifikt eller informeret samtykke. Club Matas' samtykkeløsning opfyldte dermed ikke kravene til et gyldigt samtykke, hvorfor behandling af personoplysninger om medlemmer af Club Matas ikke var sket i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 6, stk. 1, litra a, jf. artikel 4, nr. 11.

Læs afgørelsen her:
https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/apr/tilsyn-med-matas-as-behandling-af-personoplysninger

3.5 Datatilsynet fandt kritisable forhold ved Statens Serum Instituts COVID-19-modelleringsprojekt

Det danske Datatilsyn ("Datatilsynet") har den 25. marts 2021 ved afgørelse i sag med journalnummer 2020-432-0044 udtalt alvorlig kritik af Statens Serum Institut ("SSI") for at påbegynde behandling af personoplysninger uden tilstrækkelig risikovurdering, konsekvensanalyse, høring af Datatilsynet, databehandleraftaler og passende sikkerhedsforanstaltninger.

SSI blev i forbindelse med COVID-19-situationens eskalering i Danmark bedt om at nedsætte en ekspertgruppe. Ekspertgruppen havde til opgave at udføre en lang række statistiske undersøgelser af afgørende betydning for udviklingen og begrænsningen af COVID-19 i Danmark. I den forbindelse skulle SSI stille personoplysninger til rådighed for ekspertgruppen.

SSI vurderede, at risikoen for de registrerede var moderat til høj og konstaterede, at der ikke var foretaget en fuldstændig kortlægning eller vurdering af behandlingens risici, ved behandlingens start

I uge 12 påbegyndte SSI behandlingen af personoplysninger. Det var inden der var udarbejdet tilstrækkelige aftalegrundlag mellem SSI og ekspertgruppen, samt inden der var udarbejdet en risikovurdering og konsekvensanalyse. Behandlingen blev påbegyndt efter en afvejning af situationens sundhedsmæssige og økonomiske alvor for Danmark over for kravet om dokumenteret databeskyttelsesretslig compliance. Førstnævnte blev vurderet til at veje tungest.

Den tiltænkte it-løsning for dataudvekslingen var ikke klar til tiden. Derfor blev dataadgangen i stedet etableret på SSI's server i uge 12. Dataadgangen blev placeret bag en ydre firewall, hvoraf eksperterne havde mulighed for at få adgang til denne med et brugernavn og kodeord. Personoplysningerne var pseudonymiserede, og SSI vurderede, at dette var passende sikkerhed.

Risikovurderingen blev først begyndt i uge 16, og første version af en konsekvensanalyse forelå i uge 17. Databehandleraftaler med ekspertgruppens medlemmer blev underskrevet i uge 17.

Datatilsynet fandt, at der var grundlag for at udtale alvorlig kritik af SSI's behandling af personoplysninger. Datatilsynet vurderede, at denne behandling af personoplysninger var sket i strid med reglerne i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ("databeskyttelsesforordningen") artikel 28, stk. 3 om databehandlerkontrakt, artikel 32, stk. 1 om behandlingssikkerhed, artikel 35, stk. 1 om konsekvensanalyse og artikel 36, stk. 1 om forudgående høring.

Datatilsynet fandt dog, at det var formildende omstændigheder til stede. Disse formildende omstændigheder var først, at behandlingen skulle etableres under en international krisesituation, da der forelå en væsentlig samfundsinteresse i den hurtige effektuering af behandlingen. Derudover var det en formildende omstændighed, atSSI havde gjort sig overvejelser om den foreløbige fravigelse af de databeskyttelsesretlige regler og at SSI, i et vist omfang, havde forsøgt at afhjælpe disse.

På den baggrund blev sanktionen fastsat til alvorlig kritik.

Læs afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/mar/kritisable-forhold-ved-statens-serum-instituts-covid-19-modelleringsprojekt-

3.6 Datatilsynet har opdateret sin vejledning om samtykke

Datatilsynet har den 5. maj 2021 offentliggjort en opdatering til deres vejledning om samtykke som behandlingsgrundlag efter Forordning (EU) 2016/679 af 27. april 2016 ("databeskyttelsesforordningen"). Opdateringen indeholder både præciseringer, opdateringer og ny praksis fra Datatilsynet.

Det følger af databeskyttelsesforordningen, at behandling af borgeres personoplysninger skal foretages med et behandlingsgrundlag og et af de behandlingsgrundlag databeskyttelsesforordningen benytter er samtykkereglerne Formålet med Datatilsynets opdaterede vejledning er at give en introduktion til disse regler, samt at sikre, at vejledningen er aktuel og anvendelig.

Af Datatilsynets opdaterede vejledning fremgår også, at offentlige myndigheder ikke længere kan behandle persondata på baggrund af samtykke. Derudover fastslås det at borgere, der scroller eller swiper på en hjemmeside, eller anden tilsvarende brugeraktivitet, ikke kan anses for at give en utvetydig viljestilkendegivelse, der udgør et samtykke. Derudover indeholder Datatilsynets vejledning nu også praksis på samtykkeområdet. Eksempelvis fremhæves datatilsynets afgørelse i sag med j. nr. 2018-32-0357, hvor kravet om at behandling af personoplysninger til flere formål kræver opdeling af samtykket, udpensles. Danmarks Meteorologiske Institut havde i sagen ikke indhentet frivilligt samtykke, da besøgende på institutets website ikke havde mulighed for, at til- eller fravælge hvilke specifikke formål med databehandling den besøgende ønskede at samtykke til.

Læs vejledningen her: https://www.datatilsynet.dk/Media/0/C/Samtykke%20(3).pdf

3.7 EU-kommissionen har vedtaget nye standardaftaler for overførsel af personoplysninger til lande uden for EU/EØS

EU-kommissionen vedtog den 4. juni 2021 gennemførelsesafgørelse (EU) 2021/914 om nye standardkontraktbestemmelser for overførsel af personoplysninger til usikre tredjelande i henhold til Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ("databeskyttelsesforordningen").

De nuværende standardbestemmelser fra EU-Kommissionen bliver i vidt omfang anvendt som overførselsgrundlag, når der overføres personoplysninger til tredjelande i dag. Dette vil også være tilfældet med de nye standardbestemmelser. De nye standardbestemmelser forsøger at tage højde for den måde, behandling af personoplysninger finder sted i dag. De nye standardbestemmelser kombinerer en række generelle bestemmelser med en modulopbygning, med fire forskellige overførselsscenarier: Modul 1 - dataansvarlig til dataansvarlig, Modul 2 - dataansvarlig til databehandler, Modul 3 - databehandler til databehandler og Modul 4 - databehandler til dataansvarlig.

De nye bestemmelser indeholder en klausul, der gør det muligt for tredjeparter at tilslutte sig aftalen. Det gør det enklere at udskifte parter.

Standardbestemmelserne er beskrevet i et bilag til afgørelsen. Formålet med standardbestemmelserne er at sikre overholdelsen af databeskyttelsesforordningen ved overførsel af personoplysninger til tredjelande. Dette omfatter overholdelse af kravene i artikel 28, stk. 3 og 4 i databeskyttelsesforordningen om dataansvarlige og databehandleres rettigheder og pligter samt sikring af de fornødne garantirer i forordningens artikel 46, stk. 1 og stk. 2, litra c.

Bestemmelserne indeholder regler om behandling af personoplysninger, der sikrer overholdelse af de persondataretlige principper, der kendes fra databeskyttelsesforord-

ningen. Dette omfatter bestemmelser om formålsbegrænsning, gennemsigtighed, dataminimering, regler om følsomme personoplysninger og opbevaringsbegrænsning.

I bestemmelse 10 er de registreredes rettigheder fastsat. Dataimportøren skal uden unødig forsinkelse behandle anmodninger fra den registrerede i forbindelse med dennes udøvelse af sine rettigheder efter standardkontraktbestemmelserne. Efter anmodning skal dataimportøren informere den registrerede om, hvorvidt dataimportøren behandler personoplysninger om den registrerede. Derudover skal dataimportøren berigtige urigtige oplysninger om den registrerede og slette personoplysninger, hvis de er behandlet i strid med en af bestemmelserne. Der er endvidere fastsat regler om klageadgang for den registrerede i bestemmelse 11. Parterne er ansvarlige for den skade de måtte påføre hinanden eller den registrerede i forbindelse med databehandlingen.

Læs EU-kommissionens beslutning her: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en

3.8 Google vil tilpasse Google Play efter ICPEN-initiativ og Apple har tilpasset App Store

Den danske Forbrugerombudsmand ("Forbrugerombudsmanden") har i en pressemeddelelse af den 25. marts 2021 meddelt, at Apple har tilpasset deres platform, App Store. Tilpasningen er sket efter Forbrugerombudsmanden i samarbejde med 26 lande fra det internationale netværk, ICPEN, har rettet henvendelse til Apple og Google med opfordring om at foretage tilpasninger i virksomhedernes appstores.

Tilpasningen af App Store indebærer, at forbrugere bliver informeret om, hvilke oplysninger leverandørerne af de enkelte apps indsamler om forbrugeren, når de downloader og anvender en app fra App Store. Det er sikret ved, at Apple har indsat enkelte og overskuelige oplysninger om, hvordan den enkelte app anvender forbrugernes data ved download og anvendelse heraf.

Forbrugerombudsmanden har understreget vigtigheden af, at forbrugeren klart og tydeligt bliver informeret om, hvilke oplysninger leverandøren af en app indsamler om forbrugerne, samt hvad disse oplysninger bliver brugt til. Det skyldes, at flere apps tjener penge på at indsamle og videregive oplysninger om forbrugere til andre virksomheder.

Efter forhandlinger med Google vil Google også foretage tilpasninger i Google Play Store, meddeler forbrugerombudsmanden i en pressemeddelelse af den 26. maj 2021. Forbrugernes adgang til informationer om, hvilke oplysninger leverandørerne af de enkelte apps indsamler om dem er hverken klare eller tydelige på nuværende tidspunkt. Forbrugeren skal scrolle flere sider igennem og klikke på et link om dataindsamling, før forbrugeren får adgang til information. Dette vil blive ændret, og tilpasningen vil blive foretaget løbende. Det er Googles mål, at det bliver obligatorisk for alle apps at informere om indsamling og brug af data ved download af apps fra Google Play Store i 2022.

Tilpasningerne bliver foretaget efter lov nr. 426 af 3. maj 2017 ("den danske markedsføringslov") § 6, stk. 1 og § 8, der forbyder erhvervsdrivende at vildlede eller skjule væsentlige oplysninger på en uklar, uforståelig, dobbelttydig eller uhensigtsmæssig måde.

Læs nyheden om Apple her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2021/apple-tilpasser-app-store-efter-icpen-initiativ/

Læs nyheden om Google her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2021/google-vil-tilpasse-google-play-efter-icpen-initiativ/

3.9 Sony fjerner urimelige vilkår om dataindsamling via 15 produkter

Sagen vedrører brugervilkår på en række af Sony Nordic Danmarks ("Sony") produkter, som den danske Forbrugerombudsmand har anmodet om at få ændret.

Accept af brugervilkårene var en betingelse for, at forbrugeren kunne tage produkterne i brug, og de indeholdt urimelige vilkår om dataindsamling og overvågning af brugernes data. Ifølge vilkårene fik Sony ret til at indsamle store mængder data fra brugernes computere og andre enheder, der var forbundet til Sonys software. Den uklare og uforståelige formulering af vilkårene medførte en skævvridning af forholdet mellem forbrugeren og Sony.

På den baggrund vurderede Forbrugerombudsmanden, at vilkårene om indsamling af data var i strid med lov nr. 193 af 2. marts 2016 ("aftaleloven") § 36, stk. 1 og § 38, stk. 1 om urimelige aftaler. Forbrugerombudsmanden anmodede derfor om ændring af vilkårene, hvilket Sony har imødekommet at ændre.

Læs nyheden her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2021/sony-fjerner-urimelige-vilkaar-om-dataindsamling-via-15-produkter/

3.10 Byretsdom om erstatning for ikke-økonomisk skade forvoldt ved persondatakrænkelse af kommunen

Byretten i Glostrup ("byretten") afsagde den 11. maj 2021 dom i en række sambehandlede sager mellem syv borgere og Gladsaxe Kommune ("kommunen"). Sagen drejede sig om, hvorvidt kommunen som dataansvarlig, havde overholdt kravene til behandlingssikkerheden af persondata i medfør af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ("databeskyttelsesforordningen").

Sagen blev anlagt efter tyveri af fire bærbare computere fra rådhuset

i kommunen. På en af computerne, var der gemt data i et regneark, der indeholdte personfølsomme oplysninger, herunder CPR-numre, navne og adresser på private borgere. Computerens harddisk var ikke krypteret. Det, at selve lagringen af regnearket var lokalt gemt på den enkelte computer, var en overtrædelse af kommunens interne sikkerhedspolitik for håndterning af personoplysninger. Samlet indeholdt computeren information om 20.620 borgere, hvoraf syv af disse lagde sag an mod kommunen med påstand om erstatning på mellem DKK 7.500 til 30.000.

Byretten konkluderede, at kommunen som dataansvarlig ikke havde overholdt kravene til tilstrækkelig behandlingssikkerhed i databeskyttelsesforordningens artikel 32.

Et centralt spørgsmål for klagen var, hvorvidt databeskyttelsesforordningens artikel 82, der som udgangspunkt blot omhandler erstatning for materiel eller immateriel skade, kan give mulighed for erstatning for ikke-økonomisk skade. Hverken EU-domstolen eller de danske domstole har taget stilling til dette spørgsmål. Byretten fandt, at artikel 82 i databeskyttelsesforordningen skulle fortolkes således, at bestemmelsen også kan omfatte erstatning for en ikke-økonomisk skade, som det var tilfældet ved persondatakrænkelsen.

Byretten kunne efter en samlet vurdering af sagen, herunder karakteren af det brud på datasikkerheden og konsekvensen for de berørte borgere, ikke lægge til grund, at borgerne havde været udsat for en sådan skade, der kunne begrunde erstatning.

Læs et resumé af dommen her: https://domstol.dk/glostrup/aktuelt/2021/5/7-borgere-i-gladsaxe-kommune-havde-ikke-krav-paa-erstatning/

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


Delphi

Peter Nordbeck og Amanda Strömbäck

IMY:S BESLUT I 1177-ÄRENDET

Den svenska tillsynsmyndigheten Integritetsskyddsmyndigheten (”IMY”) meddelade i början av juni beslut i flera ärenden med anledning av granskningen av den så kallade ”1177-incidenten”.[1] Två aktörer pekades ut som huvudansvariga, MedHelp AB (MedHelp) i rollen som personuppgiftsansvarig och Voice Integrate Nordic AB (Voice Integrate) i rollen som personuppgiftsbiträde. Kritiken gentemot bolagen omfattande främst brister i lämpliga tekniska och organisatoriska åtgärder i strid med artikel 32.1, men IMY fann även brister i legalitet och transparens gentemot den registrerade i strid med artiklarna 5.1.a, 6 och 9.1 GDPR. De konstaterade att det även funnits brister i säkerhetskopieringen.

1 Integritetsskyddsmyndighetens samlade rapport DI-2021-5220 av den 7 juni 2021.

Bakgrund

Granskningen inleddes den 18 februari 2019, efter att det i media publicerats en artikel där det uppmärksammats att en stor mängd inspelade samtal till sjukvårdsrådgivningen 1177 funnits tillgängliga på en server utan lösenordsskydd eller annan säkerhet. Anmälningar inkom därefter från flera aktörer som var inblandade i incidenten, bland annat MedHelp, Voice Integrate och det thailändska bolaget MediCall Co Ltd (MediCall). Orsaken till incidenten var ett säkerhetshål i servern VoiceNAS som tillhandahölls av Voice Integrate. Utredningen kom att omfatta totalt sex aktörer som kunde kopplas till incidenten eller sjukvårdsrådgivningen 1177 i övrigt.

IMY:s bedömning

Av central betydelse i besluten var att fastställa rollfördelningen mellan aktörerna. Det är den personuppgiftsansvarige som bär det yttersta ansvaret för behandlingen av personuppgifter, men även personuppgiftsbiträdet har vissa skyldigheter. I detta fall gjorde IMY bedömningen att MedHelp agerat som personuppgiftsansvarig då de i rollen som vårdgivare besvarade samtal för regionernas räkning. MedHelp hade därmed en skyldighet att se till att de inkommande samtalen var skyddade. IMY fann att MedHelp brustit i fyra avseenden. Bland annat riktades kritik gentemot bolaget eftersom de brustit i skyldigheten enligt artikel 32.1 GDPR att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa ett skydd för personuppgifter. MedHelp hade även lagt ut vårduppdrag och personuppgiftsbehandling på det thailändska bolaget MediCall vilket inte omfattades av tystnadsplikt i svensk lag. IMY gjorde därför bedömningen att överlämnandet av personuppgifter till MediCall saknat laglig grund enligt artikel 6 GDPR och skett i strid mot förbudet att behandla känsliga personuppgifter i artikel 9.1 GDPR. Kritik riktades mot att MedHelp i strid med artikel 13 GDPR inte informerat de som ringer till 1177 om hur deras personuppgifter skulle komma att behandlas samt att bolaget inte upplyst den vårdsökande om dess roll som personuppgiftsansvarig. IMY fann även att MedHelp brustit i skyldigheten att säkerhetskopiera inkomna samtal för att skydda dessa vid en eventuell förlust i strid med artikel 32.1 GDPR.

IMY tog även ställning till vilken roll Voice Integrate haft. Voice Integrate uppgav i incidentanmälan att de var personuppgiftsansvariga men ändrade senare sina uppgifter och hävdade att de varken hade ansvar som personuppgiftsansvarig

eller personuppgiftsbiträde. Ett avtal benämnt ”personuppgiftsbiträdesavtal” fanns upprättat mellan MedHelp och Voice Integrate. I detta fall gjorde IMY bedömningen att Voice Integrate hade ansvar som personuppgiftsbiträde och att de därmed haft en skyldighet att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda ljudfilerna som lagrats på servern. IMY beaktade i beslutet att de inspelade ljudfilerna funnits tillgängliga på internet för allmänheten under en okänd tid vilket inneburit en hög risk för obehörigt röjande och obehörig åtkomst, att personuppgifterna utgjorde känsliga personuppgifter var en försvårande omständighet.

IMY riktade även kritik mot regionerna då de ansågs ha brustit i sin skyldighet att informera den enskilde angående behandlingen av personuppgifter enligt artiklarna 13 och 14 GDPR och därmed brustit i kravet på transparens och öppenhet i kommunikationen med den enskilde. Ytterligare kritik riktades gentemot Region Stockholm då regionen inte informerat den vårdsökande om att de samlat in ytterligare personuppgifter i syfte att utveckla sjukvårdsrådgivningens funktion.

Granskningen resulterade i att IMY utfärdade sanktionsavgifter på 12 miljoner till MedHelp, 650 000 kr till Voice Integrate, 500 000 kr till Region Stockholm och 250 000 kr vardera till Region Sörmland och Värmland.

Avslutande kommentar

IMY understryker i besluten att en tydlig rollfördelning är avgörande för ett fullgott dataskydd. Det var i detta ärende tydligt att rollfördelningen mellan aktörerna varit otydlig vilket lett till brister i skyddet för personuppgifter. Besluten visar också att skyldigheten att vidta tekniska och organisatoriska åtgärder även innefattar ett krav på att fortlöpande se över och testa att säkerhetsnivån är lämplig i förhållande till risken. IMY har pekat ut personuppgiftsbiträdet Voice Integrate som huvudansvarig vid sidan av MedHelp eftersom personuppgiftsbiträden har ett självständigt ansvar att uppfylla kraven på säkerhetsåtgärder i artikel 32.1 i GDPR och IMY ansåg att Voice Integrate inte hade uppfyllt denna skyldighet.

IMY:s beslut i 1177-ärendet är de första i sitt slag där IMY bedömer ansvaret för flera parter som ingår i en kedja av behandlingar. Det är intressant att se hur IMY har fördelat ansvaret för de brister som förekommit mellan de ingående parterna. Flera av besluten har överklagats och det återstår att se om IMY:s bedömningar kommer att stå sig i alla delar.

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

Amanda Strömbäck er summer trainee i *Advokatfirman Delphi, Stockholm.*

Gorrissen Federspiel

Tue Goldschmieding

3.1 Ny lov om ophavsret

Den 7. juni 2021 trådte lov nr. 1121 af 4. juni 2021 om ændring af lov om ophavsret i kraft ("ændringsloven"). Loven gennemfører artikel 15 og 17 i Europa-Parlamentets og Rådets direktiv (EU) 2019/790 af 17. april 2019 ("DSM-direktivet") samt Europa-Parlamentets og Rådets direktiv (EU) 2019/789 af 17. april 2019 ("SatCabII-direktivet"). Lovens hovedformål er at implementere de to direktiver.

Formålet med DSM-direktivets artikel 15 er at give nye rettigheder til udgivere af pressepublikationer. Artiklen er implementeret ved ændringslovens § 69 a, der skaber en ny eneret for udgivere af pressepublikationer. Det følger af bestemmelsen, at informationssamfundstjenester ikke uden udgiverens samtykke må eftergøre publikationer online eller stille dem til rådighed på en sådan måde, at almenheden får adgang til dem. Beskyttelsen gælder i to år efter udgangen af det år, hvor udgivelsen eller offentliggørelsen fandt sted.

Formålet med DSM-direktivets artikel 17 er at beskytte digitale og grænseoverskridende anvendelser af beskyttet indhold. Artiklen er implementeret ved § 52 c i ændringsloven, hvorefter udbydere af onlineindholdsdelingstjeneste kan ifalde et ansvar for indhold uploadet af tjenestens egne brugere, medmindre udbyderen påviser, at en række betingelser er opfyldt. Resten af DSM-direktivet, som blandt andet indeholder en ny regel om aftalejustering der vil få betydning for producenter og forlag , vil blive fremsat i et selvstændigt lovforslag i efteråret.

SatCabII-direktivets primære formål er at lette grænseoverskridende udbud af onlinetjenester i forbindelse med radio- og tv udseendelser. Direktivet er implementeret ved ændringslovens § 35 og § 87 a. Bestemmelserne indfører et afsenderlandsprincip for radio- og fjernsynsforetagenders tilknyttede onlinetjenester. Baggrunden for ændringen er, at den teknologiske udvikling har medført, at der nu findes mange forskellige former for distributionsmetoder. De tidligere bestemmelse i ophavsloven afspejlede ikke denne udvikling, og man har derfor gjort de nye bestemmelser teknologi neutrale. Ændringen medfører, at såfremt radio- og fjernsynsforetagenders tilknyttede onlinetjenester udsender fra Danmark, er det også i Danmark, at rettighederne skal erhverves. Tidligere gjaldt det kun for radio- og fjernsynsforetagenders udseendelser via satellit, men er nu udvidet, så det også omfatter onlinetjenester.

En anden væsentlig ændring der følger af SatCabII-direktivet, er afklaringen af hvornår "direct injection" udgør videreudsendelse. Ved videreudsendelse af tv- og radio signaler gælder der i ophavsretsloven en tvungen aftalelicens. Direct injection er en teknisk proces, hvor både en tv-station og tv-udbyder deltager i en overføring, og det har været diskuteret hvordan processen skal behandles ophavsretligt. Ændringslovens implementering af direktivet indebærer, at en videreudsendelse af tv-signaler modtaget via direct injection både vil konstituere en videreudsendelse og en primær udsendelse, hvorefter direct injection nu også vil være omfattet af den tvungne aftalelicens.

Læs lov om ændring af lov om ophavsret her:
https://www.retsinformation.dk/eli/lta/2021/1121

3.2 Forbrugerombudsmanden sender udkast til kvikguide om "grøn" markedsføring i høring

Den danske Forbrugerombudsmand ("Forbrugerombudsmanden") har sendt et udkast til en vejledning til virksomheder i høring. Vejledningen skal sikre, at virksomheder ikke får produkter til at fremstå mere miljørigtige, end de er, og dermed forbryde sig mod lov nr. 426 af 3. maj 2017 ("den danske markedsføringslov") ved at vildlede forbrugere.

På baggrund af modtagne klager, samt en stor undersøgelse i samarbejde med EU-kommissionen, har Forbrugerombudsmanden kunne identificere et stort antal sager, hvor virksomheder har vildledt forbrugere i en sådan grad, at myndighederne har vurderet, at den pågældende markedsføring var i strid med Europa-Parlamentets og Rådets Direktiv (EU) 2005/29/EF af 11. maj 2005 ("direktiv om urimelig handelspraksis").

Vejledningen skal læses i sammenhæng med EU-kommissionens førnævnte undersøgelse, som er refereret i seneste version af Lov & Data.

Forbrugerombudsmandens udkast til kvikguide indeholder en ræ-

kke eksempler på markedsføring, der overtræder den danske markedsføringslov. Vejledningen fremhæver konkrete reklamer for et produkts positive indvirkning på miljøet som eksempler på overtrædelse af den danske markedsføringslovs §§ 5 og 6 om vildledende oplysninger samt § 13 om producentens dokumentation af rigtigheden af oplysningerne.

Vejledningen angiver, at markedsføringen er vildledende, hvis produkter ikke kan dokumenteres at have den virkning, som er tilsikret i en reklame. Vejledningen anbefaler, at virksomhederne tilstræber en så høj grad af præcision som muligt om et produkts virkning på miljøet for at undgå overtrædelser af den danske markedsføringslov.

Læs guiden her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2021/forbrugerombudsmanden-sender-udkast-til-kvikguide-om-groen-markedsfoering-i-hoering/

3.3 Domænenavnet "newjob.dk" skulle ikke overdrages til klageren

Det danske klagenævn for domænenavne ("Klagenævnet for Domænenavne") traf den 8. april 2021 afgørelse i sag 2020-0273 mellem NewJob ("klager") og RAINER ("indklagede"). Klagenævnet for Domænenavne fandt frem til, at domænet "newjob.dk" ikke skulle overdrages til NewJob.

NewJob gjorde gældende, at denne tidligere havde været registrant af domænenavnet, "newjob.dk", og at NewJob udelukkende mistede registeringen af domænenavnet som følge af en fejl. Desuden fremførte NewJob, at RAINER, der er en virksomhed registeret i Polen, er en såkaldt domænehaj, da virksomheden ikke benyttede sig af domænet. Derfor mente NewJob at RAINER ikke havde nogen reel interesse i det omtvistede domænenavn.

RAINER gjorde gældende, at denne havde registreret domænenavnet "newjob.dk" i begyndelsen af 2019, fordi RAINER ønskede at anvende domænenavnet til et nyt koncept. COVID-19 pandemien havde imidlertid forsinket RAINERs udvikling af dette koncept. RAINER bestred at være en domænehaj, da denne som ejer af NewJob.dk ApS har en naturlig interesse i domænenavnet.

Klagenævnet for Domænenavne konstaterede, at domænenavnet ikke har kommerciel betydning for NewJob.

Da RAINER drev virksomhed som bl.a. rekrutterings- og vikarbureau og reklamerer herfor på "newjob.dk", gav Klagenævnet derimod RAINER medhold i, at denne havde en forretningsmæssig interesse i domænenavnet. Derudover mente Klagenævnet for Domænenavne ikke, at NewJob havde løftet bevisbyrden for, at denne har større interesse i domænenavnet end RAINER. Afslutningsvist fandt Klagenævnet for Domænenavne ikke, at RAINER gennem indregistreringen af domænenavnet "newjob.dk", havde handlet i strid med reglerne om god domænenavnsskik i den danske domænelovs § 25, stk. 1.

På den baggrund kunne Klagenævnet for Domænenavne ikke overdrage domænenavnet til NewJob.

Læs afgørelsen her: https://www.domaeneklager.dk/sites/default/files/2021-04/2020-0273%2C%20newjob.dk_.pdf

3.4 Domænenavnet "palbostaal.dk" skulle ikke overdrages til klageren

Det danske klagenævn for domænenavne ("Klagenævnet for Domænenavne") traf den 8. april 2021 afgørelse i sag 2020-0331 mellem Catharina Palbo ("klager") og Palbo Stål A/S ("indklagede"). Sagen omhandlede, hvorvidt domænenavnet "palbostaal.dk" skulle overdrages til klager.

Klager gjorde gældende, at slægtsnavnet "Palbo" var et særligt beskyttet slægtsnavn efter lovbekendtgørelse nr. 767 af 7. august 2019 ("den danske navnelov"), da der blot er 28 personer, der bærer dette efternavn. Derudover mente klager, at indklagedes uhjemlede brug af navnet, Palbo, som både domænenavn og forretningskendetegn, var i strid med lovbekendtgørelse nr. 763 af 23. juli 2019 ("den danske selskabslovs") § 2, stk. 2, den danske navnelovs § 3, stk. 1 og § 27, samt lov nr. 164 af 26. februar 2014 ("den danske domænelovs") § 25. Til støtte herfor anførte klager, at klager er ejer af en enkeltmandsvirksomhed under firmanavnet og brandnavnet, Palbo.

Klager anførte, at indklagede vildledte offentligheden ved at bruge slægtsnavnet, Palbo, idet selskabsnavnet Palbo Stål A/S og domænenavnet "palbostaal.dk" var åbenbart forvekslelig med slægten, Palbo, og klagerens enkeltmandsvirksomhed Palbo v/ Catharina Palbo.

Klagenævnet for Domænenavne vurderede først, om anvendelse af domænenavnet "palbostaal.dk" indebar en overtrædelse af den danske navnelovs § 27 om uberettiget anvendelse af et navn. Klagenævnet bemærkede, at navneretten ikke indebar en fortrinsret til domænenavnet, "palbostaal.dk", forud for andre der har ret til at anvende navnet, Palbo, i anden betydning.

Klagenævnet fandt ikke grundlag for, at indklagedes brug af domænenavnet "palbostaal.dk" indebar en krænkelse af klagerens rettigheder efter den danske navnelov. Klagenævnet lagde vægt på, at "palbostaal.dk" siden 2008 har været anvendt af indklagede, uden at det har ført til forvekslinger med klageren eller dennes familie. Klagenævnet lagde også vægt på, at indklagedes selskabsnavn og domænenavn afveg fra klagerens efternavn med tilføjel-

sen "stål"/"staal". Klagenævnet fandt derfor, at domænenavnet "palbostaal.dk" ikke skulle overføres til klager.

Læs afgørelsen her: https://www.domaeneklager.dk/sites/default/files/2021-04/2020-0331%20palbostaal.dk%20BERIGTIGET.pdf

3.5 EUIPO erklærede fejlagtigt et design af en byggeklods fra LEGO ugyldigt

EU-Domstolen afsagde den 24. marts 2021 dom i sagen T 515/19 mellem Lego A/S ("Lego") og Den Europæiske Unions Kontor for Intellektuel Ejendomsret ("EUIPO"). Delta Sport Handelskontor GmbH ("Delta") var intervenient.

Sagen var en prøvelse af en afgørelse truffet den 10. april 2019 af Tredje Appelkammer ved EUIPO (sag R 31/2018-3). Dette var en ugyldighedssag efter artikel 52 i Forordning (EF) nr. 6/2002 af 12. december 2001 ("designforordningen") mellem Delta og Lego om Legos EF-design. I sagen var Legos EF-design erklæret ugyldigt. Ugyldigheden fulgte af designforordningens artikel 8, der udelukker opretholdelse af designbeskyttelse for de elementer af et produkts udseende, der er bestemt af deres tekniske funktion.

Tredje Appelkammer havde fundet, at alle elementerne i Legos design alene var bestemt af produktets tekniske funktion - at samle Legoklodser og skille dem ad. Derfor var registreringen ugyldig efter artikel 8(1). I sagen havde Lego argumenteret for, at designet alligevel kunne beskyttes efter artikel 8(3). Artikel 8(3) opretholder beskyttelse af design, der giver mulighed for en mangfoldig sammenbygning eller sammenkobling af produkter i et modulopbygget system bestående af indbyrdes udskiftelige elementer. Bestemmelsen udgør dog alene en undtagelse til artikel 8(2), om udelukkelse af beskyttelse af design, der må reproduceres i deres nøjagtige form, for at kunne kobles til et andet element.

Tredje Appelkammer havde ikke taget stilling til dette argument i deres afgørelse. EU-Domstolen fandt, at Tredje Appelkammer derved havde begået en retlig fejl. Dette var yderligere begrundet af EU-Domstolen ved, at designet både var omfattet af artikel 8(1) og 8(2), hvorfor designet kunne undtages efter artikel 8(3). På den baggrund annullerede EU-Domstolen afgørelsen afsagt af Tredje Appelkammer.

EU-Domstolen bemærkede yderligere, at Tredje Appelkammer ikke havde identificeret alle elementerne, og vigtigere, ikke havde etableret, at alle elementerne alene var bestemt af deres tekniske funktion i Legos design. Legos EF-design var dermed gyldigt.

Læs et resumé af afgørelsen her: https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-03/cp210048en.pdf

Læs hele afgørelsen her: https://curia.europa.eu/juris/document/document.jsf?text=&docid=239258&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=14776676

3.6 Smykker fra Maanesten A/S havde et vist kommercielt særpræg og nød derfor beskyttelse mod meget nærgående eller slaviske efterligninger

Sø- og Handelsretten afsagde den 29. marts 2021 dom i sagen BS-26853/2020-SHR mellem Maanesten A/S ("Maanesten") og Mash 16 ApS ("Mash 16"). Sagen angik, hvorvidt øreringen "Nubria" samt fingerringen "Pari", der begge var Maanestens produkter, nød beskyttelse efter henholdsvis lov nr. 1144 af 23. oktober 2014 ("den danske ophavsretslov") og lov nr. 426 af 3. maj 2017 ("den danske markedsføringslov"). I så fald var spørgsmålet, om Mash 16, ved salg af lignende produkter, havde krænket disse rettigheder.

Sø- og Handelsretten fandt indledningsvist, at hverken "Nubria" eller "Pari" nød beskyttelse efter den danske ophavsretslov. Begge smykker var inspireret af en indisk næsering, og derfor fandt retten, at de ikke var udtryk for en selvstændig skabt indsats. Smykkerne levede derfor ikke op til betingelserne for ophavsretlig beskyttelse i den danske ophavsretslovs § 1, stk. 1. I stedet fandt retten, at smykkerne var udtryk for en teknisk bearbejdning.

Retten fandt dog, at smykkerne havde et vist kommercielt særpræg, og dermed var beskyttet efter den danske markedsføringslov. I forhold til Boiis smykker fandt retten, at de udgjorde meget nærgående eller slaviske produktefterligninger, og at de derfor krænkede Maanestens smykker efter den danske markedsføringslovs § 3, stk. 1 om god markedsføringsskik.

Retten tog på denne baggrund Maanestens påstande til følge i forhold til både "Nubria" og "Pari" og fastsatte erstatning samt rimeligt vederlag til DKK 250.000.

Læs et kort resumé af afgørelsen her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-26853-2020-SHR.2276.aspx

Læs hele afgørelsen her: https://domstol.fe1.tangora.com/media/-300011/files/DOM_BS-26853-2020-SHR.pdf

3.7 Stilov ApS' rettigheder til Shangies-sandalmodel var krænket

Sø- og Handelsretten afsagde den 11. juni 2021 dom i sagen BS-38961/2020-SHR mellem Stilov ApS ("Stilov") og MOZZ A/S ("Mozz"). Sagen omhandlede, hvorvidt Mozz ved salg og markedsføring af en serie "Lovelies" sandaler havde krænket Stilovs rettigheder efter lov nr. 426 af 3. maj 2017 ("den danske markedsføringslov") § 3, stk. 1 om god markedsføringsskik. "Lovelies" sandalerne lignede Stilovs sandalserie "Shangies" til kvinder samt "Shangies" til børn.

Sø- og Handelsretten fandt, at Mozz' salg og markedsføring af sandalmodellerne "Tallala" og "Laguna" krænkede Stilovs rettigheder efter den danske markedsføringslovs § 3, stk. 1. Stropdesignet på sandalmodellerne var de samme som på "Shangies", var skabt af et lignende materiale og havde samme farveudtryk. Modellerne "Tallala" og "Laguna" ansås derfor som nærgående efterligninger af sandalmodellen "Shangies" til kvinder og børn. Mozz' sandalmodeller "Matara", "Cavallet", "Weligama" og "Pongwe" samt "Dei Due Mari" blev derimod ikke anset for at krænke Stilov rettigheder efter den danske markedsføringslov, idet de havde et andet udtryk end "Shangies".

Retten fremhævede, at Mozz ved salget af de krænkende sandaler ikke kunne antages at have været i god tro. Derfor har Mozz handlet retsstridigt og erstatningsansvarspådragende over for Stilov. Selvom der var anvendt forskellige salgskanaler, bemærkede Sø- og Handelsretten, at der var en høj grad af substituerbarhed mellem Mozz' sandalmodeller og Stilovs "Shangies".

Salget af de krænkende sandalprodukter måtte derfor antages at have medført et afsætningstab for Stilov og en ikke ubetydelig markedsforstyrrelse. Af disse grunde fastslog Sø- og Handelsretten, at Mozz skulle betale et skønsmæssigt fastsat beløb i vederlag og erstatning til Stilov på DKK 65.000.

Læs et kort resumé af afgørelsen her: https://www.domstol.dk/soeoghandelsretten/aktuelt/2021/6/om-kraenkelse-af-sandaler/

Læs hele afgørelsen her: https://domstol.fe1.tangora.com/media/-300011/files/BS-38961-2020-SHR_-_Dom.pdf?rev1

3.8 Sø- og Handelsretten fandt en krænkelse af Nordlux A/S' ophavsret til pendellamper

Den danske Sø- og Handelsret ("Sø- og Handelsretten") afsagde den 7. juni 2021 dom i sag BS-29181/2020-SHR mellem Secto Design Oy ("Secto") og Nordlux A/S ("Nordlux"). Sagen angik spørgsmålet om en krænkelse af Sectos rettigheder af designet til to pendellamper.

Sectos to lamper er begge designet af bøjede trælameller og har desuden et særpræget udtryk. De omstridte lamper produceret af Nordlux er ligeledes karakteriseret ved bøjede trælameller. Sø- og Handelsretten fastslog, at Sectos lamper var ophavsretligt beskyttet brugskunst.

For den ene model, fandt Sø- og Handelsretten, at de identitetsskabende og særegne træk, der prægede Sectos lampe, var at finde i Nordlux' design i en sådan grad, at Nordlux måtte have efterlignet Sectos design. Tydelige kvalitetsforskelle ændrede ikke helhedsindtrykket og kunne dermed ikke føre til et andet resultat. Retten fastslog derfor, at der forelå en krænkelse af Sectos ophavsret efter lov nr. 1144 af 23. oktober 2014 ("den danske ophavsretslov") § 1, nr. 1 om beskyttede værker. Retten fandt desuden, at markedsføringen af lampen udgjorde en krænkelse af lov nr. 426 af 3. maj 2017 ("den danske markedsføringslov") § 3, stk. 1 om god markedsføringsskik.

For Sectos anden model, fandt Sø- og Handelsretten, at lampen var af et væsentligt mere simpelt design sammenlignet med den første model. Nordlux' lampe består af færre trælameller end Sectos, hvilket gav lampen et mere åbent udtryk ved at sprede lysfaldet rundt i rummet. Lysfaldet på Sectos lampe var derimod rettet nedad. Retten fandt på denne baggrund, at Nordlux' design var frigjort i tilstrækkelig grad fra Sectos, at der dermed ikke forelå en krænkelse af Sectos ophavsret, ligesom at der ikke var sket en krænkelse af den danske markedsføringslov.

Retten afgjorde, at Nordlux skulle tilbagekalde den lampe, som krænkede ophavsretten efter reglerne i den danske ophavsretslov § 84, stk. 1 om tilintetgørelse og den danske markedsføringslov § 24, stk. 1 om retsmidler. Nordlux skulle ligeledes betale et skønsmæssigt fastsat vederlag til Secto på DKK 50.000 efter den danske ophavsretslov § 83, stk. 1 om erstatning og den danske markedsføringslov § 24, stk. 3.

Læs et kort resumé af afgørelsen her: https://www.domstol.dk/soeoghandelsretten/aktuelt/2021/6/ophavsret-til-pendellamper/

Læs hele afgørelsen her: https://domstol.fe1.tangora.com/media/-300011/files/BS-29181-2020-SHR_Dom.pdf

3.9 Body All Mind ApS skal betale erstatning for krænkelse af varemærket "BODY – SDS" i et gentagelsestilfælde

Den danske Sø- og Handelsret ("Sø- og Handelsretten") afsagde den 2. juni 2021 dom i sag BS-45203/2020-SHR mellem BODY-SDS A/S ("BODY-SDS") og Body All Mind ApS ("Body All Mind"). Sagen angik, om Body All Mind havde krænket BODY-SDS' varemærkerettigheder ved at have anvendt "BODY SDS" i markedsføring af kropsterapeutuddannelse.

Body All Mind havde den 23. juni 2020 markedsført sin kropsterapeutuddannelse på Google, hvori "Body SDS" indgik i annonceoverskriften. Body All Mind påstod, at angivelsen var en fejl begået af deres reklamebureau. Tidligere i 2018 havde Body All Mind offentliggjort en lignende annonce, hvor Body All Mind gennem et forlig måtte betalte DKK 20.000 til BODY-SDS.

Sø- og Handelsretten fandt, at Body All Mind havde krænket BODY-SDS' varemærke, jf. lov nr. 88 af 29. januar 2019 ("den danske varemærkelov") § 4, idet BODY-SDS ikke havde givet samtykke til anvendelsen. Derudover havde Body All Mind handlet groft uagtsomt ved ikke at konkretisere over for reklamebureauet, at de ikke

måtte anvende varemærket "BODY-SDS".

Sø- og Handelsretten fandt også, at annoncen var i strid med lov nr. 426 af 3. maj 2017 ("den danske markedsføringslov") §§ 3, 5, stk. 1, 20, stk. 1, og 22 om hhv. god markedsføringsskik, vildledende reklame og beskyttelse af forretningskendetegn. BODY-SDS havde ikke lidt noget beviseligt tab, men Body All Mind blev tilpligtet til at betale et vederlag på 40.000 kr. af, jf. den danske varemærkelovs § 43, stk. 1, nr. 1, og den danske markedsføringslovs § 24, stk. 3.

Læs et kort resumé af afgørelsen her: https://www.domstol.dk/soeoghandelsretten/aktuelt/2021/6/kraenkelse-af-varemaerke/

Læs hele afgørelsen her: https://domstol.fe1.tangora.com/media/-300011/files/BS-45203-2020-SHR_-_Dom.pdf

3.10 Euro Play ApS markedsførte og solgte af en række fodboldmål, hvilket krænkede Dutch Toys Groups rettigheder efter designforordningen og markedsføringsloven

Sø- og Handelsretten afsagde den 29. april 2021 dom i sag BS-4213/2018-SHR mellem Dutch Toys Group B.V ("Dutch Toys Group") og Euro Play ApS ("Euro Play"). Sagen angik, hvorvidt Euro Plays fodboldmål havde krænket Dutch Toys Groups rettigheder efter Forordning (EF) nr. 6/2002 af 12. december 2002 ("designforordningen") og lov nr. 426 af 3. maj 207 ("den danske markedsføringslov").

Der har tidligere verseret en krænkelsessag mellem parterne, hvor Sø- og Handelsretten ved dom af 28. november 2016 fandt, at Euro Plays fodboldmål "My Hood Munich" og "My Hood Rebounder", krænkede Dutch Toys Groups rettigheder efter designforordningen og den danske markedsføringslov. Sø- og Handelsretten fastslog i denne dom, at også Euro Plays mål "Hood Chelsea", "My Hood Madrid" og "My Hood Rebounder", havde krænket Dutch Toys Groups rettigheder efter designforordningen og den danske markedsføringslov.

Efter en samlet vurdering af henholdsvis Euro Plays fodboldmål og Dutch Toys Groups fodboldmål, lagde Sø- og Handelsretten vægt på, at målene gav det samme helhedsindtryk. Sø- og Handelsretten vurderede, at Euro Play krænkede Dutch Toys Groups rettigheder efter den danske markedsføringslov § 3 om god markedsføringsskik, idet Euro Plays fodboldmål udgjorde en meget nærgående efterligning af Dutch Toys Groups fodboldmål.

Sø- og Handelsretten fandt, at Euro Play skulle betale vederlag og erstatning fastsat skønsmæssigt til DKK 1 mio. i overensstemmelse med Dutch Toys Groups påstand, jf. lovbekendtgørelse nr. 89 af 29. januar 2019 ("den danske designlovs") § 37 og den danske markedsføringslov § 24. Euro Play skulle endvidere betale sagens omkostninger.

Læs et kort resumé af afgørelsen her: https://www.domstol.dk/soeoghandelsretten/aktuelt/2021/4/kraenkelse-af-ef-design-mv/

Læs hele afgørelsen her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-4213-2018-SHR.pdf

3.11 Sø- og Handelsretten udstedte et forbud mod produktion, markedsføring og salg af visse røgalarmer, der var beskyttet af ophavsretsloven

Den danske Sø- og Handelsret ("Sø- og Handelsretten") afsagde den 30. marts 2021 dom i sagen BS-9628/2020-SHR mellem Cavius ApS ("Cavius") og Schneider Electric Danmark A/S ("SE"). Sagen angik spørgsmålene om 1) fire røgalarmer designet af Cavius nød ophavsretlig og/eller designretlig beskyttelse, og hvis spørgsmål 1 blev besvaret bekræftende, 2) om SE's produktion, markedsføring og salg af lignende røgalarmer krænkede disse rettigheder.

Under besvarelse af spørgsmål 1, vurderede Sø- og Handelsretten beskyttelsen efter de designretlige- og dernæst ophavsretlige regler. Retten fandt, at to af Cavius' designs var offentliggjort på sociale medier mere end et år før indgivelse af ansøgning om EF-design og var dermed ikke nye på ansøgningstidspunktet. Derfor var de to EF-designregistreringer ugyldige, jf. Forordning (EF) nr. 6/2002 af 12. december 2001 ("EF-designforordningen") artikel 25, stk. 1, litra b om ugyldighedsgrunde, jf. artikel 7, stk. 1 om offentliggørelse. Retten fandt imidlertid, at to andre af Cavius' EF-designs ikke savnede nyhed. De havde individuel karakter, der gav den informerede bruger et andet helhedsindtryk end de øvrige, offentliggjorte designs. De to EF-designregistreringer var derfor gyldige. Retten fandt, at SE's røgalarm gav det samme helhedsindtryk som Cavius' EF-designs, og at denne dermed krænkede Cavius' designregistreringer.

I vurderingen af, om SE havde krænket Cavius' ophavsret, fandt retten, at røgalarmerne nød ophavsretlig beskyttelse som brugskunst efter lov nr. 1144 af 23. oktober 2014 ("den danske ophavsretslov") § 1, nr. 1 om beskyttede værker. Det var fordi, røgalarmerne var udtryk for designerens egen intellektuelle frembringelse og frie kreative valg.

Under besvarelse af spørgsmål 2, fandt Sø- og Handelsretten, efter en sammenligning med SE's røgalarmer, at der var en sådan lighed mellem dem, at SE's røgalarmer krænkede Cavius' ophavsret. Retten fandt, at markedsføringen af produkterne ikke var i strid med lov nr. 426 af 3. maj 2017 ("den danske markedsføringslov") § 3, stk. 1 om god markedsføringsskik, § 5, stk. 2 om vildledende oplysninger, § 9 om

vildledende handelspraksis. Retten fandt endvidere ikke grundlag for at konkludere, at der var sket et brud på lov nr. 309 af 25. april 2018 ("den danske lov om forretningshemmeligheder").

På baggrund af ovenstående fandt Sø- og Handelsretten, at SE skulle betale et rimeligt vederlag til Cavius på DKK 150.000, jf. lov nr. 89 af 29. januar 2019 ("den danske designlov") § 37, stk. 1, nr. 1, samt den danske ophavsretslovs § 83, stk. 1, nr. 1, jf. § 76, stk. 1, nr. 1, jf. § 2, stk. 1 om rimeligt vederlag. SE blev desuden tilpligtet at standse alt salg samt tilbagekalde og destruere de pågældende røgalarmer.

Læs et kort resumé af afgørelsen her: https://www.domstol.dk/soeoghandelsretten/aktuelt/2021/3/ophavs-og-designret-kraenket/

Læs afgørelsen her: https://domstol.fe1.tangora.com/media/-300011/files/BS-9628-2020-SHR_Dom.pdf

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


simonsen vogtwiig

Hedda Baumann Heier
og Emile Schjønsby-Nolet

Gjennomføring av CRM-direktivet i norsk rett

Den 5. mai 2021 vedtok Stortinget lov nr. 49 av 28. mai 2021 om kollektiv forvaltning av opphavsrett mv. som gjennomfører Direktiv (EU) 2014/26 (CRM-direktivet) i norsk rett. Loven trådte i kraft 1. juli 2021. Stortinget også vedtok forskrift til loven 9. august 2021.

Tilsynsmyndigheten for overholdelsen av loven er Patentstyret jf. lovens § 49. Etter samme bestemmelse er Klagenemda for mediesaker klageinstans for vedtak fra Patentstyret.

Les loven og forskriften i Lovdatas database.

Endringer i prosessretten øker tryggheten ved å bruke patentrådgivere

Stortinget vedtok den 1. juli 2021 lov nr. 126 av 18. juni 2021 om endringer i tvisteloven og straffeprosessloven. Endringsloven innfører et bevisforbud for kommunikasjon med patent-rådgivere i straffeprosessloven § 119 og tvisteloven § 22-5 på lik linje med advokater, leger og psykologer mm.

Les endringsloven i Lovdatas database.

Oslo tingrett: tolkning av normalkontrakter i bokbransjen

Den 30. april 2021 avsa Oslo Tingrett dom i saken mellom Gyldendal Norsk Forlag AS og datterselskapet Lydbokforlaget AS på den ene siden (heretter "Gyldendal") og forfatter Jørn Lier Horst og illustratør Sandnes Media AS på den andre (heretter Horst). Tvisten gjaldt retten til å gi ut nærmere bestemte bøker som lydbok.

Saksforholdet var i korte trekk at Horst hadde inngått to avtaler med Gyldendal om enerett til lydbokutnyttelse av bestemte bøker. Den ene avtalen gjaldt stykksalg av lydbøkene (heretter "lydbokkontrakten"), mens den andre gjaldt strømming av lydbøkene (heretter "strømmeavtalen").

Saken oppstod som en følge av Horsts misnøyde over at lydbøkene ikke ble gjort tilgjengelig for hele strømmemarkedet, men bare på visse strømmetjenester. Holst valgte derfor i 2020 å si opp både lydbokkontrakten og strømmekontrakten.

Det springende punkt var om lydbokkontrakten kunne sies opp. Oppsigelsesklausulen i kontrakten lød: *"Avtalen kan etter at det er gått minst fem år fra den ble undertegnet sies opp av hver av partene med et halvt års varsel med mindre det er solgt minst 300 eksemplarer det siste året."* Det var solgt mindre enn 300 eksemplarer året før oppsigelsen, men lydbøkene hadde likevel generert atskillige inntekter gjennom å bli strømmet i strømmeapplikasjonen Fabel. Det avgjørende spørsmålet var derfor om "eksemplarer" skulle tolkes slik at det inkluderte strømming.

Gyldendal viste til at det dreide seg om samme verk og samme lydkilde og at avtalen burde tolkes dynamisk i tråd med formålet. Tingretten slo imidlertid fast at ordlyden av "eksemplar" etter en naturlig språklig forståelse ikke omfattet strømming, og videre at det skal mye til for å fravike den naturlige forståelsen ved tolkningen av en standardkontrakt som er blitt til gjennom forhandlinger mellom interesseorganisasjoner.

Selv om retten et stykke på vei var enig i at formålet med bestemmelsen var å oppstille et minstesalgsnivå for lydbøkene og at dette nivået ble tilfredsstilt gjennom strømmeinntektene, mente retten at dette ikke var nok til å fravike den naturlige ordlydstolkningen. Retten henviste blant annet til spesialitetsprinsippet i åndsverklovens § 67.

Gyldendal fikk heller ikke medhold i anførselen om at grunnlaget for å si opp lydbokavtalen måtte anses som endret i og med inngåelsen av strømmeavtalen. Etter rettens syn gjaldt de to avtalene ulike former for distribusjon og det var videre ingenting i strømmeavtalens ordlyd som skulle tilsi at den ville ha en slik virkning. Det var uansett også Gyldendal som var nærmeste til å rydde opp i eventuelle uklarheter ved inngåelsen av strømmeavtalen.

Tingretten gav derfor Horst medhold i at kontraktene kunne sies opp med den konsekvensen ble at lydbokrettighetene gikk tilbake til Horst. Ettersom hovedkravet ikke var sannsynliggjort, fikk Gyldendal heller ikke medhold i kravet om midlertidig forføyning. Begge parter ble frifunnet for hverandres erstatningskrav.

Les tingrettsavgjørelsen med saksnummer TOSL-2020-174346 i Lovdatas database. Dommen er anket, og er derfor ikke rettskraftig.

Bidragene er skrevet av seniorådvokat Hedda Baumann Heier og advokatfullmektig Emile Schjønsby-Nolet. Begge arbeider i Advokatfirmaet Simonsen Vogt Wiig AS sin avdeling for Teknologi og Media i Oslo.


Bird & Bird

Mariam Hussein og Gunnar Hjalt

”En svensk strategi för AI” – ett projekt som görs möjligt tack vare PRV:s roll inom upphovsrätt

Bakgrund

Patent- och registreringsverket (PRV) har i juni 2021 lämnat över en promemoria till den svenska regeringen med en kort lägesbeskrivning av området för artificiell intelligens (AI). I promemorian med titeln *”Artificiell intelligens & immaterialrätt – ett tankepapper från Patent- och registreringsverket”* belyser PRV med stöd av en expertgrupp utmaningar och möjligheter som AI har och kommer att ha över samhälls- och rättsutvecklingen och att det finns behov av en svensk strategi som har ett immaterialrättsperspektiv. PRV lämnade en rad rekommendationer till den svenska regeringen, bland annat att Sverige ska ta en aktiv roll inom ramen för arbetet i EU, WIPO samt WTO i frågor relaterade till AI och immaterialrätt. Vidare gavs rekommendationen att regeringen skulle överväga att: *”ge PRV, alternativt en särskild utredare, ansvar för en större utredning av tvärdisciplinär karaktär avseende immaterialrätt som konkurrensfördel vid AI-genererad innovation i ett tillväxtperspektiv”*.[1]

PRV:s roll inom upphovsrättens område

Sedan några år tillbaka har PRV ett uttryckligt uppdrag inom upphovsrätt, såväl avseende information och opinionsbildning som tillsyn. PRV har bland annat medverkat i internationella samarbeten inom upphovsrätt, lanserat webbplatsen streamalagligt.se, utformat utbildningar inom upphovsrätt, samt hanterat ett ärende om tillsyn avseende STIM:s tillämpning av graderingssystemet för fördelning av rättighetsintäkter. PRV:s roll inom upphovsrätt får anses väletablerad vid det här laget.

Innehållet i promemorian

Promemorian ger en mycket bra inledande översikt över området AI och viktiga rättsliga frågor i anslutning till immaterialrätt, framför allt patent och upphovsrätt. Bland annat beskrivs ärendena vid EPO och USPTO beträffande innovatören och ifrågasatta uppfinnaren DABUS. EPO kommer att påbörja prövningen av det överklagade beslutet i december 2021. Samma uppfinnare har nyligen befäst sin roll som uppfinnare vid patentverket i Sydafrika.[2] Sista ordet är uppenbarligen inte sagt i den här frågan. Arbetsgruppen bakom promemorian anser att det bör tas proaktiva åtgärder i lagstiftningsarbetet och *”inte enbart låta EU-domstolen samt EPO leda utvecklingen på rättsområdet med de begränsningar som eventuellt följer av det befintliga immaterialrättsliga systemet”*.

Förhoppningar på promemorian

Det tycks som PRV har bra förutsättningar att kunna ta ansvar för den föreslagna utredningen av tvärvetenskaplig karaktär. Behovet av harmonisering i ett större perspektiv är önskvärt vilket framgår mycket tydligt av promemorian men utgångspunkten förefaller fastna vid frågeställningen om AI som innovationsskapare eller hur skydd kan åstadkommas med bas i AI.

Inte mycket nämns om de konsekvenser som kan följa av att en immateriell rättighet skapats genom AI. Exempelvis hur uppdelningen av upphovsrätt i en ekonomisk och en ideell del påverkas, möjligheterna att kalla en AI i dess egenskap av upphovsperson eller uppfinnare som vittne i domstol, möjligheterna för en AI-robot att signera formella dokument beträffande överlåtelse eller avstående av rättigheter. Mer långsökta men tänkbara konsekvenser att eventuellt ta ställning till kan vara möjligheten för AI att bli ekonomiskt kompenserad för sin kreativa insats, att AI kan ha någon form av personlig integritet, att ha ett intresse att inte bli kränkt eller att åtnjuta dataskydd.

Låt oss hoppas att PRV eller den som får uppdraget att ansvara för en kommande utredning kommer att kunna belysa frågor som inte enbart har att göra med skapande av rättigheter utan även hantering av beviljade rättigheter.

Mariam Hussein, Associate & Gunnar Hjalt, Senior Counsel, Bird & Bird Advokat.

1 *https://www.prv.se/globalassets/in-swedish/om-oss/aktuellt/promemoria-kring-ai--immaterialratt-210527.pdf*

2 Patently brilliant... AI listed as inventor for first time | News | The Times

LOVDATA PRO

Lovdata Pro
- gratis ut året for nye kunder

pro.lovdata.no

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

Karnov Lovkommentarer, sømløst integrert i Lovdata Pro.

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

KOMMENTARENE

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

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

MER INFORMASJON

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

www.karnovgroup.no

KARNOV GROUP

BESTILL I DAG

Er du Lovdatakunde kan du bestille direkte gjennom Lovdata Pro.

https://pro.lovdata.no

LOVDATA PRO

Produksjon: 07 Media AS