

LOV & Data

Nr. 153
Mars 2023

Nr. 1/2023

Innhold

Leder 2

Artikler

Ingvild Ericson:
MyGame, strømming av breddeidrett og barns
personvern. 4

Erika Priimets:
The birth of digital society 9

Regine S. Antonsen og Stian H. Oddbjørnsen:
Lov og lootbokser – a lov(e) story?..... 12

Hanne Pernille Gulbrandsen, Steinar Østmoe
og Ole Martin Moe:
Kameraovervåking og særlige kategorier av
personopplysninger 19

Thale Cecilia Gautier Gjerdsbakk
Rettferdige algoritmer – matematikk og etikk 26

JusNytt 32

Halvor Manshaus:
Rettslig regulering av AI – ulike tilnærminger

Rettsinformatisk litteratur 38

Nytt om personvern 39

Nytt om immaterialrett. 52

Nytt om IT-kontrakter. 61

Nytt fra Lovdata. 68



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.lod.lovdata.no

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

Ansvarlig redaktør er Jarle Roar Sæbø

Medredaktør er Trine Shil Kristiansen, Lovdata.

Redaktører for Danmark er dr.juris Henrik Udsen ved Center for informations- og innovationsret, Københavns universitet og Tue Goldschmieding, partner i firmaet Gorrissen Federspiel, København.

Redaktør for Sverige er Daniel Westman, uavhengig rådgiver og forsker.

Fast spaltist er Halvor Manshaus, partner i advokatfirmaet Schjødt.

Trykk: ISSN 0800-7853

Elektronisk: ISSN 1503-8289

Utkommer med 4 nummer pr. år.

Abonnementspriser for 2023

Norge: nkr 385,- pr. år

Utlend: nkr 468,- pr. år

Studenter, Norge: nkr 182,- pr. år

Studenter, utland: nkr 244,- pr. år

Alle fritt tilsendt.

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

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

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

Trykk og layout: Aksell AS



Leder

Regelekspllosion – hvordan skal it-jurister gripe det an?

I de senere år har EU sat turbo på teknologireguleringen, og vi har fått en meget lang række retsakter, der enten er vedtaget eller ved at blive vedtaget. I realiteten startede denne bølge vel med databeskyttelsesforordningen (GDPR), men det har for alvor taget fart sig i de sidste par år med Data Governance Act, Digital Services Act, Digital Markets Act, NIS2-direktivet, DORA, AI Act og Data Act, hvoraf de første fem er vedtaget og de sidste to fortsatt er under forhandling. Hertil kommer en eventuel ePrivacy forordning, hvis skæbne fortsatt er ukendt, og en række andre reguleringsinitiativer, der er under forhandling, bl.a. Cyber Resilience Act, AI liability direktivet og nyt produktansvarsdirektiv.



Professor, dr.jur. Henrik Udsen, Det Juridiske Fakultet, Københavns Universitet

Der er mange, og også gode, grunde til, at vi netop nu ser denne regelekspllosion i teknologiregulerin-

gen. Dette omfatter behovet for privatlivsbeskyttelse i den digitale tidsalder, inddæmning af techgiganterne og deres monopolpræget adfærd, risikoen for cyberangreb, samfundsmæssige værn med misinformation og de potentielle skadevirkninger ved ny teknologi, herunder skærmafængighed, uhensigtsmæssig brug af AI mv. Samtidig må man efterhånden også blive bekymret for, om reguleringen er ved at blive så omfattende og kompleks, at ingen eller kun ganske få i realiteten kan overskue og gennemskue den – med den risiko for retssikkerheden dette indebærer.

Denne mere generelle bekymring bliver meget konkret, når man arbejder som it-jurist og dermed bliver mødt med forventninger om kendskab til netop denne type regler. For realiteten er jo nok, at ingen it-jurister i dag er i stand til at overskue alle disse nye regelsæt og have et mere indgående kendskab til dem alle. Hertil kommer der for mange nye regler på for kort tid, som er kendetegnet ved at være meget om-

fattende, ekstremt komplekse og med indbyrdes sammenhænge og overlap, der tilføjer et betydeligt lag af yderligere kompleksitet. Skal man hertil lægge afgørelser, vejledninger mv. for disse nye regelsæt i samme omfang, som vi har set med GDPR, kan man godt følge den tyske it-advokat, der som en kommentar til den nævnte udvikling indledte et meget delt LinkedIn-opslag med spørgsmålet »should I give up?«.

Det tror jeg ikke, at vi som it-jurister skal. Men der er utvivlsomt et behov for at overveje, hvordan vi metodisk griber denne udfordring an. Et godt udgangspunkt vil formentlig være en øget systematisering af de mange nye regelsæt og regler med udgangspunkt i de klassiske retsområder. It-retten har altid været tværgående i sin natur og fungerer i samspil med de mere klassiske vertikale retsdiscipliner. Det er i realiteten denne øvelse, som den nye generation it-ret står overfor. Øvelsen vanskeliggøres imidlertid af, at de nye regler etablerer helt nye retsdiscipli-

ner. Der er således ikke blot tale om at fordele de nye regler i velkendte kasser men også om at identificere ny kasser. Når dette nye landkort er optegnet, kan man bruge det til at »mappe« de mange nye regelsæt op imod de enkelte retsdiscipliner (hvorved man vil konstatere, at de enkelte regelsæt indeholder regler fra forskellige retsdiscipliner). Hermed vil der være skabt et udgangspunkt for, at den enkelte it-jurist kan vurdere, hvilke dele af de mange nye regler, den pågældende særligt skal koncentrere sig om. Jeg håber at kunne give mit eget bud på et sådant overblik i et af de kommende numre af Lov&Data men håber, at andre læsere også vil give deres bud – alternativt måske et helt andet bud på, hvordan vi håndterer regelekspllosionen. Eller skulle vi spørge Chat-GPT?

Henrik Udsen



MyGame, strømming av breddeidrett og barns personvern

Av Ingvild Ericson

1. Innledning

Diskusjonen rundt strømming av barn i breddeidrett, inntok nyhetsbildet med strømmetjenesten MyGames installasjon av automatiserte kameraer i idrettsanlegg i hele Norge.¹ MyGame er en strømmeplattform som strømmer kamper i en rekke lagidretter for visning på TV2 Play, i samarbeid med Norges idrettsforbund og seks særforbund.² Selskapet oppgir formålene med tjenesten primært å være spillerutvikling, økt engasjement for breddeidrett, samt bedring av klubbenes økonomi. Det fremheves også at organisert strømming er tryggere enn den ulovlige strømmingen som i dag allerede finner sted i stor skala.³

Protester fra flere hold medførte en midlertidig stans i filmingen av spillere under 18 år, og viste et behov for rettslige avklaringer knyttet til personvern. De synlige utfordringene omhandler eksponering av barn i lys av deres rett til et privatliv. De mindre synlige utfordringene omhandler potensialet for kommersiell masseinnsamling av personopplysninger gjennom smartkameraer. Spørsmålet er om regelverket åpner for databehandling med denne type personvernrisiko for barn.

All behandling av personopplysninger krever et rettslig grunnlag etter personvernforordningen (PVF).⁴ I denne artikkelen diskuteres krav til



Ingvild Ericson

behandlingsgrunnlag ved kommersiell strømming av barns breddeidrett, avgrenset til de mest relevante – berettiget interesse etter PVF art. 6 (1) f og samtykke etter PVF art. 6 (1) a. Artikkelen er aktualisert av MyGame, men belyser generelle spørsmål knyttet til strømming av barn.

” De synlige utfordringene omhandler eksponering av barn i lys av deres rett til et privatliv. De mindre synlige utfordringene omhandler potensialet for kommersiell masseinnsamling av personopplysninger gjennom smartkameraer.

2. Personvernregelverket gjelder

Personvernforordningen gjelder der personopplysninger behandles etter art. 4 nr. 1, hvilket krever at en person er «identifisert eller identifiserbar». Deltagerne i en

strømmet kamp er identifiserbare ved utseende, kombinert med nummer og navn på ryggen. Hva gjelder MyGame, er deres systemer videre integrert med idrettens systemer, slik at fullt navn automatisk vises ved lagoppstilling og sentrale kamphendelser.⁵ Strømming av barn i breddeidrett er dermed beskyttet under personopplysningsloven,⁶ som i § 1 gjennomfører personvernforordningen til norsk rett. I tillegg til forordningens generelle vern, skal det etter fortalepunkt 38 hensyntas at barn er en sårbar gruppe av registrerte «as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data». All tolkning etter forordningen skal reflektere barns særlige vern, slik dette også er forankret i FNs barnekonvensjon⁷ og i Grunnloven (Grl.)⁸ § 104 om barns «rett til vern om sin personlige integritet».

Personopplysningsvernet er likevel ikke absolutt, men må veies mot andre beskyttelsesverdige interesser. Personopplysningsloven § 3 gjør omfattende unntak fra loven ved behandling av personopplysninger for «journalistiske formål». Begrepet journalistikk skal tolkes vidt, og kan etter omstendighetene favne strømming av barn i idrett.⁹ Formidlingen må likevel være «nødvendig» av hensyn til yttrings- og informasjonsfriheten. Bestemmel-

1 Barn er personer under 18 år, jf. FNs Barnekonvensjon av 20-11-1989 art. 1.
2 Særforbundene for fotball, håndball, ishockey, basket, volleyball og bandy, se <https://mygame.no/personvernerklæring-kamper/>.
3 <https://mygame.no/trygg-strømming-av-breddeidretten/>.
4 For (EU) 2016/679.

5 Her foreligger felles behandlingsansvar, og behandlingsgrunnlag må foreligge også for slike formål.

6 Lov av 15. juni 2018 nr. 38.

7 Konvensjon av 20-11-1989.

8 LOV-1918-05-17.

9 Se bl.a. EU-domstolen C73/07, *Satakunnan Markkinapörssi and Satamedia*, avsnitt 61.

sen skal beskytte samfunnsdebatten i vid forstand, og veies mot retten til et privatliv.¹⁰ For MyGame er journalistikk kun et underordnet formål, hvilket i seg selv gjør unntaket uanvendelig.¹¹ Som diskutert nedenfor er strømming av barn i breddeidrett uansett utenfor kjernen av ytringsfriheten, på et område med høy grad av personvernrisiko. Avveid mot formidlingens begrensede bidrag til samfunnsdebatten, kan unntaket vanskelig anvendes på generelt grunnlag, selv om vurderingen for mer særegne arrangementer kan bli motsatt.

3. Berettiget interesse som behandlingsgrunnlag, jf. PVF art. 6 (1) f

MyGame påberoper berettiget interesse som behandlingsgrunnlag for strømmingen.¹² Etter PVF art. 6 (1) f kan det uten innhentning av samtykke behandles personopplysninger som er nødvendig for å ivareta en berettiget interesse som veier tyngre enn hensynet til den registrerte. Bestemmelsen er én av få i forordningen som direkte viser til forsiktighet der barn er involvert.

De fleste lovlige og fornuftig begrunnede interesser vil kunne anses berettigede etter bestemmelsen, og favne både økonomi, idrettsengasjement, spillerutvikling og reduksjon av ulovlig strømming – som vist til av MyGame.¹³ At databehandlingen må være «nødvendig», betyr likevel at den kun er tillatt dersom interessene ikke kan fremmes med mindre inn-

gripende tiltak. Hvis eksempelvis ulovlig strømming kan bekjempes på bedre måter enn å tillate organisert strømming, vil databehandlingen ikke være nødvendig.

De berettigede interessene må avveies mot den enkeltes personvern, i en bred vurdering av databehandlingens formål, omfang og konsekvenser.¹⁴ Tyngden av de berettigede interessene, vil bero på positive effekter for både selskapet og andre. Organisert strømming vil oppleves som et gode for mange i idretten og dens krets, og kunne bidra til opprydning i den uregulerte strømmingen som i dag tidvis er på kant med regelverket. Formidlingen er også vernet av retten til ytringsfrihet etter den europeiske menneskerettighetskonvensjon (EMK)¹⁵ art. 10 og GrL § 100, som etter sistnevntes annet ledd skal bidra til «sannhetsøken, demokrati og individets frie meningsdannelse». I kjernen av prinsippet står ytringer av allmenn interesse.¹⁶ Breddeidrett er - i motsetning til toppidrett - åpent for alle. Det strekker seg fra ungdom i lek, til satsing og talentspeidere. Den allmenne interessen vil kunne variere med resultater, sluttspill eller andre særegenheter. Samfunnsinteresse omfatter likevel ikke ethvert forhold noen finner interessant, og den jevne breddeidrettskamp er utenfor ytringsfrihetens kjerne. Dette har betydning i avveiningen mot retten til et privatliv etter GrL § 102 og EMK art. 8.

Av kriterier utviklet av den europeiske menneskerettighetsdomstol (EMD), kan det utledes at strømming av barn i breddeidrett medfører høy personvernrisiko.¹⁷ Dette skyldes blant annet høy eksponeringsgrad ved at barna er fullt identifiserbare, at personavbildning i seg

selv anses inngripende,¹⁸ og at eksponeringspotensialet er stort både i antall barn, timer og potensielle tilskuere. Bruk av videokameraer på borgerne er normalt underlagt svært streng regulering, og risiko for mobbing og deling på sosiale medier forsterkes der strømming også tilbys i opptak. Personvernet blir videre mer tilfeldig der ansvaret for stans av filming ved sårbare episoder ligger på foreldre i sekretariatet.¹⁹ Til dette kommer risiko for eksponering av barn som lever under beskyttelse. Selv om automatiserte systemer i slike situasjoner skal hindre strømming, er systemene ikke feilfrie. Det må tas hensyn til et sårbart mindretall, også om strømming for et flertall er positivt. Det må videre tas høyde for at timevis med strømming også kan avdekke særlige kategorier personopplysninger etter PVF art. 9, eksempelvis knyttet til biometri, helse eller etnisitet. PVF art. 9 regulerer behandling av opplysninger som etter sin kontekst kan oppleves særlig sensitive, og som ikke kan forankres i behandlingsgrunnlaget berettiget interesse.

I tillegg til risikoen ved selve eksponeringen, foreligger et åpenbart potensiale for kommersiell bruk av personopplysningene utover hva som er nødvendig for strømmingen. I en digital økonomi der slike data har enorm markedsverdi, må balansen reflektere risikoen for at det omfattende datamaterialet kan bli brukt eksempelvis til utvikling av individuelle spilleranalyser, eller som råvare til «overvåkningsøkonomien» med aktører som Facebook og Google i front. I den anledning bemerkes at enhver databehandling etter forordningen er underlagt grunnleggende krav til åpenhet og formålspresisering etter PVF art. 5 (1). En kommersiell aktør er rettslig av-

10 Jf. PVF art. 85, Prop. 158 L (2020-2021) *Endringer i personopplysningsloven og offentleglova (ytrings- og informasjonsfrihet mv.)* pkt. 1, 3.6.2 og 3.5.3 om at journalistikk må være det hovedsakelige formålet. Ordlyden ble endret i 2021, bl.a. for å hindre at det i uforholdsmessig stor grad ble gjort unntak for slike formål.

11 <https://mygame.no/personvernerklaering-kamper/> pkt. 7.

12 Ibid. pkt. 8.

13 Se Artikkel 29-gruppen *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* pkt. III.3.1.

14 Ibid. pkt. III.3.4 og III.3.5.

15 Konvensjon av 04-11-1950.

16 Wessel-Aas og Ødegaard, *Personvern Publisering og behandling av personopplysninger* (2018) kap. 4.2.

17 Ibid. kap. 5.4 med videre henvisninger.

18 EMD von Hannover v. Germany (no. 2) (40660/80 and 60641/08) avsnitt 96.

19 <https://mygame.no/slik-skal-mygame-stromme-breddeidretten/>.

skåret fra bruk av personopplysningene til andre formål enn hva som i forkant er formidlet, også ved bruk av ny teknologi. Bevissthet knyttet til klare presiseringer i formålsangivelse og partenes avtaler, vil dermed kunne dempe risikoen.

” I tillegg til risikoen ved selve eksponeringen, foreligger et åpenbart potensiale for kommersiell bruk av personopplysningene utover hva som er nødvendig for strømmingen.

Risikoreduserende tiltak kan avgjøre om berettiget interesse kan påberopes. Det må vurderes om de aktuelle interessene kan ivaretas også om man reduserer graden av identifiserbarhet (eksempelvis ved å fjerne barnas navn), og graden av eksponering (eksempelvis ved å begrense fremvisning til lagets egen krets, ved kun å strømme i sanntid, eventuelt kombinert med opptak i et begrenset antall dager for laget selv). Det bør samtidig skilles mellom breddekamper etter sin nyhetsverdi og inngripen i personvernet. En eventuell reservasjonsrett vil også fungere risikodempende. Idrettens digitale systemer er eksempelvis forhåndsinnstilt på å tillate strømming fra MyGame, og spillerne kan anonymt velge seg ut av tjenesten. En reservasjonsrett vil likevel kun fungere etter sin hensikt ved fravær av press fra fellesskapet om ikke å benytte den. Dette i likhet med kravet til frivillighet som vilkår for et samtykkes gyldighet, vurdert nedenfor.

Under enhver omstendighet skal interesseavveiningen tydelig vise hvordan et barns særlige vern er avveid mot interessene i å eksponere det. Fravær av en slik avveining fikk EMD til å konstatere brudd på barnets rett til privatliv etter EMK art. 8

i I.V.T. v. Romania.²⁰ Konkret for MyGames personerklæring betyr dette at et fokus kun på påberopte berettigede interesser, uten en synlig avveining mot barnets beskyttelse, ikke er tilstrekkelig.²¹

Strømming av barn i breddekamper, innfører en ny normaltilstand av eksponering med høy personvernrisiko. Det følger av rettskildet bildet at behandlingsgrunnlaget berettiget interesse da har begrenset anvendelse. Uten en nærmere differensiering av breddekamper basert på nyhetsverdi og risiko, kan jeg ikke se at berettigede interesser på generelt grunnlag veier tyngre enn personvernrisikoen for den enkelte. Jeg kan dermed heller ikke se at behandlingsgrunnlaget er anvendelig.

4. Samtykke som behandlingsgrunnlag, jf. PVF art. 6 (1) a

Også samtykke er et relevant behandlingsgrunnlag å vurdere ved strømming av barn for offentlig fremvisning. Et samtykke skal være en villet handling, og et utslag av den enkeltes selvbestemmelsesrett. Det stilles derfor strenge krav til både rettslig handleevne og materiell gyldighet.

Reglene for rettslig handleevne er i liten grad harmonisert på EU-nivå, og reguleres derfor av nasjonal rett.²² I norsk rett er aldersgrensen for å «foreta rettslige handlinger» 18 år etter vergemålsloven § 9.²³ Bestemmelsen omfatter kompetanse til å samtykke til behandling av personopplysninger, og skal beskytte mot både rett og plikt til å inneha et ansvar den mindreårige mangler modenhet til å forstå.²⁴

20 EMD (2022 - 189) avsnitt 59, 62.

21 <https://mygame.no/personvernerklæring-kamper/> pkt. 8.

22 Se f.eks. 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» pkt. 2.1 og 1.2.

23 LOV-2010-03-26-9.

24 Ot.prp. nr. 110 (2008–2009) s. 172.

Bestemmelsen åpner for unntak. Et slikt unntak blir tidvis innfortolket i barneloven²⁵ § 33, om at barn har rett til gradvis økt selvbestemmelse i tråd med egen utvikling. Sett i sammenheng med barneloven § 30 gjelder bestemmelsen likevel kun «personlege tilhøve», og betyr at barn etter en individuell vurdering kan samtykke til avbildning og begrenset eksponering. Da et samtykke til strømming for offentlig fremvisning ikke er å anse som personlige forhold, er bestemmelsen likevel ikke anvendelig. Det ville da også vært praktisk umulig for en strømmeprodusent å vurdere det enkelte barns modenhetsnivå.

Et viktig unntak i barns digitale hverdag følger av PVF art. 8 og personopplysningsloven § 5, som gir norske barn samtykkekompetanse fra fylte 13 år ved bruk av de fleste online tjenester - som sosiale medier. Å bruke en tjeneste er imidlertid noe annet enn å være produktet for den, og aldersgrensen gjelder ikke eksponering gjennom strømming.²⁶ Aldersgrensen gjelder heller ikke behandling av særlige kategorier personopplysninger etter PVF art. 9, og en person under 18 år kan altså ikke samtykke til strømming dersom slike forhold avdekkes.²⁷

” Å bruke en tjeneste er imidlertid noe annet enn å være produktet for den, og aldersgrensen gjelder ikke eksponering gjennom strømming.

Jeg kan heller ikke se at det finnes relevante aldersgrenser i særlovgivningen, for verken direkte eller

25 LOV-1981-04-08-7.

26 Se også Kirsten Kvalø «Barns rett til selvbestemmelse etter ulike aldersgrenser» 2022 pkt. 3.2.

27 Se Ingvild Ericson «Barns samtykkekompetanse på personvernfeltet» Utredning for Personvernkommissjonen 2022 pkt. 2.2.2 med videre henvisninger.

analogisk anvendelse. Et barn kan etter barneloven § 32 avgjøre foreningsmedlemskap fra fylte 15 år, og med en slik kompetanse bør innfortolkes en samtidig rett til behandling av nødvendige personopplysninger. Da strømming for offentlig fremvisning likevel ikke er en nødvendig konsekvens av medlemskap i idrettens forbund, kan bestemmelsen ikke brukes.

Datatilsynet har inntil nylig gitt uttrykk for en generell personvernsmessig 15-årsgrense. En slik aldersgrense vil gi klarhet i en fragmentert rettstilstand, men er omdiskutert, har en uklar rettslig forankring, og er ikke lenger omtalt på tilsynets nettsider.²⁸ I fravær av relevante unntak, og i påvente av en helhetlig rettslig regulering av samtykkespørsmålet, bør det derfor innhentes foreldresamtykke for strømming av personer under 18 år for offentlig fremvisning – en kompetanse som skal utøves i tråd med barnets beste og barnets medbestemmelsesrett.²⁹

Et samtykke må videre være gyldig etter definisjonen i PVF art. 4 nr. 11, om et samtykke som en «frivillig, spesifikk, informert og utvetydig viljesytring». Samlet skal kravene sikre et reelt *ønske* om en aktuell databehandling.³⁰

Fordi folk flest sjelden endrer standardinnstillingene i en digital tjeneste, vil samtykkeraten påvirkes av om innstillingen binder ved aktivitet (opt-in) eller passivitet (opt-out). Skal samtykket bygge på et bevisst valg, kreves derfor en «*utvetydig*» og aktiv handling, som å klikke eller hake av i en boks. Forhåndsinnstillinger i idrettens digitale systemer som tillater strømming ved passivitet – som for reservasjonsretten omtalt under berettiget interesse – oppfyller dermed ikke vilkåret.

28 Ibid. pkt. 2.1.3.1.

29 Grt. § 104, FN's barnekonvensjon art. 3 og 12 og vgml. § 17 (4).

30 Personvernrådet «*Guidelines 05/2020 on consent under Regulation 2016/679*» pkt. 3.4.

Samtykket må videre være «*informert*», så den enkelte kan forstå hva det samtykkes til. Spesielt sentralt er informasjon om hva personopplysningene skal brukes til, og det kreves at samtykket er en «*spesifikk*» viljesytring knyttet til et klart og presist formulert formål.

Kravet til at et samtykke skal være «frivillig», innebærer fravær av press eller risiko for negative konsekvenser.³¹ Vilkåret skaper utfordringer i lagidrett, rett og slett fordi mennesker er ulike. På et lag vil trolig en rekke samtykker på individuell basis være frivillige. Reell valgfrihet skal likevel foreligge også for dem som ikke ønsker strømming. Fordi en kamp kun filmes der alle deltagere på banen har samtykket, vil ett uteblitt samtykke blokkere for alle. Selv om samtykkeløsningen er anonym, må man ved spørsmål fra lagkamerater enten lyve eller tåle rollen som «syndebukk». Dette skaper et press som i praksis gjør det umulig å dokumentere at samtlige samtykker på et lag er frivillige, og dermed gyldige.

Samtykke er derfor lite egnet som behandlingsgrunnlag i lagidrett. Det kan likevel være påkrevet etter en norsk særregel i åndsverkloven (åvl).³² I det følgende diskuteres om



Fordi en kamp kun filmes der alle deltagere på banen har samtykket, vil ett uteblitt samtykke blokkere for alle. [...] Dette skaper et press som i praksis gjør det umulig å dokumentere at samtlige samtykker på et lag er frivillige, og dermed gyldige.

31 Ibid. pkt. 3.1.2 og PVF fortalepunkt 42.

32 LOV-2018-06-15-40.

strømming for offentlig fremvisning krever samtykke etter åvl. § 104 om retten til eget bilde.

5. Kreves samtykke etter åndsverkloven § 104 om retten til eget bilde?

Åndsverkloven § 104 verner retten til eget bilde, og krever samtykke ved publisering av fotografi eller film som «avbilder en person». Strømming av identifiserbare deltagere for offentlig fremvisning er omfattet av hovedregelen.³³ Også denne personvernbestemmelsen må imidlertid veies mot retten til ytringsfrihet, jf. unntak i første ledd bokstav a-c. Bokstav a om «*aktuell og allmenn interesse*» krever en bred interesseavveining av hensynene til ytringsfrihet, allmennhetens informasjonsinteresse og den avbildedes personvern. Som vurdert under berettiget interesse, finner jeg ikke at slik allmenn interesse foreligger for den jevne breddekamp, vurdert opp mot ytringsfrihetens kjerne.³⁴ Jeg kan heller ikke se at «*personen er mindre viktig enn hovedinnholdet i bildets*» etter bokstav b. Unntaket brukes primært der de avbildede inntar en birolle i et annet hovedmotiv, som der tilfeldige turister avbildes ved et kjent bygg.³⁵ Det kan i lagidrett argumenteres for at den enkelte person er mindre viktig enn hovedinnholdet, som er kampbildet som sådan. Eksempelvis viser MyGame til at strømmingen har fokus «på spillet og idretten, og ikke på enkeltindivider».³⁶ På den annen side er motivet lite annet enn nettopp summen av personene. Blikket vil videre dras mot den som til enhver tid fører spillet, som med dette blir bildets hovedmotiv. At

33 Wessel-Aas og Ødegaard, *Personvern Publisering og behandling av personopplysninger* (2018) kap. 6 med videre henvisninger. Se Rt. 1995 s. 1948 (Diana Ross) s. 1953 om at film omfattes.

34 Ibid.

35 Ibid. kap. 6.5.

36 <https://mygame.no/personvernerklaering-kamper/> pkt. 8.

bokstav c gjør unntak for «forsamlingen» og «folketog» viser videre at unntak for menneskelig aktivitet er forbeholdt større samlinger av mennesker. Jeg kan med dette ikke se at hovedregelens samtykkekrav kan fravikes på generelt grunnlag.

Åndsverksloven § 104 er ikke del av personvernforordningen, og påvirker ikke direkte et behandlingsgrunnlags gyldighet etter PVF art. 6 (1). Bestemmelsen kan likevel være avgjørende for en tjenestes lovlighet, da strømming av barn for offentlig fremvisning i Norge krever både samtykke etter åvl. § 104 og behandlingsgrunnlag etter PVF art. 6. Med forordningens strenge samtykkekrav, vil et samtykke etter PVF art 6 (1) a oppfylle vilkårene etter begge regelsett. Bruk av berettiget interesse som behandlingsgrunnlag etter PVF art. 6 (1) f, vil derimot

også kreve innhenting av samtykke etter åvl. § 104.

6. Avslutning

Slik jeg ser det, er det vanskelig å etablere rettslig grunnlag for å innføre en normalsituasjon av strømming og offentlig fremvisning av barn i breddekamper. Bruk av barns samtykke er vanskelig både i lys av kravet til frivillighet og manglende rettslige handleevne. Bruk av berettiget interesse er ikke anvendelig der det i stor grad gripes inn i barns personvern. Det er ovenfor vist til en rekke risikofaktorer. Retten til privatliv er en individuell rettighet som skal verne et sårbart mindretall, også om effekten for et flertall er positiv. Jeg kan ikke se at de berettigede interessene på generelt grunnlag veier tyngre enn hensynet til barnas personvern.



Retten til privatliv er en individuell rettighet som skal verne et sårbart mindretall, også om effekten for et flertall er positiv.

Flere av de rettslige spørsmålene hviler likevel på avveininger av personvern mot andre beskyttelsesverdige interesser. Strømming er ikke et spørsmål om ja eller nei. Risikoreduserende tiltak kan minske både eksponerings- og identifiseringsgrad, og følgelig påvirke de rettslige vurderingene. Eventuell strømming må da skje i lys av klare formålsangivelser, og avtaler som avgrenser videre kommersiell bruk av personopplysningene.

The birth of digital society

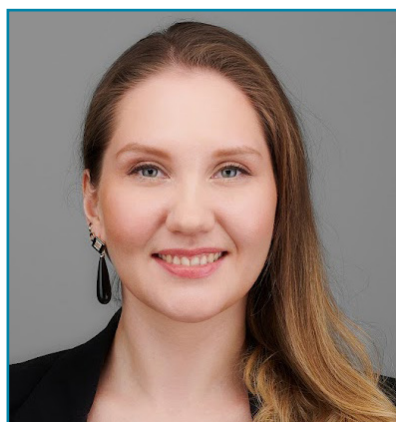
Av Erika Priimets

Estonia, a tiny Nordic country that became re-independent in 1991, was confronted with a dilemma – either to try its best catching up to developed modern states using the traditional building blocks or try to accelerate the growth through different approach no one had ever tried before. Digital by default vision was then adopted and digital-minded leadership allowed to steer the country through agile and pragmatic decision-making focused on problem-solving and “let’s do it” mentality.

This approach has led Estonia to be among the most digital societies in the world, a benchmark for many, and a leader in digital public services, according to DESI 2021 report (source: Digital Economy and Society Index (DESI) 2021 | Shaping Europe’s digital future (europa.eu)). But applying technology has never been the goal on its own, rather focusing strongly on the citizen-centric mindset, a fundamental principle that has guided Estonia’s digital strategy.

” Digital by default vision was then adopted and digital-minded leadership allowed to steer the country through agile and pragmatic decision-making focused on problem-solving and “let’s do it” mentality.

Naturally, digital society and its services run on data. However, during the era of data overload we must keep in mind that only quality data is what we are after. Quality,



Erika Priimets

meaning structured, systemised, described, and standardised data enables the intertwined blood circle of complex digital services. Decentralised governance model, where different spheres of life are governed by ministries while keeping relevant databases and key registries in the domain of the certain ministry, is the common administrative practice for many countries. Also, the shared concern is that data needed to provide several services (online or offline, alike) is not always kept in the domain of a certain ministry offering the service.

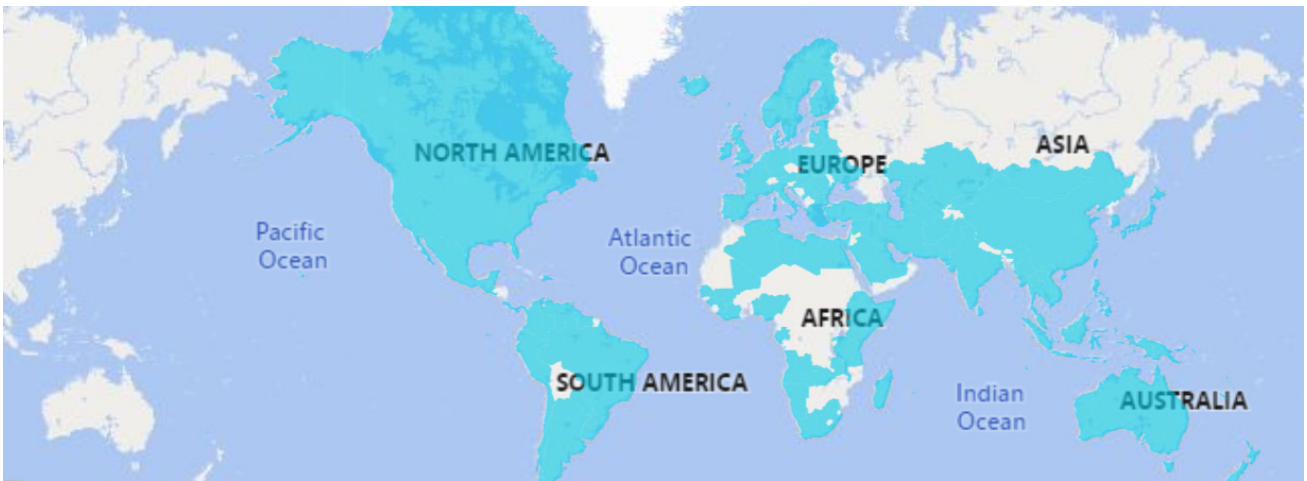
In case of lacking information, the obvious source to turn to retrieve relevant data, is the party possessing the correct and updated data – specifically meaning, the citizen about to consume the service. However, Estonia has purposefully designed its legislative system keeping in mind the **once only principle**. Simply put, the citizen’s responsibility is to provide a government authority with their personal information only one time. From there, the authorised institutions must figure out a way to share the corresponding data while needed to provide an overlapping service.

” But applying technology has never been the goal on its own, rather focusing strongly on the citizen-centric mindset, a fundamental principle that has guided Estonia’s digital strategy.

Interoperable by demand

Sharing data is a pragmatic and understandable concept, making it efficient, convenient, and secure is a whole other challenge, requiring the desire for cooperation, clear guidelines, and standards. Providing digital services and exchanging different quantity and quality of data is something that many other governments in the world are doing. What sets Estonia apart from many is an interoperable wholesome infrastructure of connected all public institutions, obligated by law, and many private companies, joined voluntarily due to value proposition enhancing their services.

The X-Road, a secure and interoperable data exchange platform, is a modular API-based middle layer software connecting distributed data holders to service providers seamlessly in real time. While every institution manages its own processes, government institutions can decide independently which platforms and technologies they use over X-Road. This decentralised approach means that there is not one big super-database which would be extremely attractive for hackers. All data transfers are end-point to end-point encrypted. And we can see that Estonia is on the right track



” The X-Road, a secure and interoperable data exchange platform, is a modular API-based middle layer software connecting distributed data holders to service providers seamlessly in real time.

because many other countries have gotten onboard with our solution – international X-Road network amounts to 2693 participating members, serving over 253M end-users globally [source: X-Road World Map — X-Road® Data Exchange Layer]. Estonia has been using the X-Road as the backbone of our digital society already from 2001, setting a standard for interoperable processes, that so many other countries are looking to implement nowadays.

Digital infrastructure as a value

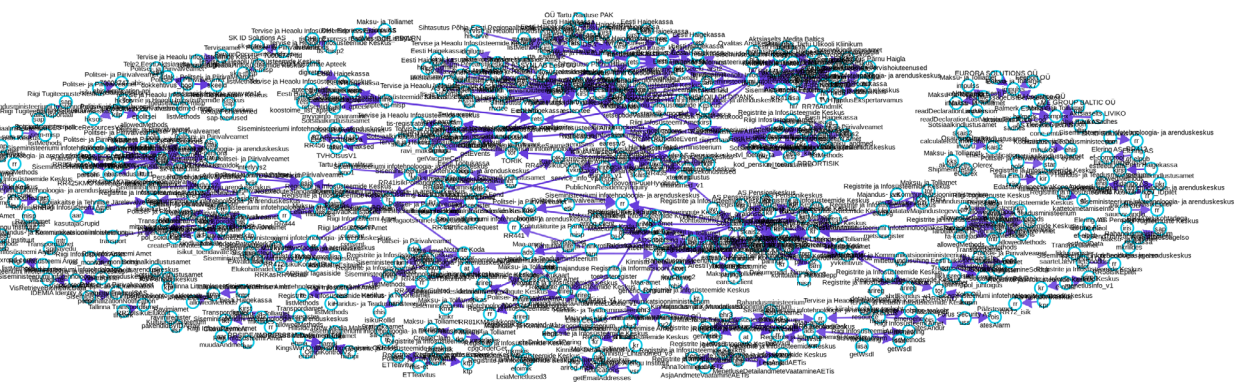
I get asked often to name my favourite e-service in Estonia, and I must disappoint – every digital service is a step towards convenience but my most appreciated aspect is the wholesome functioning ecosystem where I would not point out any specific service. I strongly believe in automated processes running the operations, instead people manually engaging in them. The state of my dreams works on the background and delivering me value through proactive and life event-based services. X-Road ecosystem delivered over 2.2B requests in 2022, which makes on average 1700 requests per Estonia’s citizen – would you imagine submitting your personal data and filling applications roughly 140 times by hand every month? [data source: X-TEE FACTSHEET EE].

The first milestone of developing e-services meant enabling different systems to communicate with each other, but life-event/business-

event services are activated automatically based on the events taking place in a person’s life, instead the end-user having to turn for every institution themselves.

Overlapping and automatically triggered services, however, do not happen by default after the technology necessary has been implemented. Instead, it requires a genuine will for collaboration, setting egos aside and working in unity through digital-minded leadership, focusing on delivering value to the user, rather than feeding a political agenda to show *something* as a result of the time in cabinet.

We could have a friendly laugh on Estonians’ expense, saying, of course the closed introverted people decided to digitise all public services to never ever having the need to leave their homes, and God forbid, have a face-to-face communication while running their errands. Perhaps there might be a touch of truth in this pun, but I personally would much rather fill my socializing need



from interacting with my family and friends, instead quarrelling with a Tax Authority officer over the blanks on my declaration form.

The amount of digital services available for the end-users does not deliver any value on its own. The time and location independent secure access to these services for whomever might need them is the true value proposition from the e-government. A citizen's privacy to access their services independently is respected, and their freedom of choice to engage either via physical or virtual service is granted. The debate about necessity of a digital infrastructure does not start with choosing technology, it starts with the political agreement based on values stating how a state should serve its citizens.

Secure by design

Digital infrastructure, however convenient, comes with plenty of risks and requires constant attention due to rapid advancement of technology. Estonia decided to apply digital-first strategy, meaning offline services have the digital alternative. In spite of all the convenience it brings, none of it can come by sacrificing an inch of security.

'Do Estonia use Blockchain?', is a frequent question while discussing security. The answer is yes, but not like you might think. We do not store personal data on the Blockchain as that would be a data protection and privacy nightmare. Instead, all the data exchanges, M2M communications, data at rest, and log files are independently and fully accountable thanks to Blockchain-like technology. With KSI Blockchain, provided by Estonian blockchain company Guardtime, deployed in Estonian government networks, history cannot be rewritten by anybody, and the authenticity of the electronic data can be math-

ematically proven. It means that no one – not hackers, not system administrators, and not even the government itself – can manipulate the data and get away with it. Integrity of data is one of the strongest principles tied to e-governance.

Another cornerstone of e-Estonia is its secure cyberspace. Naturally, a digital society will be exposed to cyber threats. With solid investments in cyber security infrastructure, Estonia has developed extensive expertise in this area, becoming one of the most recognised and valued international cyber security experts. Did you know that the average discovery of data breaches takes around 7 months around the world? Thanks to Estonian Blockchain technology these breaches can be discovered instantly.



'Do Estonia use Blockchain?', is a frequent question while discussing security. The answer is yes, but not like you might think.

Start with WHY, but show HOW

Estonian society was not born digital and we had to start teaching information literacy to students with Tiger Leap and the elderly with Look@World programs to help them learn to consume e-services.

Estonia aims to implement modern digital technology more efficiently and effectively in learning and teaching to improve the digital skills of the entire nation. Estonia has also adopted a lifelong learning strategy because the modern world needs more tech-savvy users. Thus, both state and private sector companies offer a variety of (often free) IT-courses for enthusiasts of any age. This gives the opportunity for

people to educate themselves and increase their IT skills while making it easier to make the necessary changes in their career choices and make e-services as a natural part of their lives.

No one is born with a digital gene and forming new digital habits need support and is not immediate. Developing skills takes time, as we are still working on it over 20 years later from implementing e-services. However, just because it is complicated and time-consuming, does not mean we should not put the effort in developing the essential skills that is fundamental in forming the digital habits of the people.

With giving all the credit to the importance of training, it is worth highlighting the underlying goal. The double-check question to see if you are on the right track could be something like this – am I driving technology, or does the technology build a convenient enjoyable customer path for my users?



The double-check question to see if you are on the right track could be something like this – am I driving technology, or does the technology build a convenient enjoyable customer path for my users?

Starting by understanding the end-user's needs and eliminating bottle necks are definitely good indicators to look for while building a successful functioning e-state.

Erika Piirmets, Digital Transformation Adviser at e-Estonia Briefing Centre.

Lov og lootbokser – a lov(e) story?

Av Regine S. Antonsen og Stian H. Oddbjørnsen

1. innledning

Pengespill er regulert på nasjonalt nivå, og utgangspunktet i norsk rett er simpelthen at pengespill er forbudt. Det er likevel slik at lovgivningen tillater at Norsk Tipping og Norsk Rikstoto tilbyr statlig kontrollerte pengespill. Med ny pengespillov¹ som trådte i kraft 1. januar 2023 ble enerettsmodellen videreført og styrket.²

Samtidig som ny pengespillov er blitt vedtatt, har rask teknologisk utvikling ført til at det har oppstått uklare grenser mellom dataspill og pengespill. Spillselskapenes inntekter har historisk sett hovedsakelig vært knyttet til salg av spill. Men, den senere tiden har verktøyene for å lage dataspill blitt tilgjengelig for flere, og kombinert med nye mobile plattformer og digital distribusjon, har dette ført til at antall spill i markedet har økt enormt, mens spillerens betalingsvilje for selve spillet har gått drastisk ned.³ De senere årene har det derfor utviklet seg forretningsmodeller som baserer seg på kjøp i *dataspillet*, herunder kjøp av såkalte *lootbokser*. I 2020 genererte salg av lootbokser på verdensbasis om lag 150 milliarder kroner i inntekt for spillselskapene.⁴

Det finnes ikke en ensartet definisjon av hva som utgjør en loot-



Regine S. Antonsen

boks. I teorien er det tatt til orde for at nettopp dette skaper et problem som gjør det vanskelig å regulere bruken av lootbokser⁵. Vi kommer tilbake til hva en lootboks er nedenfor, men kort forklart er det lotterilignende belønningsmodeller i dataspill, som inneholder virtuelle gjenstander som er ukjente frem til boksen åpnes. Lootboksene kan kjøpes for ekte penger eller spillvaluta, eller de blir delt ut gratis når spilleren når bestemte mål.⁶

Naturlig nok har bruk av lootbokser blitt stadig mer populært i spillindustrien som en måte å tjene penger på utover den opprinnelige summen for kjøp av spillet. Mens bruk av lootbokser har vist seg å være en lønnsom strategi for spillutviklere, har det også skapt kontroverser. På grunn av likhetene med pengespill, og risikoen for at lootbokser fremmer spillavhengighet og introduserer barn og unge til spillmekanismer som i stor grad likner gambling, er det blitt tatt til

5 Are Loot Boxes Gambling? Random Reward Mechanisms in Video Games (2018) Lundedal Nielsen og Grabarczyk s. 2.
6 Prop. 220 L (2020-2021) punkt 5.3.1.



Stian H. Oddbjørnsen

orde for at lootbokser bør vurderes opp mot pengespillovgivningen.⁷

Spørsmålet vi stiller i denne artikkelen, er hvorvidt ny pengespillov åpner for at lootbokser kan vurderes opp mot definisjonen av hva som utgjør *pengespill* i § 2, og dermed være underlagt pengespillovgivningen. Dersom det viser seg at noen eller alle typer av lootbokser faller innenfor definisjonen av *pengespill*, innebærer det i praksis at det er ulovlig å tilby kjøp av disse lootboksene i Norge.

” Spørsmålet vi stiller i denne artikkelen, er hvorvidt ny pengespillov åpner for at lootbokser kan vurderes opp mot definisjonen av hva som utgjør pengespill i § 2, og dermed være underlagt pengespillovgivningen.

7 Se for eksempel UK Gambling Commission (2018) og Insert Coin (2022), Forbrukerrådet og Prop. 220 L (2020-2021) punkt 5.3.1.

1 Lov 18. mars nr. 12 om pengespill (pengespilloven).

2 Prop. 220 L (2020-2021) Lov om pengespill (pengespilloven) punkt 2.2.

3 Rapport om gråsonespill (2018) Forum for spilltrender, punkt 1.

4 Loot boxes: How the gaming industry manipulates and exploits consumers (2022) Forbrukerrådet, tilgjengelig her: <https://www.forbrukerradet.no/siste-nytt/loot-boxes-how-the-gaming-industry-manipulates-and-exploits-consumers/>

I det følgende skal vi vurdere om noen eller alle typer av lootbokser faller innenfor definisjonen av *penge-spill*. I denne vurderingen skal vi først på en kortfattet måte forklare hva en lootboks er, før vi deretter redegjør for formålet med penge-spillovgivningen og vurderer om lootbokser oppfyller vilkårene for å anses som et pengespill. Til sist konkluderer vi kort om hvorvidt lootbokser møter lov(e) i Norge.

2. Overordnet om hva en lootboks er

En lootboks er en virtuell forandringspakke som kan kjøpes i noen dataspill. Lootbokser inneholder virtuelle gjenstander som vanligvis er ukjente frem til «boksen» åpnes. Slike bokser kan kjøpes for ekte penger eller spillvaluta, eller de blir delt ut gratis som en form for belønning når spilleren når bestemte mål.⁸ I de tilfellene hvor en lootboks kan erverves gratis, tilbys den også tilnærmet alltid i en butikk-funksjon hvor den kan kjøpes for spillvaluta som veldig sjeldent svarer med ekte penger. Ettersom innholdet i lootboksene er ukjent, vet spilleren aldri hvor mange lootbokser som må erverves eller kjøpes og åpnes for spilleren teoretisk sett får den *ønskede* premien. Målet er ofte å dele ut lootbokser med høy nok frekvens til at spilleren alltid føler at de er nærmere en svært attraktiv gjenstand, men holde sjansen lav nok til at spilleren blir oppmuntret til å gjøre prosessen raskere gjennom kjøp av flere lootbokser⁹.

Det finnes flere kategorier av lootbokser, og selv om de aller fleste har visse fellestrekk, er det store variasjoner mellom hvordan belønningsmodellen er implementert i spillene. *Forum for spilltrender* har identifisert likhetstrekk ved noen av

belønningsmodellene og kategorisert visse lootbokser i lys av fellestrekkene.¹⁰

Den første kategorien som *Forum for spilltrender* har identifisert handler om hvilken funksjon belønningene som spilleren mottar ved å åpne en lootboks har i spillet. Det skilles ofte mellom kosmetiske belønninger og belønninger som gir spilleren tilgang på oppgraderinger eller nytt innhold. Kosmetiske belønninger gir tilgang på visuelle elementer som ikke gir noen fortrinn i spillet som sådan, men det kan likevel ha verdi for spilleren og gi spilleren status innad i spillet.

Motsatsen er belønninger i form av oppgraderinger som gir tilgang på nye eller bedre figurer, evner, skjulte spillsekvenser, våpen eller liknedne. Dette vil enten gi spilleren et fortrinn i spillet, eller la spilleren oppleve nytt innhold. Slike belønninger er det i større grad pekt på at kan skape de samme problemene som tradisjonelt pengespill. Det er fordi de etablerer en direkte kobling mellom pengebruk og prestasjon. Spillentusiaster omtaler ofte denne typen spill eller mekanisme med den nedsettende betegnelsen «*pay-to-win*»¹¹.

Den andre kategorien, handler om hvorvidt belønningene fra en lootboks har en *økonomisk verdi*. *Forum for spilltrender* peker på at dette spørsmålet er tett knyttet til de enkelte spillenes forretningsmodell, og til om det er mulig å konvertere digitale gjenstander eller valutaer til ekte penger. I mange dataspill er svaret nei, ettersom gjenstander er låst til spillerkontoen uten mulighet for byttehandel mellom spillere. Men, det finnes spill hvor konvertering til økonomiske verdier er mulig, enten direkte gjennom spillers offisielle auksjonssystem eller indirekte gjennom uoffisielle svartebør-

ser på nett.¹² I slike tilfeller vil det være vanskelig å avgjøre om økonomien i spillet er lukket på en slik måte at verdier innad i spillet ikke kan konverteres til en verdi utenfor spillet. Dette har betydning for hvorvidt pengespillovgivningen kommer til anvendelse, noe vi kommer tilbake til nedenfor i punkt 3.

Som et eksempel på et spill som til viss grad åpner for at verdier innad i spillet kan konverteres til en verdi utenfor spillet, er fotballspillet FIFA. I dette spillet kan spillere kjøpe og selge spillerkort fra lootbokser til hverandre gjennom et offisielt auksjonssystem. Dette systemet tillater kun bruk av virtuell valuta, og lar ikke spillere konvertere verdier til ekte penger. Det finnes imidlertid uoffisielle kanaler som tilrettelegger for bytte og salg av virtuell valuta i FIFA på eksterne nettsider og auksjoner.

Et eksempel på et annet spill er *Counter-Strike Global Offensive (CS:GO)* som legger til rette for kjøp og salg av virtuelle gjenstander gjennom auksjonssystemet på den digitale plattformen «*Steam*». Pengene spillerne tjener på slikt salg, kan ikke tas ut av *Steam*, men kan brukes ved fremtidige kjøp av dataspill eller virtuelle gjenstander på lik linje med andre betalingsmidler. *Forum for spilltrender*, sammenlikner denne spilløkonomien med en type *gavekort*. Det finnes også her et svart marked for direktehandel og nettkasinoer med gjenstander fra *CS:GO* og andre dataspill som benytter seg av *Stems* auksjonssystem.

” Som et eksempel på et spill som til viss grad åpner for at verdier innad i spillet kan konverteres til en verdi utenfor spillet, er fotballspillet FIFA.

8 Spillerom – Dataspillstrategi 2020-2022 (2019) Kulturdepartementet side 5.

9 Lotterimekanismer i videospill (2021), Rydland s. 7.

10 *Forum for spilltrender Rapport om gråsonespill* punkt 3.

11 *Forum for spilltrender Rapport om gråsonespill* punkt 3.1.1.

12 *Forum for spilltrender Rapport om gråsonespill* punkt 3.1.1.

Spørsmålet er om spillene som faller innenfor de ovennevnte kategoriene, samt også andre spill hvor det tilbys kjøp av lootbokser, faller innenfor pengespillovens definisjon av *pengespill* i § 2.

3. Kan en lootboks anses som «pengespill»

3.1 Lootbokser og formålet med pengespillovgivningen

Det følger av ny pengespillov § 1 at formålet med lovgivningen er å

«(a) forebygge spillproblemer og andre negative konsekvenser av pengespill, (b) å sikre at pengespill gjennomføres på en ansvarlig og trygg måte og (c) å legge til rette for at overskudd fra pengespill går til ikke-fortjenestebaserte formål».

Det overordnede målet med å regulere markedet for pengespill i Norge er å sikre at pengespill blir tilbudt i trygge og ansvarlige former for å begrense spillavhengighet og sørge for at spill som blir tilbudt ikke fører til at flere utvikler problemer med spillavhengighet. Særlig legges det vekt på å skjerme barn og unge fra å utvikle spilleproblemer.

Det følger av forarbeidene til ny pengespillov at forskere har pekt på at det er sammenheng mellom lootbokser og problemspill på pengespillområdet. Forskningen sier imidlertid ingenting om hvorvidt det er lootbokser som fører til problemspill eller om det er problemspillerne som har en tendens til å bruke mer penger på kjøp av lootbokser enn andre spillere.¹³

Departementet skriver i forarbeidene til ny pengespillov at noen elementer i dataspill har klare likhetstrekk med pengespill¹⁴. Spillkonseptene ligger tett opp til pengespillreguleringens virkeområde, men avviker likevel fra de tra-

disjonelle, regulerte pengespillene, fordi de finner sted i en virtuell verden der både innskudd og gevinst ofte består av noe annet enn vanlige penger.

Uavhengig av denne forskjellen, er det klart ut fra forskning at bruk av lootbokser er *egnet til* i alle fall å bygge opp under problematisk spilleatferd. Konseptet med lootbokser er forankret i atferdspsykologi, og Forum for spilltrender viser til at der et dataspill åpner for at spilleren kan kjøpe lootbokser med innhold som kan gi fordeler i spillet, er de beste gjenstandene som regel også de sjeldneste, og de oppleves som svært attraktive av engasjerte spillere. Dette synes relativt tydelig i både reaksjonsvideoer av spillere som får attraktive gjenstander i sine lootbokser, og i spill hvor det finnes svartebørsmarked for attraktive gjenstander og disse omsettes for tusenvis av kroner¹⁵.

Videre viser forskning at det viktigste er trekningshastighet når man vurderer risiko for å utvikle spilleproblemer.¹⁶ Dersom forskning på pengespill er overførbart til dataspill, vil dette bety at jo raskere og lettere man får kjøpt og åpnet en pakke for å få vite hva den inneholder, jo større er sannsynligheten for at konseptet kan gi spilleproblemer. Som med spilleautomater og skrapelodd er mekanismene i en lootboks lagt opp til rask turnover, hvor tiden fra kjøp til åpning av en lootboks er kort, samtidig som lyd- og bildeeffekter aktivt brukes for å trigge psykologiske mekanismer som hjernen forveksler med belønninger. Selve prosessen rundt åpningen av for eksempel FIFA Ultimate Team-kortpakker, er designet slik at jo edlere valør innholdet har, jo mer fargerikt og eksplosiv er åp-

ningen.¹⁷ Dette kan være svært avhengighetsskapende for personer som utviser problematisk spilleatferd. På den bakgrunn er det ganske klart at *formålet* med pengespillreguleringen i alle fall ikke stenger for at lootbokser kan falle innenfor definisjonen av pengespill i lovens § 2.

” Dersom forskning på pengespill er overførbart til dataspill, vil dette bety at jo raskere og lettere man får kjøpt og åpnet en pakke for å få vite hva den inneholder, jo større er sannsynligheten for at konseptet kan gi spilleproblemer.

3.2 De nærmere vilkår i pengespilloven

3.2.1 Innledning

Det følger videre av ny pengespillov § 2 at «Loven gjelder pengespill der deltakere mot en innsats *kan vinne* en premie av økonomisk verdi, og resultatet er helt eller delvis tilfeldig».

For det første må det foreligge en «innsats». Dette er enkelt nok «det spilleren må betale for å kjøpe en vinnerjanse»¹⁸. Dernest må det foreligge en premie av økonomisk verdi. En premie av økonomisk verdi vil etter det departementet legger til grunn være «penger, gjenstander eller andre formuesgoder av økonomisk verdi»¹⁹. Det siste vilkåret, om at resultatet skal være helt eller delvis tilfeldig skal forstås slik at dette er tilfeller der utfallet av et spill, lotteri eller konkurransen ligger utenfor

15 Forum for spilltrender *Rapport om gråsonespill* punkt 2.3

16 Forum for spilltrender *Rapport om gråsonespill* punkt 2.3

17 Forum for spilltrender *Rapport om gråsonespill* punkt 2.3

18 Prop 220 L (2020-2021) punkt 5.6.2

19 Prop 220 L (2020-2021) punkt 5.6.4

13 Prop 220 L (2020-2021) punkt 5.3.4.

14 Prop 220 L (2020-2021) punkt 5.3.1.



Illustrasjonsfoto: Colourbox.com

spillerens kontroll.²⁰ Departementet viser til at vilkåret alltid er oppfylt der vinneren blir kåret ved trekning eller gjetting, mens det også kan være oppfylt i spill hvor gevinstmuligheten i noen grad kan være avhengig av deltakernes ferdigheter.

Når det kommer til spørsmålet om lootbokser faller innenfor definisjonen av pengespill, blir det altså et spørsmål om alle vilkårene er oppfylt: (i) må spilleren ut med en innsats for å kjøpe en lootboks, (ii) er resultatet ved hva man får ved kjøp av en lootboks helt eller delvis tilfeldig og (iii) vil belønningen være en premie av økonomisk verdi. Hvorvidt vilkårene er oppfylt beror på en konkret vurdering av det aktuelle spillet og den angjeldende lootboks. I det følgende skal vi imidlertid se mer generelt på vilkårene og vurdere om lootbokser *kan* falle innenfor definisjonen.

3.2.2 «Innsats»

Det første vilkåret i pengespilldefinisjonen er at det må foreligge en «innsats». Innsats vil ifølge departementet være det spilleren må betale for en sjanse til å vinne. Vilkaeret er oppfylt dersom spilleren kjøper vinnerensjansen for vanlige penger eller andre verdier som kan veksles inn i vanlige penger. Det er lagt til grunn av Kulturdepartementet at i de tilfellene hvor spilleren bruker andre former for *innsats*, for eksempel tidsbruk, måloppnåelse eller deltakelse i bytte mot personopplysninger, så skal *ikke* dette omfattes av definisjonen.²¹

En spiller kan kjøpe en lootboks gjennom en betaling med «vanlige penger», for eksempel via kredittkort, direkte til spillutvikleren. I lys av at ett av formålene med pengespillovgivningen er å forhindre de negative sosiale konsekvensene som kan ta form av økonomiske vanskeligheter som følge av spilleavhengig-

het²² eller problematisk spillatferd, er vilkåret om *innsats* klart nok oppfylt ved betaling med vanlige penger. Vilkaeret *kan* imidlertid også være oppfylt dersom en lootboks kjøpes for spilllets interne valuta.

Flere dataspill bruker spillvaluta. Denne typen valuta skiller seg fra ekte penger ved at den kun eksisterer innad i spillet. Det kan for eksempel være virtuelle «coins», «gold» eller «gems», og er ikke akseptert som betalingsmidler utenfor spillet. Avhengig av videospillet, kan spillvaluta bli brukt av spillerne til å kjøpe for eksempel oppgraderinger, og i noen spill, lootbokser. Dersom man sammenlikner kjøp av lootbokser med mer «tradisjonell» gambling på kasinoer, vil det å bruke spillvaluta for å kjøpe en lootboks, være lik det samme som å bruke sjetonger for å delta i et spill; verdien av både sjetongen og spillvalutaen kan uttrykkes i vanlig pengevaluta, og

20 Prop 220 L (2020-2021) punkt 5.6.3

21 Prop 220 L (2020-2021) punkt 5.6.2.

22 Meld St. 12 (2016-2017) s. 33-34.

fungerer begge som en indirekte betaling for å delta sjansespillet.

Det er kun i de tilfellene hvor spillvaluta blir kjøpt for vanlige penger og *deretter* brukt til å kjøpe lootbokser, at vilkåret om innsats vil være oppfylt. Det kan argumenteres for at det er svært viktig at nettopp disse tilfellene faller innenfor definisjonen, ettersom bruk av spillvaluta kan gjøre det uklart for spilleren hvor mye dette er verdt i vanlige penger og dermed kan bruk av spillvaluta føles abstrakt og mindre alvorlig.

Videre er innsatsvilkåret ifølge departementet, også oppfylt dersom man kan betale for å delta i en trekning, selv om det også er mulig å delta i trekningen gratis²³. Det betyr at innsatsvilkåret vil være oppfylt dersom spillet gir mulighet for å kjøpe lootbokser eller andre pengespilliknende elementer i dataspill, selv om de også kan opptjenes gjennom spillet.

På den bakgrunn, er det klart at innsatsvilkåret i alle fall i noen tilfeller vil være oppfylt når det foreligger mulighet for kjøp av lootbokser i dataspill.

3.2.3 «Helt eller delvis tilfeldig resultat»

Vilkåret i ny pengespillov knyttet til at resultatet må være «helt eller delvis tilfeldig» er videreført fra bestemmelsen i lotteriloven, og skal basere seg på etablert tolkningspraksis under denne loven. I det ligger at tilfeller der utfallet av et spill, lotteri eller konkurranse ligger utenfor spillerens kontroll, er det tilstrekkelig for at vilkåret skal være oppfylt.

I dataspill er det ofte en sammensetning av spillerens egne ferdigheter og tilfeldigheter som utgjør resultatet i et spill. Det kan derfor stilles spørsmål ved om et utfall anses som helt eller delvis tilfeldig der spillerens egne ferdigheter er med på å bestemme resultatet. Som ordlyden gir anvisning på, er det tilstrekkelig at utfallet delvis er avhen-

gig av tilfeldighet. Med dette, omfattes blant annet spill der gevinstmuligheten i noen grad kan være avhengig av deltakerens ferdigheter, reaksjonsevner eller liknende. Hensikten med utvidelsen av lotteribegrepet var å fange opp arrangementer som har så mye til felles med lotterier at de bør omfattes av loven.²⁴ Generelt kan man si at spillet må yte lik motstand til alle deltakere, og forutsetningen for deltakelse i konkurransen, må være den samme for alle deltakerne. Departementet legger til grunn i forarbeidene til ny pengespillov at enkelte kreative konkurranser vil ha mye til felles med lotterier, fordi de oppfattes som svært sjansepreget²⁵.

En klar forskjell mellom lootbokser og de vanlige pengespillene, er at i de vanlige pengespillene står spilleren i fare for å ikke vinne noe ting i det hele tatt. Dersom noen for eksempel kjøper et skrapelodd eller en lottorekke, vil resultatet mest sannsynlig være at man ikke vinner noe som helst.²⁶ Dette resultatet er tilfeldig. En lootboks derimot, inneholder alltid *noe*, det vil si at den aldri er tom. Det betyr at man aldri kan gå tomhendt fra et lootbokskjøp. Denne forskjellen mellom vanlig pengespill og kjøp av lootbokser, var bestemmende for at det amerikanske organet som vurderer videospill (ESRB) kom til at lootbokser i dataspill *ikke* skulle anses for å være pengespill.²⁷

Vår vurdering er imidlertid at tilfeldighets-elementet er så fremtredende ved kjøp av lootbokser, at det ville være kunstig å vurdere det til å falle utenfor pengespilldefinisjonen utelukkende av den grunn i alle til-

feller. Konseptet med mange lootbokser er basert på en mekanisme hvor en spiller kjøper en lootboks, med et håp om å finne noe de ønsker seg på innsiden, uten å ha noen form for påvirkningskraft over dette. Det er verken ferdigheter eller kunnskap som bestemmer hva spilleren vil få i lootboksen. Presumptivt er resultatet basert på en algoritme, men for spilleren oppleves det å åpne en lootboks som et sjansespill. Svært ofte vil spilleren ikke motta de mest verdifulle eller ønskede gjenstander etc. Vi er på den bakgrunn av den oppfatning at det tilfeldige utfallet *er* en særegenhet for lootbokser, som gjør det i alle fall kan argumenteres for at vilkåret er oppfylt i flere tilfeller.

” Vår vurdering er imidlertid at tilfeldighets-elementet er så fremtredende ved kjøp av lootbokser, at det ville være kunstig å vurdere det til å falle utenfor pengespilldefinisjonen utelukkende av den grunn i alle tilfeller.

3.2.4 «Premie av økonomisk verdi»

Det tredje vilkåret i pengespilldefinisjonen er at det må være mulig å vinne en premie av *økonomisk verdi*. Dette er en kodifisering av rettstilstanden før ny pengespillov og er tatt inn i lovteksten fordi departementet ønsket å tydeliggjøre kravet om økonomisk verdi.²⁸ En økonomisk premie kan bestå av penger, gjenstander eller annet av økonomisk verdi. I utgangspunktet vil alt av verdi kunne ses på som en premie etter lotteriloven.

Når man vurderer lotteriliknende konkurranser opp mot lotteridefinisjonen, er det vanlig praksis at gjen-

24 Prop 220 L (2020-2021) punkt 5.2.2.

25 Prop 220 L (2020-2021) punkt 5.2.3.

26 Regulation of loot boxes - How lottery-like mechanisms in video games are and should be regulated (2019) Korhonen s.19.

27 Regulation of loot boxes - How lottery-like mechanisms in video games are and should be regulated (2019) Korhonen s. 19.

28 Prop 220 L (2020-2021) punkt 5.6.4.

23 Prop 220 L (2020-2021) punkt 5.6.2

stander av ubetydelig verdi faller utenfor gevinstbegrepet.²⁹ Hva som for eksempel utgjør gjenstander av ubetydelig verdi tok Kulturdepartementet stilling i sak 21/715 (Klubblood, Spond og Spleis). Her ble gevinster som t-skjorter, pokal, kalender og fruktkurv ansett for å utgjøre gevinster av ubetydelig verdi som falt utenfor datidens lotterilov. Det ble uttalt at i konkurranser der minste mulige innsats (prisen per lodd) er høyere enn gevinstens omsetningsverdi, vil gevinsten klart måtte anses for å være av ubetydelig verdi. I tilfellet nevnt ovenfor ble gevinstenes omsetningsverdi vurdert som relativt beskjeden, noe som gjorde at utsiktene til fortjeneste ved videresalg var svært små. Økonomisk vinning ble derfor ikke ansett for å kunne være en reell motivasjon for de som valgte å delta i konkurransen, og konseptet ble ansett for å falle utenfor lotteridefinisjonen.

Annerledes stilte det seg i Lotterinemndas vedtak i sak 10/02241 i *Alta Laksefiskeri interessentskap*. Saken gjaldt en trekning av rett til å kjøpe fiskekort i en svært populær lakseelv. Deltakerne betalte for å delta i trekningen der det var to kvoter. Én kvote var forbeholdt fastboende, og her var det forbudt å videreselge fiskekortet. Den andre kvoten var for utenbysboende, men her var videresalg tillatt. Klager mente at denne praksisen var et ulovlig lotteri, men fikk bare delvis medhold i dette. Lotterinemnda uttalte at det forelå en gevinst i den delen av konkurransen der det var mulig å videreselge fiskekortet fordi vinneren da kunne ta høyere pris for fiskekortet og på den måten oppnå en fortjeneste. I de tilfeller der hvor det var forbudt å selge fiskekortet videre, ville det derimot ikke utgjøre en gevinst, forutsatt at vinneren ikke betalte underpris for fiskekortet. Nemnda konkluderte

29 Forum for spilltrender *Rapport om gråsonespill* punkt 4.3.2

derfor med at trekninger av retten til å kjøpe fiskekort i kvoten som var forbeholdt utenbysboende, var et lotteri etter daværende lotterilov § 1 første ledd a.

Innholdet i en lootboks vil normalt være en virtuell gjenstand. Imidlertid vil innholdet i ulike lootbokser kunne ha svært ulik subjektiv eller objektiv «verdsettelse». Innholdet i en lootboks kan gi en spiller høyere status, økt popularitet eller følelsen av å prestere bedre i spillet – også kalt den subjektive verdien.³⁰ Det følger imidlertid av forarbeidene til ny pengespillov at det å medregne den subjektive verdien under kriteriet om premie av økonomisk verdi, vil være svært lite forutsigbart og ikke forenlig med et krav om tilstrekkelig klar og tydelig handlingsnorm for å kunne ilegge overtredelsesgebyr eller straffesanksjoner³¹.

Den objektive verdien vil være det den virtuelle gjenstanden kan omsettes for, enten i spillet eller på nettsider utenfor spillet dersom det er mulig å ta den virtuelle gjenstanden med seg ut av spillet. Gjenstander i lootbokser vil ha svært varierende økonomisk verdi: noen er nesten helt verdiløse i et økonomisk perspektiv, mens andre vil ha stor samleverdi. I dataspillet CS:GO kan vanlige og lite verdifulle skins for eksempel omsettes for noen få øre. I noen dataspill kan gjenstander omsettes enten i eller utenfor spillet. Verdien på gjenstander vil også kunne variere over tid. Gjenstander som har en økonomisk verdi, kan oppfylle pengespillovens vilkår om premie av økonomisk verdi. Det kan derfor være naturlig å vurdere verdiløse eller nesten verdiløse gjenstander på samme måte som gevinster som i henhold til praksis faller utenfor gevinstbegrepet.³²

30 Forum for spilltrender *Rapport om gråsonespill* punkt 4.3.2

31 Prop 220 L (2020-2021) punkt 5.6.4.

32 Forum for spilltrender *Rapport om gråsonespill* punkt 4.3.2

Dersom den virtuelle gjenstanden kan kjøpes i spilllets egen butikk, kan vi legge denne prisen til grunn som gjenstandens verdi.³³ Forum for spilltrender tar på den måten til orde for at også det som har en økonomisk verdi i *spillet* kan falle innenfor definisjonen i datidens lotterilov. Departementet tar imidlertid avstand fra dette standpunktet i forarbeidene til ny pengespillov.

Det følger av forarbeidene at

«Departementet har falt ned på at pengespillovens omfang på dette tidspunktet bør begrenses til tilfeller hvor en premie i et dataspill kan veksles inn i eller omsettes til vanlige penger eller annet som har økonomisk verdi utenfor dataspillverdenen»³⁴ (vår utheving).

Det er etter dette ikke helt klart hva som skal utgjøre rammene for vurderingen av «økonomisk verdi». I alle fall i tilfeller hvor spillet har en markeds plass eller tilbyr bytte og salg med definerte priser i vanlige penger, kan det argumenteres for at premien mottatt ved kjøp av en lootboks har en objektiv økonomisk verdi *utenfor dataspillverdenen*. Etter vår forståelse, må heller ikke premien alltid være omsettelig. Så lenge det vil koste en gitt sum vanlige penger å få tak i premien, kan det argumenteres for at dette også anses for å oppfylle vilkåret.

4. Konklusjon

Som vist ovenfor, *kan* kjøp av lootbokser falle innenfor definisjonen i pengespillov § 2. Departementet synes imidlertid som et utgangspunkt å være lite villige til å åpne for denne forståelsen av pengespillov.

Selv om spørsmålet skulle komme på spissen, er lovgiver relativt klar i sine utsagn på at det skal mye

33 Forum for spilltrender *Rapport om gråsonespill* punkt 4.3.2

34 Prop 220 L (2020-2021) punkt 5.6.4.

til for å regulere lootbokser under pengespillovgivningen. En av årsakene til dette, er at grensen mellom dataspill og pengespill er et regulatorisk felt som er lite harmonisert internasjonalt, men som nå diskuteres i internasjonale fora. På den bakgrunn, legger departementet til grunn en forsiktighet i reguleringen av pengespill på nåværende tidspunkt.³⁵ Vi vil anta at man også er noe varsom med å trekke spillmonopolet for langt opp mot EØS-retten.

35 Prop 220 L (2020-2021) punkt 5.6.4.



Som vist ovenfor, kan kjøp av lootbokser falle innenfor definisjonen i pengespiloven § 2.

Samtidig er det slik at over 85 % av barn og unge mellom 9 og 19 år spiller videospill. Dersom man skal ta formålet med pengespillovgivningen på ordet – nemlig å sørge for at pengespill tilbys innenfor ansvarlige rammer og at man i størst mulig grad skal skjerme barn og unge fra spillavhengighet, taler dette for at myndighetene – uavhengig av signa-

lene internasjonalt – for at lootbokser bør reguleres.

Som vist i gjennomgangen i punkt 3, er det ganske klart at lootbokser *kan* falle innenfor pengespilldefinisjonen i ny pengespillov § 2. Det er derfor ingen hindringer for at lov og lootbokser i alle fall kan utvikles til å bli *a lov(e) story*. Men, per nå, synes lovgiverviljen å stå noe i veien for at kjærligheten kan blomstre fullt ut.

Regine S. Antonsen og Stian H. Oddbjørnsen, CMS Kluge Advokatfirma.

Kameraovervåking og særlige kategorier av personopplysninger

Av Hanne Pernille Gulbrandsen, Steinar Østmoe og Ole Martin Moe



Hanne Pernille Gulbrandsen



Steinar Østmoe



Ole Martin Moe

Innledning

Kameraovervåking er svært utbredt. Videokameraer fanger opp mye informasjon og kan ofte avsløre svært private detaljer om oss. Er vi syke eller friske? Hvilken religion eller politisk tilhørighet har vi, eller hvilken seksuell orientering eller kjønnsuttrykk har man?

For behandlingsansvarlige kan det være vanskelig å forutse akkurat hva kameraet vil fange opp. Hvor man filmer vil selvfølgelig ha betydning, men det er vanskelig å utelukke at opptaket implisitt eller eksplisitt kan gi kunnskap om særlige kategorier av personopplysninger knyttet til den som filmes.

Det Europeiske Personvernrådet (EDPB) har laget retningslinjer som gjelder kameraovervåking. I fjor sommer kom det en dom fra EU-domstolen som kan få betydning for vurderingen av når man fanger opp artikkel 9-opplysninger og som gjør at man kan stille spørsmål om EDPBs retningslinjer fremdeles gir uttrykk for gjeldende rett.

I denne artikkelen vil vi se nærmere på EU-domstolens sak C-184/20 og hvilken betydning domstolens uttalelser kan ha for kameraovervåking.

Kameraovervåking i personvernforordningen

Kameraovervåking er i dag svært lett tilgjengelig. Man kan enkelt kjøpe og installere et kamera med tilhørende programvare. Kameraovervåking har mange lovlige bruksområder for eksempel som et sikkerhetstiltak, men ansees samtidig som er inngripende tiltak som krever gode vurderinger og begrunnelse. Derfor finnes svært mange eksempler på tilfelle der tilsynsmyndigheter og domstoler har ansett videoovervåking som ulovlig.

Kameraovervåking innebærer ofte behandling av personopplysninger, med den konsekvens at personvernregelverket gjelder. Det betyr at den som kameraovervåker må oppfylle kravene i personvernforordningen, hvor kravet til rettslig grunnlag er



I denne artikkelen vil vi se nærmere på EU-domstolens sak C-184/20 og hvilken betydning domstolens uttalelser kan ha for kameraovervåking.

helt sentralt. Forordningens artikkel 6 nr. 1 inneholder alternative rettslige grunnlag, hvor interesseavveiningen i bokstav f ofte er det meste aktuelle grunnlaget i denne sammenheng.

Særlige kategorier

Når man filmer med et kamera, fanger man i utgangspunktet opp alt som skjer der det filmes. Man ser hvilke personer som går forbi, hvordan de ser ut, hvordan de oppfører seg og hvor lenge de er der. Man kan utlede mye informasjon fra hvordan man ser ut og hvordan man oppfører seg. Man kan også utlede mye informasjon basert på hvor man oppholder seg. Dersom en person besøker et trossamfunn for bønn, en politisk organisasjon for et møte eller oppsøker helsehjelp kan man for eksempel utlede hvilken religion eller politisk parti de tilhører, hvordan helsen deres er, eller hvilken seksuell orientering man har.

Kameraovervåking kan dermed fange opp karakteristikk eller adferd som kan avsløre *særlige kategorier av opplysninger*. Personvernforordningens artikkel 9 gir et særlig vern for særlige kategorier personopplysninger. Dette vernet innebærer at det er

forbudt å behandle slike personopplysninger med mindre et av unntakene i bestemmelsen er oppfylt. Et sentralt spørsmål blir om den behandlingsansvarlige må oppfylle et av unntakene i artikkel 9, i tillegg til å ha et rettslig grunnlag for kameraovervåkingen etter artikkel 6 nr. 1.

Det Europeiske Personvernrådet har publisert retningslinjer for behandling av personopplysninger gjennom videoteknologi («Guidelines 3/2019 on processing of personal data through video devices»). I disse retningslinjene uttaler Personvernrådet seg om grensene for når man behandler særlige kategorier av personopplysninger gjennom kameraovervåking og ikke:

Video surveillance systems usually collect massive amounts of personal data which may reveal data of a highly personal nature and even special categories of data. Indeed, apparently non-significant data originally collected through video can be used to infer other information to achieve a different purpose (e.g. to map an individual's habits). However, video surveillance is not always considered to be processing of special categories of personal data.

Som et eksempel på dette, skriver rådet at opptak som viser en person som har på seg briller eller sitter i rullestol ikke i seg selv utgjør særlige kategorier av personopplysninger.

Rådet skriver videre at selv om man filmer mennesker som går til gudstjeneste i en kirke, innebærer ikke dette at man behandler opplysninger om religiøs tilhørighet. Ifølge retningslinjene er formålet med kameraovervåkingen avgjørende for om man behandler særlige kategorier eller ikke. Dersom formålet for eksempel er å forhindre hærverk, behandler man altså ikke opplysninger om religiøs tilhørighet selv om man filmer personer på vei til gudstjeneste.

C-184/20 (Vyriausioji tarnybinės etikos komisija)

I saken C-184/20 (Vyriausioji tarnybinės etikos komisija) fra 2022 kommer imidlertid EU-domstolen med uttalelser om rekkevidden av artikkel 9 som kan ha betydning for når man behandler særlige kategorier av personopplysninger gjennom kameraovervåking.

Saken handlet om nasjonal lovgivning i Litauen. Som følge av FN's konvensjon mot korrupsjon fra 2003 og at EU tiltrådte denne i 2008, vedtok Litauen lovgivning for å dokumentere interessekonflikter for «those working in the public sector or in the public interest». Lovgivningen påla ansatte å oppgi en rekke opplysninger om dem selv og ektefellen, samboeren eller partneren deres til «Chief Official Ethics Committee», blant annet navn, medlemskap eller virksomhet med fagforeninger eller politiske partier og finansielle opplysninger dersom de hadde overført mer enn 3000 euro de siste 12 månedene. Den etiske komiteen skulle deretter publisere en erklæring om hver enkelt ansatt, hvor de fjernet de særlige kategoriene fagforeningsmedlemskap og politisk tilhørighet. Selv om disse opplysningene ble fjernet ville likevel navnet på ektefelle, partner eller samboer bli publisert fordi de i seg selv ikke ble ansett som særlige kategorier av personopplysninger.

En offentlig ansatt utfordret denne lovgivningen og argumenterte for at det å publisere navnet på ektefellen ville avsløre vedkommendes seksuelle orientering. Saken endte i EU-domstolen, som tok stilling til hvorvidt å publisere navnet på ektefellen innebar behandling av særlige kategorier av personopplysninger.

Domstolen tok utgangspunkt i ordlyden til den engelske versjonen av personvernforordningen:

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the

processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
(Vår utheving)

Ifølge ordlyden i artikkel 9 er det altså avgjørende om personopplysningene avslører særlige kategorier av opplysninger. Det er interessant å merke seg at i den norske oversettelsen av artikkel 9 er verbet «revealing» utelatt:

Behandling av personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering, er forbudt.
(Vår utheving)

Spørsmålet for domstolen var dermed hva det innebærer at noe «revealing» eller «avslører» seksuell orientering. Kort oppsummert kom domstolen til at formålet med bestemmelsen, å gi et ekstra vern til særlig beskyttelsesverdige typer personopplysninger, må føre til at opplysningene om ektefelle eller samboer i dette tilfellet omfattes av artikkel 9. Domstolen minner samtidig om at det følger av EU-rettspraksis at man ved tvil skal velge det tolkningsalternativet som best ivaretar hensynet bak en lovbestemmelse. Å publisere navnet på ektefellen vil gjøre at man indirekte kan utlede den seksuelle orienteringen til den offentlige ansatte, og dermed er opplysningene vernet av artikkel 9.

Når innebærer videoovervåkning behandling av særskilte kategorier?

EU-domstolens uttalelser i C-184/20 (Vyriausioji tarnybinės etikos komisija) *kan* tolkes dithen at tilnærmet enhver kobling som gjør at man kan utlede særlig kategorier av personopplysninger, må vurderes etter kravene i personvernforordningen artikkel 9. Generaladvokatens beskrivelse av terskelen for når en personopplysning ansees som «særlige kategorier» som gjentas av EU-domstolen i C-184/20 illustrerer dette:

«the verb 'reveal' is consistent with the taking into account of processing not only of inherently sensitive data, but also of data revealing information of that nature indirectly, following an intellectual operation involving deduction or cross-referencing»

EU-domstolen går inn videre inn på hvordan vurderingen skal gjøres. Beskrivelsen kan minne om terskelen for hva som regnes som anonymiserte personopplysninger etter fortalen til personvernforordningen punkt 26: «opplysninger som ikke kan knyttes til en identifisert eller identifiserbar fysisk person, eller personopplysninger som er blitt anonymisert på en slik måte at den registrerte ikke lenger kan identifiseres». Terskelen for anonymisering er ansett å være høy, blant annet fordi en behandlingsansvarlig i vurderingen skal ta hensyn til «alle midler som det med rimelighet kan tenkes at den behandlingsansvarlige eller en annen person kan ta i bruk for å identifisere vedkommende direkte eller indirekte». I vurderingen skal det tas hensyn til eksisterende teknologi. I tillegg må den behandlingsansvarlige ta med i betraktning den teknologiske utviklingen og gjøre revurderinger av anonymiseringsprosessen i lys av denne. Dersom en slik tolkning legges til grunn, vil resultatet være at langt flere behandlingsansvarlige må oppfylle kravene i artikkel 9, også ved kameraovervåkning, enn det som er tilfellet i dag.

Den *formålsbaserte* tilnærmingen i personvernrådets veileder står dermed i kontrast til EU-domstolens kontekstbaserte tilnærming i denne saken.¹ Er formålet avgjørende, eller vil mye av det man fanger opp med et kamera kunne omfattes av artikkel 9? Skal fremdeles EDPBs retningslinjer legges til grunn, eller må behandlingsansvarlige ta utgangspunkt i EU-domstolens uttalelser ved kameraovervåkning?

Personvernrådets retningslinjer

Personvernrådets retningslinjer går langt i å antyde at det er formålet med kameraovervåkingen som er avgjørende for om man behandler særlige kategorier av opplysninger eller ikke.² Dette reiser spørsmålet om hvilken rettskildemessig vekt disse retningslinjene har.

Retningslinjene er ikke rettslig bindende, men er en viktig rettskilde for pliktsubjektene etter personvernregelverket, ettersom man ofte kun har ordlyden i personvernforordningen og muligens noen uttalelser i fortalen å forholde seg til.

En av Personvernrådets nøkkeloppgaver etter personvernforordningen er å lage retningslinjer for hvordan man skal tolke og anvende regelverket. Retningslinjene er autoritativ «soft law» som det er forventet at de europeiske datatilsynsmyndighetene følger når de håndhever personvernforordningen. Det norske Datatilsynet bruker for eksempel retningslinjer fra Personvernrådet konsekvent i sin praksis.³ Den europeiske menneskerettighetsdomstolen har også brukt Personvernrådets retningslinjer i saker knyttet til retten til privatliv i den europeiske menneskeret-

tighetskonvensjonen artikkel 8.4 I norsk rett brukte lagmannsretten retningslinjer fra artikkel 29-gruppen til å tolke innholdet i personvernforordningen artikkel 6 nr. 1 bokstav f.5 Lagmannsretten uttalte samtidig at uttalelser fra EUs personvernråd er relevante ved fortolkningen, med henvisning til Prop.56 LS (2017–2018), pkt. 30.2.

EU-domstolen har ikke uttalt seg om den rettskildevekten til retningslinjene. Generaladvokatene i EU har imidlertid flere ganger systematisk brukt retningslinjene til Personvernrådet og rådets forløper, Artikkel 29-gruppen, som kilder for å tolke regelverket.⁶

I sak C-210/16 Wirtschaftsakademie Schleswig-Holstein, refererte domstolen for eksempel til Generaladvokatens uttalelse i saken, som inne-

4 Se EMDs sak *M.L. and W.W. v. Germany*, App. Nos. 60798/10 and 65599/10, fra 28. juni 2018, avsn. 63; Partly Dissenting Opinion of Judge Pinto de Albuquerque i *Bărbulescu v. Romania*, App. No. 61496/08, av 12. januar 2016, avsn. 7, 11, 12, 13, 19 og 22; Concurring Opinion of Judge Pinto de Albuquerque i *Szabó and Vissy v. Hungary*, App. No. 37138/14, av 12. januar 2016, avsn. 16.

5 LB-2020-18230, pkt. 3.4.

6 Se Opinion of Advocate General Cruz Villalón i sak C-70/10, *Scarlet Extended*, fra 14. april 2011, avsn. 76; Opinion of Advocate General Jääskinen i sak C-131/12, *Google Spain*, fra 25. juni 2013, avsn. 31; Opinion of Advocate General Jääskinen i sak C-212/13, *Ryneš*, av 10. juli 2014, avsn. 30 and 57; Opinion of Advocate General Cruz Villalón in Case C-230/14, *Weltimmo*, av 25. juni 2015, paras. 30, 33, 35, 40 and 62; Opinion of Advocate General Sánchez-Bordona in Case C-582/14, *Breyer*, delivered on 12. mai 2016, avn. 57 and 66; Opinion of Advocate General Bot i sak C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, av 24. oktober 2017, avsn. 7, 46, 61, 76 and 81; Opinion of Advocate General Mengozzi i sak C-25/17, *Jehovan todistajat*, av 1. februar 2018, avsn. 64, 69 and 71; Opinion of Advocate General Szpunar i sak C-136/17, *GC and Others (De-referencing of sensitive data)*, av 10. januar 2019, avsn. 70; Opinion of Advocate General Szpunar i sak C-507/17, *Google (Territorial scope of de-referencing)*, delivered on 10. januar 2019, avsn. 34; Opinion of Advocate General Szpunar in Case C-673/17, *Planet49*, av 21. mars 2019, avsn. 81.

1 Malgieri & Quinn (2021) side 1590

2 Guidelines 3/2019 on processing of personal data through video devices, avsnitt 66.

3 Se for eksempel 20/02136-18 (overtredsgebyr til Grindr).

holdt et langt sitat fra Artikkel 29-gruppens retningslinjer. Retningslinjene fra Personvernrådet og Artikkel 29-gruppen har slik indirekte påvirket domstolens tolkning av europeisk personvernlovgivning. EU-domstolen har ellers uttalt at man ikke kan si at ikke-bindende instrumenter som retningslinjer ikke er en rettskilde kun på grunn av deres ikke-bindende karakter. Domstolen uttalte i sak C-322/88 Grimaldi:

«The national courts are bound to take recommendations into consideration in order to decide disputes submitted to them, in particular where they cast light on the interpretation of national measures adopted in order to implement them or where they are designed to supplement binding Community provisions».
(Vår utheving)

Domstolen uttalte også i C-188/91 Deutsche Shell:

«Although the recommendations of the Joint Committee cannot confer upon individuals' rights which they may enforce before national courts, the latter are nevertheless obliged to take them into consideration in order to resolve disputes submitted to them, especially when, as in this case, they are of relevance in interpreting the provisions of the Convention»
(Vår utheving)

Uttalelser fra Generaladvokat Kokott i sak C-226/11 Expedia antyder også at man må begrunne – «give reasons» - dersom offentlige myndigheter eller domstoler avviker fra slike retningslinjer:

«must take due account of the Commission's competi-

*tion policy notices».*⁷ *That would entail that, «even though no binding requirements [...] arise» from such notices,*⁸ *those authorities and courts must consider the Commission's assessment as set out in those notices, and «must give reasons which can be judicially reviewed for any divergences».*⁹

Personvernrådets retningslinjer er altså relevante og viktige kilder for tolkning av personvernforordningen.

Det bemerkes også at selv om domstolene i Norge har lagt til grunn Personvernrådets veiledning i Legeliste-saken¹⁰, har Personvernemnda i flere saker underspilt vekten retningslinjer fra Personvernrådet har. Nemnda har også avveket fra retningslinjene uten å begrunne dette.¹¹ Vi fremhever her særlig PVN-2021-13, som nettopp gjaldt kameraovervåking.¹²

C-184/20-s betydning for kameraovervåking

EU-domstolen tok ikke direkte stilling til kameraovervåking eller EDPBs veileder for kameraovervåking i C-184/20, og det er flere forskjeller på behandlingsaktivitetene som er dekket av veilederen og faktum i avgjørelsen. Man kan derfor stille spørsmål om den rettskil-

messige vekten dommen har ved tolkning av personvernregelverket utover den konkrete saken, og særlig når det gjelder videoovervåking.

EU-domstolen har kompetanse til å tolke EU-retten jf. TEU art. 19, og hensynet til ensartethet tilsier at EØS-avtalen tolkes samsvar med EU-retten. EU-domstolens uttalelser i C-184/20 er imidlertid først og fremst bindende for den nasjonale domstolen i Litauen som har sendt spørsmål til EU-domstolen for en «preliminary ruling»¹³, og dermed bindende for partene i saken. C-184/20 gjelder publisering av tekst på internett og en helt annen type behandling av personopplysninger enn kameraovervåking. Det kan derfor stilles spørsmål ved betydningen dommen har for kameraovervåking. I kontrast til etterspillet av Schrems II-dommen¹⁴, har ikke EDPB eller de nasjonale tilsynsmyndighetene endret sine veiledere om kameraovervåking etter C-184/20. Dette kan tilsi at de ikke anser behovet for å oppdatere veiledningen som viktig, selv i lys av hvor utbredt kameraovervåking er i samfunnet. En årsak til dette kan være at man ikke anser at rettstilstanden er endret i vesentlig grad.

Det skal også nevnes at selv om den kontekst-baserte tilnærmingen EU-domstolen legger til grunn i C-184/20 gir uttrykk for hovedregelen for vurdering av knytning mellom en opplysning og en enkeltperson i personvernforordningen, gjør ordlyden i artikkel 9 et unntak for biometrisk og genetisk data der formålet er avgjørende for å vurdere om kravene artikkel 9 kommer til anvendelse: «purpose of uniquely identifying a natural person» brukes om genetiske eller biometriske personopplysninger, mens «revealing» eller «concerning» brukes for å vurdere behandling av alle andre sær-

7 Opinion of Advocate General Kokott in Case C-226/11, *Expedia*, delivered on 6 September 2012, para. 38.

8 Ibid, para. 39.

9 Ibid.

10 LB-2020-18230, pkt. 3.4.

11 Se blant annet PVN-2021-13 og PVN-2021-09.

12 «Selv om det etter ordlyden i artikkel 5 og 6 kan se ut som det skal foretas tre selvstendige vurderinger, er det nemndas syn at disse tre kriteriene henger tett sammen i en samlet vurdering». Dette til tross for praksis fra både EU-domstolen og Høyesterett gjør det klart at «berettiget interesse», «nødvendighet» og den konkrete interesseavveiningen er tre selvstendige og kumulative vilkår, se HR-2021-2403-A, avsn. 48 flg, og C-13/16.

13 https://curia.europa.eu/jcms/jcms/J02_7024/en/ (sist besøkt 22. Februar 2023).

14 Sak C-311/18

lige kategorier. Det har vært hevdet at unntaket for biometriske personopplysninger er inntatt nettopp for å unngå at alle visuelle representasjoner av en enkeltperson skal omfattes av kravene i artikkel 9.¹⁵ Der som en streng kontekst-basert tilnærming legges til grunn for de andre andre kategoriene i artikkel 9 når behandlingen gjelder bilder eller opptak, vil dette lett bli resultatet. Det foreligger imidlertid ingen eksplisitte unntak for opptak eller bilder i artikkel 9, og en slik tolkning har derfor mindre støtte i ordlyden.

Selv om saken gjelder publisering av tekst på internett, kommer domstolen med generelle uttalelser om tolkning av EU-retten, personvernforordningen og artikkel 9 konkret. Domstolen henviser også til egen praksis når den uttaler at særlige kategorier skal forstås vidt og at formålet med å gi et ekstra vern til opplysningene som er nevnt i personvernforordningen artikkel 9.¹⁶ Dette tilsier at det skal mye til for at domstolen avviker fra disse generelle uttalelsene i senere praksis knyttet til artikkel 9. Det er en viktig presisering av EU-domstolen å fremheve at hensynet bak artikkel 9 er tungtveiende når man skal tolke bestemmelsen. Man må ikke tolke bestemmelsen innskrenkende, slik at man svekker det ekstra vernet bestemmelsen er ment å gi for bestemte typer personopplysninger, bare fordi den sensitive informasjonen er implisitt. Dette vil også kunne være i tråd EU-domstolens tradisjon for å tolke EU-regelverket i lys av formålet, som i personvernforordningen er å sikre «vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger».

Selv om dommen fra EU-domstolen gjelder publisering av navn på ektefelle, vil de samme hensynene som ligger til grunn for at personvernfor-

ordningen gir en særlig beskyttelse for opplysningskategoriene i artikkel 9 gjøre seg gjeldende ved kameraovervåking. Det er nettopp disse hensynene som fremheves av EU-domstolen i vurderingen av om opplysningene omfattes av artikkel 9 eller ikke. Såfremt det som vises på kameraovervåking direkte eller indirekte avslører den religiøse eller politiske tilhørigheten din, helseopplysningene dine, opplysninger om den seksuelle orienteringen din eller de andre kategoriene av opplysninger som er beskyttet av artikkel 9, er det mye som taler for at man er innenfor artikkel 9.

Grensene for artikkel 9 har imidlertid ikke kommet helt på spissen i C-184/20, og vi vil sannsynligvis få ytterligere presiseringer fra domstolen i fremtidig praksis.

Utfordringer dersom kameraovervåking omfattes av artikkel 9

Det reiser noen særskilte utfordringer for den behandlingsansvarlige når kameraovervåking omfattes av artikkel 9.

Personvernforordningen artikkel 6 nr. 1 bokstav f vil ofte være det mest aktuelle grunnlaget for kameraovervåking.¹⁷ Bestemmelsen er godt egnet som rettslig grunnlag når man ikke vet hvem de registrerte vil være, og man vurderer rettslig grunnlag for en større gruppe registrerte. Den behandlingsansvarlige vil som regel ikke vite hvem som kan fanges opp av kameraovervåkingen, med mindre man overvåker et område hvor kun en bestemt krets personer ferdes. I så fall kan også spesialreglene i forskrift om kameraovervåking i virksomhet (kameraforskriften) § 3 sette grenser for lovligheten.

Hvis kameraovervåkingen omfattes av artikkel 9, må imidlertid den behandlingsansvarlige i tillegg oppfylle et av unntakene i artikkel 9 nr. 2.

Bestemmelsen inneholder flere alternative unntak, men felles for mange av disse er at det kreves et supplerende grunnlag i nasjonal lovgivning.

Bokstav a sier likevel at samtykke fra den registrerte kan utgjøre et slikt unntak, og krever ikke supplerende rettsgrunnlag. For kameraovervåking er imidlertid dette lite praktisk, ettersom man ikke alltid vet hvem som blir filmet. Det er dermed tilnærmet umulig å innhente et samtykke som oppfyller kravene i personvernforordningen. Det er også fremhevet at Personvernrådet at samtykke er lite praktisk for kameraovervåking: kun i «rather exceptional cases».¹⁸

” Såfremt det som vises på kameraovervåking direkte eller indirekte avslører den religiøse eller politiske tilhørigheten din, helseopplysningene dine, opplysninger om den seksuelle orienteringen din eller de andre kategoriene av opplysninger som er beskyttet av artikkel 9, er det mye som taler for at man er innenfor artikkel 9.

Personvernrådet har også uttalt veldig klart at den behandlingsansvarlige ikke kan benytte seg av artikkel 9 nr. 2 bokstav e: at den registrerte har offentliggjort opplysningene om seg selv:

More specifically, data controllers processing those data in the context of video sur-

15 Malgieri & Quinn (2021) side 1594

16 Se C-184/20, avsnitt 125 og 126, og C-101/01 og C-136/17.

17 Guidelines 3/2019 on processing of personal data through video devices, avsnitt 16.

18 Guidelines 3/2019 on processing of personal data through video devices, avsnitt 16 og 43 flg.

veillance cannot rely on Article 9 (2) (e), which allows processing that relates to personal data that are manifestly made public by the data subject. The mere fact of entering into the range of the camera does not imply that the data subject intends to make public special categories of data relating to him or her.

Selv om dette ikke er rettslig bindende, er det en viktig rettskilde innenfor et rettsområde med få kilder. Som nevnt ovenfor er det også svært retningsgivende for hvordan tilsynsmyndighetene vil vurdere regelverket ved tilsyn.

Spørsmålet om rettslig grunnlag for særlige kategorier som utledes indirekte, vil settes på spissen etter hvert som ny teknologi bidrar til å øke datamengden som kan knyttes til hvert enkelt av oss, og ikke bare i forbindelse med kameraovervåking. Forskning på data i metaverset viser hvor enkelt det er å identifisere en enkeltperson ved hjelp av enkelte datapunkter knyttet noen få til fysiske parameter, og videre hvordan man særlig med kunstig intelligens og målinger over kort tid kan utlede særlige kategorier av personopplysninger.¹⁹ Uten dataminimerende tiltak, kan man stille spørsmålet om vi kommer i en situasjon der behandlingsansvarlige som hovedregel må oppfylle de strengere kravene for behandling i artikkel 9.

Konklusjon

Formålet med denne artikkelen har vært å fremheve noen av utfordringene som oppstår dersom kameraovervåking omfattes av artikkel 9 i personvernforordningen.

¹⁹ Nair, Garrido og Song (2022)

Selv om EU-domstolen ikke har vurdert når kameraovervåking omfattes av bestemmelsen, bør behandlingsansvarlige ha denne dommen med seg når man vurderer om overvåking er lovlig eller ikke. Domstolen kommer med generelle uttalelser knyttet til artikkel 9, som er relevante utover saken som ble prøvd.

Dersom det er mulig, bør man som behandlingsansvarlig vurdere å innføre tiltak som gjør at man ikke fanger opp særlige kategorier av personopplysninger der det er mulig. Avhengig av formålet med overvåkingen kan man vurdere sladding av opptak eller bruk av smarte kameraer som filtrerer informasjonen som man samler inn. Datatilsynet har for tiden et prosjekt i den regulatoriske sandkassen for kunstig intelligens som gjelder nettopp sladding av videostreamer²⁰, og det finnes teknologi på markedet som gjør dette mulig.

Dersom man legger en streng tolkning av C-184/20 til grunn, vil alle kameraer kunne fange opp særlige kategorier av personopplysninger. Vi kan bære religiøse symboler, bruke hjelpemidler eller utvise adferd som avslører helseopplysningene våre. Vi kan også være med på aktiviteter som avslører for eksempel politisk tilhørighet eller fagforeningsmedlemskap. Og vi kan også oppholde oss på steder som avslører politisk eller religiøs tilhørighet, fagforeningsmedlemskap, helseopplysninger, seksuell orientering og mer. Etter vårt syn tilsier EU-domstolens uttalelser at man bør gjøre en særlig grundig vurdering av lov-

²⁰ <https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/pagaende-prosjekter2/doorkeeper/> (sist besøkt 22.02.23)

lighet dersom man kameraovervåker på steder som kan avsløre særlige kategorier, som for eksempel trossamfunn, interesseorganisasjoner, helsehjelp, og samlingssteder for minoriteter i samfunnet.

” Etter vårt syn tilsier EU-domstolens uttalelser at man bør gjøre en særlig grundig vurdering av lovlig-
lighet dersom man kameraovervåker på steder som kan avsløre særlige kategorier, som for eksempel trossamfunn, interesseorganisasjoner, helsehjelp, og samlingssteder for minoriteter i samfunnet.

Hvordan kameraovervåking er satt opp, hvilke steder det filmes, og om det gjøres opptak eller ikke er alle faktorer som påvirker hvor inngripende overvåkingen er i personvernet.

Som all etterlevelse av personvernregelverket er det viktigste imidlertid å gjøre grundige vurderinger av hvorvidt en planlagt behandling er innenfor regelverket eller ikke, og å dokumentere vurderingene i tråd med ansvarlighetsprinsippet i personvernforordningen artikkel 5 nr. 2.

Partner Hanne Pernille Gulbrandsen,
Senior Manager Steinar Østmoe og
Advokatfullmektig Ole Martin Moe.

Kilder:

Norsk rettspraksis:

- HR-2021-2403-A (Legelisten)
- LB-2020-18230 (Legelisten)

EU-domstolen:

- Sak C-101/01 *Bodil Lindqvist*
- Sak C-13/16 *Rīgas satiksme*
- Sak C-136/17 *GC and Others*
- Sak C-184/20 *Vyriausioji tarnybinės etikos komisija*
- Sak C-311/18 *Facebook Ireland and Schrems*
- Generaladvokat Kokotts uttalelse i sak C-226/11, Expedia, av 6. september 2012.

Den europeiske menneskerettighetsdomstolen:

- M.L. and W.W. v. Germany, App. Nos. 60798/10 and 65599/10, fra 28. juni 2018
- Partly Dissenting Opinion, Judge Pinto de Albuquerque i *Bărbulescu v. Romania*, App.

No. 61496/08, av 12. januar 2016

- Concurring Opinion, Judge Pinto de Albuquerque i *Szabó and Vissy v. Hungary*, App. No. 37138/14, av 12. januar 2016

Personvernrådets retningslinjer:

- Guidelines 3/2019 on processing of personal data through video devices
- Norsk forvaltningspraksis: PVN-2021-09
- PVN-2021-13
- Datatilsynets vedtak 20/02136-18

Litteratur:

- Malgieri, Gianclaudio og Quinn, Paul. «The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection

Framework», *German Law Journal*, Volume 22, Issue 8, desember 2021, pp. 1583 – 1612.

doi: 10.1017/glj.2021.79

- Nair, Vivek; Garrido, Gonzalo Munilla og Dawn Song. «Exploring the Unprecedented Privacy Risks of the Metaverse», 26. juli 2022. Hentet fra <https://arxiv.org/abs/2207.13176> 24. februar 2023. Doi: 10.48550/arXiv.2208.05604

Nettsider:

- https://curia.europa.eu/jcms/jcms/Jo2_7024/en/ (sist besøkt 24.02.23)
- <https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/pagaende-prosjekter2/doorkeeper/> (sist besøkt 24.02.23)

Rettferdige algoritmer – matematikk og etikk

Av Thale Cecilia Gautier Gjerdsbakk

Dette er den tredje og siste artikkelen i en artikkelserie om kunstig intelligens og hvordan det utfordrer rettferdighets- og åpenhetsprinsippet i personvernforordningen (pvf.) art. 5 nr. 1 (a).¹ De to første artikkelen ble publisert i Lov & Datas 3. og 4. utgave 2022.

Dagens teknologi gjør det mulig å samle inn, dele og sammenstille store mengder personopplysninger og andre data.² Denne muligheten har gitt grobunn for utviklingen av kunstig intelligens (KI) på et nytt nivå. KI har et vidt anvendelsesområde; det kan bidra til alt fra å effektivisere byråkratiske prosesser til å hjelpe leger med å forutsi faren for hjertesvikt. KI har åpenbare fordeler, og brukes stadig mer.³ For eksempel blir KI stadig oftere benyttet til beslutningsstøtte, nettopp av effektiviseringshensyn. Med beslutningsstøtte mener jeg tilfeller der KI brukes som ledd i å fatte en beslutning, men ikke helautomatiserte avgjørelser etter pvf. art. 22 nr. 1.



Thale Cecilia Gautier Gjerdsbakk

Det er KI brukt som beslutningsstøtte artikkelserien tar for seg.

Bruken av KI innebærer imidlertid utfordringer for personvernet. Manglende transparens (åpenhet) og urettferdighet trekkes gjennomgående frem som problematiske forhold ved KI. Denne artikkelen fokuserer på rettferdighetsprinsippet i pvf. art. 5 nr. 1 (a) og algoritmeskjevheter som utfordring knyttet til overholdelsen av rettferdighetsprinsippet ved bruk av KI som beslutningsstøtte.⁴

1. Rettferdighetsprinsippet

1.1 Hva er rettferdighet?

Rettferdighet er ett av de grunnleggende prinsippene ved behandling av personopplysninger, og er plassert i artikkelen som gjerne kalles for personvernets grunnlov; pvf. art. 5. Likevel er det lite diskutert begrep som ikke brukes like aktivt som for eksempel åpenhetsprinsippet. En mulig grunn til dette er at rettferdighet er vanskelig å definere.

Rettferdighet er et vidt begrep uten én forent definisjon. Rettferdighet er heller ikke et statisk begrep, og hva som er rettferdig avhenger av tid, sted og kontekst. For

eksempel beskriver det bibelske begrepet «øye for øye, tann for tann» gjengjeldelse som rettferdig straff. I Norge i dag straffes ingen gjerningspersoner med forbrytelsen de selv begikk. Men samfunnets rettferdighetsoppfatning kan endres raskere enn det. Både terrorhendelsen 09.11.2001 og covid 19-pandemien er eksempler på at rettferdighetsoppfatningen kan endres av enkelthendelser. De to hendelsene medførte at overvåking, og dermed oppgivelse av personopplysninger, i større grad anses som rettferdig, når formålene er å hindre terror og så stanse smittespredning.⁵ Hva som oppfattes som rettferdig kan i tillegg være betinget av kulturelle, politiske og subjektive forskjeller.

” Denne artikkelen fokuserer på rettferdighetsprinsippet i pvf. art. 5 nr. 1 (a) og algoritmeskjevheter som utfordring knyttet til overholdelsen av rettferdighetsprinsippet ved bruk av KI som beslutningsstøtte.

1 Europaparlamentets og Rådets forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF [personvernforordningen/pvf.].

2 Pvf. fortalepunkt 6.

3 NOU 2020:11 Den tredje statsmakt – Domstolene i endring, s. 254.

4 Pvf. art. 5 nr. 1 (a).

5 ACLU, «Surveillance Under the Patriot Act» <https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act>, Deborah Brown & Amos Toh, «Technology is Enabling Surveillance, Inequality During the Pandemic», hrw.org, <https://www.hrw.org/news/2021/03/04/technology-enabling-surveillance-inequality-during-pandemic>

To mer grunnleggende tanker om hva rettferdighet kan være, er *likebehandling* og *ulike behandling for likt resultat*. Ulik behandling for likt resultat, handler om rettmessig forskjellsbehandling. Man tar utgangspunkt i ulikheter og prøver å justere for disse. Denne rettferdighetstankingen kjenner vi igjen fra velferdsstaten. Noen får mer penger fra staten i form av trygd eller andre goder, mens andre betaler mer penger til staten i form av skatter og avgifter. Målet er at folk skal ende opp likere økonomisk enn om staten ikke hadde blandet seg inn. Likebehandling handler på sin side om at alle vurderes ut ifra like kriterier, uten å ta hensyn til forskjeller man ønsker å korrigere for. Et eksempel her er uttak til et landslag. Her ønsker man å ha med de beste utøverne, uansett om ikke alle har hatt de samme forutsetningene for å bli gode nok til å kvalifisere seg.

1.2 Hvordan vurdere hva som er rettferdig i ditt behandlingstilfelle?

Ettersom rettferdighet ikke har én forent definisjon må hver behandlingsansvarlig selv vurdere hva som er rettferdig i sitt behandlingstilfelle. Dette følger av ansvarlighetsprinsippet i art. 5 nr. 2. For å kartlegge hva rettferdig behandling innebærer må rettferdighetsbegrepet kontekstualiseres. Hva som er rettferdig i et enkelt behandlingstilfelle kan handle om ønsket resultat, politikk eller til og med filosofisk overbevisning eller ideologi. Hva som er rettferdig behandling vil ikke være likt for alle, men som behandlingsansvarlig må man artikulere hvordan rettferdighetsbegrepet skal forstås i den konteksten man behandler personopplysninger.

Når en behandlingsansvarlig skal vurdere hva som er rettferdig i sitt tilfelle, er det nyttig å se på en rekke faktorer. Her kan både personvernforordningens fortale og Det Europeiske personvernrådets (EDPB) retningslinjer bidra med relevante vurderingsmomenter.

Diskriminering og urettmessig forskjellsbehandling er av de tydeligste eksemplene på urettferdig bruk av personopplysninger. At behandling må skje på en måte som hindrer diskriminering uttales blant annet i relasjon til profilering i fortalepunkt 71. Ved forståelsen av hva som utgjør diskriminering som innebærer urettferdig behandling av personopplysninger, vil likestillings- og diskrimineringslovens (ldl.) regler ha betydning. Hovedpoenget er at personer med diskrimineringsvern ikke «behandles dårligere enn andre», jf. ldl. § 7. I forarbeidene utdypes det at det avgjørende er om forskjellsbehandlingen fører til «skade eller ulempe for den som forskjellsbehandles, for eksempel at forskjellsbehandlingen fører til tap av fordeler, økonomisk tap eller færre muligheter sammenlignet med andre i en tilsvarende situasjon. Forholdet må ha en konkret og direkte betydning for bestemte fysiske personer.»⁶ Dette innebærer at ikke alle forskjeller som gjøres mellom ulike grupper av mennesker faktisk utgjør diskriminering. Nøyaktig hvor grensen går må avgjøres i det konkrete tilfellet.

EDPB har i sin veiledning om behandling med grunnlag i kontraktoppfyllelse etter GDPR art. 6 (1) b) uttalt at rettferdighetsprinsippet innebærer en anerkjennelse av de registrertes rimelige forventninger til behandlingen, at behandlingsansvarlig må ta hensyn til mulige negative konsekvenser og for de registrerte og effekten en eventuell ujevn maktbalanse mellom de registrerte og behandlingsansvarlig.⁷

Også i sin veiledning om innbygd personvern etter GDPR art. 25 lister EDPB opp en rekke nøk-

kelementer for å sikre rettferdighet. Blant dem er at behandlingen bør være i samsvar med den registrertes forventninger, at behandlingen ikke skal være diskriminerende, asymmetriske maktforhold skal hensyntas og behandlingen skal være etisk forsvarlig i den forstand at behandlingsansvarlig tar hensyn til de større innvirkningene på den registrertes rettigheter. De legger også til at der algoritmer brukes må algoritmene være rettferdige, den registrerte må ha informasjon om algoritmene og det må skje kvalifisert menneskelig innblanding for å hindre maskinelle skjevheter.⁸

Oppsummert fra fortalen og EDPBs to veiledere vil nyttige spørsmål som behandlingsansvarlige kan stille seg være:

- Om behandlingen innebærer en risiko for diskriminering eller andre negative konsekvenser for de registrerte, også i en større sammenheng
- Om behandlingen er i tråd med rimelige forventninger som de registrerte har
- Om det er en ujevn maktbalanse mellom behandlingsansvarlig og de registrerte
- Hvordan man kan gi de registrerte så god informasjon at de klarer å vurdere om personopplysningene deres blir rettferdig behandlet

2. Algoritmeskjevheter

2.1 Hva er algoritmeskjevheter?

KI medfører noen særlige risikoer for prinsippet om rettferdig behandling av personopplysninger. En sentral problemstilling innen bruken av KI er risikoen for *algoritmeskjevheter*. Dette er skjevheter i algoritmene som gjør at KI'en vektlegger uønskede faktorer som igjen kan medføre et uønsket utfall. Algoritmeskjevheter (på engelsk «machine

6 Prop. 81 L (2016-2017), kap. 30, kommentar til § 7

7 EDPB, 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, version 2.0, adopted October 8th 2019, avsn. 12.

8 EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, adopted November 13th 2019, avsn. 72.

bias») kan defineres som systematiske og gjentatte feilslutninger i KI-systemer som medfører uønskede utfall, eksempelvis at en gruppe mennesker prioriteres over en annen. Som beskrevet i min første artikkel utvikles KI ved å trene algoritmer på store mengder data som fungerer som læringseksemplere for KIen. Dersom læringseksemlene KIen trenes på inneholder uønskede skjevheter, smitter skjevhetene over på algoritmene som igjen vil produsere skjeve resultater.

Det er flere mulige måter læringseksemlene kan inneholde skjevheter, og derfor også mange grunner til at algoritmeskjevheter kan oppstå. Skjevheter kan blant annet oppstå hvis datagrunnlaget er for tynt. Det er statistisk større sjanse for å finne ekstremer i mindre grupper. Dersom KIen trenes på for lite data, kan det derfor hende at dataen ikke vil være presis eller reell nok. En annen risiko er at algoritmen er trent på data som ikke er representativ for alle gruppene med mennesker KIen skal benyttes på. Denne typen algoritmeskjevheter har blitt avdekket i flere ulike ansiktsgjenkjenningsprogrammer.⁹ I en analyse gjennomført av forskere ved MIT og Stanford ble det avdekket at tre ansiktsgjenkjenningsprogrammer hadde svært store forskjeller i evnen til å gjenkjenne hvite menn og kvinner med mørk hudfarge. Alle de tre ansiktsgjenkjenningsprogrammene hadde feilmargin på 0,8 prosent eller lavere når det kom til å gjenkjenne kjønn til hvite menn. For kvinner med mørk hudfarge var feilmarginen mellom 20 og 34 prosent. Ett av de store teknologiselskapene som hadde utviklet den ene ansiktsgjenkjenningsprogramvaren påstod at deres programvare hadde en

9 Hardesty, Larry, «Study finds gender and skin-type bias in commercial artificial-intelligence systems», MIT News, 11.02.2018, (<https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212>)

treffsikkerhet på over 97 prosent. I datasettet med ansikter som var brukt for å evaluere ansiktsgjenkjenningens treffsikkerhet var mer enn 77 prosent av ansiktene mannlige, og over 83 prosent hadde hvit hudfarge. Tilfellet viser hvordan datasett som brukes både til å trene og evaluere KI har stor betydning for treffsikkerheten.

En annen måte algoritmeskjevheter kan oppstå er dersom dataen som algoritmene trenes på inneholder skjevheter og diskriminering. KIen vil da lære av den diskriminerende praksisen i læringseksemlene. Dette kan bidra til å skape eller forsterke uønsket forskjellsbehandling gjennom systematisering av den diskriminerende praksisen.

I de neste punktene vil jeg trekke frem noen aspekter ved algoritmeskjevheter som utgjør en risiko for prinsippet om rettfærdig behandling av personopplysninger, og som behandlingsansvarlige må være bevisste på ved bruk av KI.

2.2 Risikoen for diskriminering

I min første artikkel konstruerte jeg et eksempel der en KI ble trent på historiske data med det formål å hjelpe dommere med å avsi fengslingskjennelser.¹⁰ KIen i eksempelet så blant annet at det var større sannsynlighet for å bli fengslet dersom man ikke brukte briller. Selv om denne slutningen statistisk hadde vært riktig, ønsker vi jo ikke at KI vektlegger brillebruk for å hjelpe dommere med å avsi fengslingskjennelser. Brillebruk er en irrelevant faktor, da det ikke har noe med fengslingsgrunnene å gjøre. Om man bruker briller eller ikke virker som en relativt uskyldig faktor å vektlegge. Men hva om vi bytter ut brillebruk med hudfarge?

Det viste seg å være tilfellet da ProPublica undersøkte beslutningsstøtteverktøyet «COMPAS» som

10 Lov&Data nr. 151 3/2022, s. 4-6.

brukes i domstolene i USA.¹¹ COMPAS er et risikovurderingsverktøy som brukes i flere stater i USA. COMPAS bruker informasjon om den siktede, samlet inn gjennom et spørsmålsark, og gir en risikoscore på 1-10 som indikerer hvor sannsynlig det er at siktede møter opp til planlagte rettsmøter og om personen vil begå nye lovbrudd.¹² Risikoscoren presenteres for dommeren, som står fritt til å bruke risikovurderingen i spørsmålet om hvorvidt den siktede skal varetekstfengsles eller løslates i påvente av rettsak.

” I de neste punktene vil jeg trekke frem noen aspekter ved algoritmeskjevheter som utgjør en risiko for prinsippet om rettfærdig behandling av personopplysninger, og som behandlingsansvarlige må være bevisste på ved bruk av KI.

ProPublica, en uavhengig, ideell organisasjon som produserer undersøkende journalistikk i offentlighetens interesse, gjennomførte en studie på beslutningsstøtteverktøyet COMPAS. Studien konkluderte med at programvaren var diskriminerende overfor folk med mørk hudfarge. Studien så blant annet på hvor mange med henholdsvis mørk og hvit hudfarge som ble feilklassifisert som høyrisiko, altså hvor mange som fikk en risikoscore som tilsa at det var stor risiko for gjenta-

11 Julia Angwin, Jeff Larson, Surya Mattu, & Lauren Kirchner. «Machine Bias», ProPublica.no, 23.05.2016, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

12 Angwin m.fl. (2016).

gelse, men hvor det viste seg at personene ikke begikk nye lovbrudd. I tillegg undersøkte de hvor mange med henholdsvis mørk og hvit hudfarge som ble feilklassifisert som lavrisiko, altså personer som fikk en lav risikoscore for gjentagelse, men som viste seg å likevel begå nye lovbrudd. Studien viste at nesten dobbelt så mange med mørk som hvit hudfarge fikk en høy risikoscore for gjentakelsesfare, uten at personene begikk nye lovbrudd. Samtidig viste studien at nesten 20 prosent flere med hvit enn mørk hudfarge begikk nye lovbrudd til tross for at de hadde fått en lav risikoscore. Studien viser store forskjeller i feilvurderingene til KIen, til ugunst for de med mørk hud.

COMPAS ble utviklet basert på historisk data. Dette er et problem fordi det har vært og er stor grad av etnisk diskriminering i USA. Dette fikk hele verden se under Black Lives Matter-bevegelsen som startet i 2020. Når KIen lærer av data som er preget av historiske og strukturelle skjevheter, vil KIen gjenspeile disse skjevhetene. Når slike skjevheter settes i system og rulles ut i stor skala, utgjør det en trussel for rettferdighetsprinsippet.

I relasjon til problematikken rundt algoritmeskjevheter og diskriminering har Europarådet påpekt forskjellen mellom direkte og indirekte diskriminering. Dette er en nyttig distinksjon for å forstå forskjellen mellom hvordan mennesker og KI kan diskriminere.¹³ Direkte diskriminering er tilfeller der beslutningstakeren direkte baserer beslutningen på urettmessige kriterier som for eksempel hudfarge eller kjønn.¹⁴ Direkte diskriminering skjer gjerne underbevisst hos mennesker, ettersom det er vanskelig å unngå å oppfatte noens kjønn eller

hudfarge. Faktorer som kjønn og hudfarge kan imidlertid ekskluderes fra datasettet som danner grunnlaget for kunstig intelligens. Dette kan forhindre direkte diskriminering i KI som benyttes som beslutningsstøtte.



I relasjon til problematikken rundt algoritmeskjevheter og diskriminering har Europarådet påpekt forskjellen mellom direkte og indirekte diskriminering. Dette er en nyttig distinksjon for å forstå forskjellen mellom hvordan mennesker og KI kan diskriminere.

Indirekte diskriminering er vanskeligere både å oppdage og å korrigere enn direkte diskriminering. Indirekte diskriminering kan oppstå der visse karakteristikker eller faktorer opptrer hyppigere i en gruppe som det er ulovlig å diskriminere mot.¹⁵ Selv om kriterier det er ulovlig å diskriminere mot utelates fra datasettet kan KI utvikle «informati-
on proxies», basert på informasjonskombinasjoner, som med høy grad av sikkerhet kan gi den samme informasjonen som om faktoren det er ulovlig å diskriminere mot var inkludert. Så lenge det finnes skjevheter i datasettet, vil KIen finne andre korrelasjoner mellom inputfaktorene og konklusjonene som vil gi tilnærmet samme diskriminerende utslag som ved direkte diskriminering.¹⁶ Dette er mulig blant annet på grunn av de dype nevralt nettverkene som bygges basert på mønstre i dataen KIen er trent på. Apple opplevde indirekte diskriminering i

sine algoritmer da de lanserte sitt kredittkort. Etter at det ble avdekket at kvinner fikk feilaktig lavere kredittscore enn menn, sluttet Apple å samle inn informasjon om søkerne sitt kjønn. KIen fortsatte imidlertid å diskriminere kvinner også etter at kjønn ble fjernet som faktor fra datasettet.¹⁷

Indirekte diskriminering er enda vanskeligere å oppdage enn direkte diskriminering. Det innebærer at det også er vanskeligere å rette opp eventuelle skjevheter. Dersom man ikke kan dele inn og kontrollere utfallet i grupper det er ulovlig å diskriminere mot, blir det vanskelig å se mønstre som kan avdekke diskriminering mot de utsatte gruppene. Eksempelvis vil det være vanskelig å avdekke et diskrimineringsmønster dersom man ikke kan sammenligne andel feilaktige utfall for de med mørk hudfarge sammenlignet med hvite. I motsetning til mennesker klarer ikke KI å se at beslutningene gir urimelige resultater eller å motvirke diskriminering på eget initiativ. KI har ikke etiske prinsipper eller målsetninger å korrigere beslutningene sine etter. En ekstra utfordring får man dersom algoritmens læring ikke stoppes. Den vil da fortsette å lære av seg selv og forsterker sine egne skjevheter. Dette styrker KIs potensiale til å skape ekkokamre som forsterker allerede eksisterende diskriminering.

Ettersom rettferdighetsprinsippet i personvernforordningen art. 5 nr. 1 (a) forutsetter at det ikke skjer diskriminering må behandlingsansvarlig iverksette tiltak som forhindrer dette. Det kan være å inkludere faktorer det er urettmessig å vektlegge i vurderingen. Formålet er å kontrollere algoritmene opp mot de urettmessige faktorene for å se om det foreligger diskriminering og å

13 Europarådet: The Committee of Experts on Internet Intermediaries, *Algorithms and Human Rights*, DGI (2017)12, 2018. (2018), s. 27.

14 Europarådet (2018), s. 27.

15 Europarådet (2018), s. 28.

16 Europarådet (2018), s. 28.

17 Will Knight, «The Apple Card Didn't "See" Gender - and That's the Problem», wired.com, 19.11.2019, <https://www.wired.com/story/the-apple-card-didnt-see-genderand-thats-the-problem/>.

eventuelt justere algoritmens vektning i retning av å ikke diskriminere mot disse faktorene. Dette kan bli problematisk ettersom faktorer det er urettmessig å vektlegge ofte svarer med personopplysninger det i utgangspunktet er forbudt å behandle, jf. pvf. art. 9 nr. 1. EU-kommisjonen har i sitt forslag til en forordning om kunstig intelligens (Artificial Intelligence Act), foreslått en hjemmel som gjør det lovlig å behandle særlige kategorier personopplysninger etter personvernforordningen art. 9 nr. 1, dersom det er strengt nødvendig for å overvåke, avdekke og korrigere skjevheter ved bruk av høyrisiko KI.¹⁸ Det er imidlertid ikke bare ved bruk av høyrisiko KI det er en fare for diskriminering i strid med rettferdighetsprinsippet. Frem til forslaget eventuelt vedtas må alle behandlingsansvarlige som ønsker å sikre rettferdig KI bruk av særlige kategorier personopplysninger sørge for å ha et behandlingsgrunnlag i art. 9 nr. 2 og at bruk av særlige personopplysninger ikke strider mot dataminimeringsprinsippet i pvf. art. 5 nr. 1 (c).

Til slutt er det verdt å merke seg at risikoen for diskriminering har ikke bare betydning for behandlingsansvarlige som selv bestiller eller utvikler KI. Også ved kjøp av KI-programmer for behandling av personopplysninger må behandlingsansvarlige sikre at programvaren overholder rettferdighetsprinsippet. Ettersom KI lærer av dataen den trenes på, vil algoritmene reflektere de verdiene dataen representerer. Dersom man kjøper et KI-system fra et annet land, vil ikke nødvendigvis verdiene KI-en reflekterer være rettferdige. Innkjøperkompetanse og grundige kjøpspro-

sesser vil derfor være viktig for å overholde rettferdighetsprinsippet ved anskaffelse av KI.

2.3 Hvor mye urettferdighet tåler rettferdighetsprinsippet?

For å i det hele tatt kunne kontrollere om KI er rettferdig, må det fastsettes en grenseverdi som skiller mellom akseptert usikkerhet og uakseptabel forskjellsbehandling. Etter at den behandlingsansvarlige har artikulert hva som utgjør rettferdig behandling, reises spørsmålet om hvor mye potensiell urettferdighet en behandling tåler før den ikke lenger oppfyller rettferdighetsprinsippet. I menneskelige prosesser vil det alltid være en viss risiko for både bevisst og ubevisst urettferdighet. Det kan være en overarbeidet saksbehandler som ikke rekker å undersøke de større konsekvensene av vedtaket den fatter, eller en dommer som lar underbevisste fordommer spille inn på sin oppfatning av en part. De fleste av disse urettferdige tilfellene vil aldri oppdages, fordi vi mennesker er gode på å finne forklaringer vi kan slå oss til ro med. Det er derfor vanskelig å si hvor stor andel av beslutninger som tas som innebærer urettferdig behandling av personopplysninger. At vi som regel ikke har et tall å gå ut ifra gjør øvelsen med å tallfeste urettferdighet utfordrende.

Ved bruk av KI har man mulighet til å nøyaktig tallfeste når man går fra akseptabel til uakseptabel forskjellsbehandling. Grunnen er at en algoritme ikke kan bortforklare urettferdige beslutninger, i motsetning til mennesker. Når man trener en algoritme må man teste hvor treffsikkert den utfører oppgaven sin. Spørsmålet blir da når algoritmen er treffsikker nok. Dette reiser spørsmål om det er tilstrekkelig med 70 prosent riktige utfall eller 95 prosent riktige utfall for å tilfredsstillere prinsippet om rettferdighet. Et annet eksempel er tilfeller der nåværende menneskelig ekspertise er 70 prosent nøyaktig for hele befolkning-

gen, mens en KI har 95 prosent korrekte utfall for majoriteten av befolkningen, men 65 prosent korrekte utfall for en minoritet. Må minoriteten da tåle lavere andel korrekte utfall for at gjennomsnittet av korrekte utfall skal bli bedre? Tallfesting av rettferdighet er både en vanskelig og tidvis vond øvelse. Det reiser flere utforskede etiske problemstillinger, og tallfestingen av akseptabel forskjellsbehandling utgjør en risiko for behandlingsansvarlige som ønsker å bruke KI.

Når grensen for hvor stort avvik fra 100 prosent treffsikkerhet man kan akseptere er satt, må KI-en kontrolleres mot denne grensen kontinuerlig. Dette er eksempelvis fordi sammensetningen i gruppen av mennesker KI-en brukes på kan endre seg, eller algoritmen kan bli skjev over tid dersom den lærer av og systematiserer skjevheter gradvis. Å beholde en rettferdig KI er derfor et kontinuerlig arbeid, og vil kreve oppdatering og etterlæring av KI-en.

2.4 Algoritmeskjevheter og manglende kompetanse

Menneskelig innblanding blir ofte foreslått som et tiltak for blant annet å senke risikoen for algoritmeskjevheter og dermed sikre overholdelse av rettferdighetsprinsippet.¹⁹ Det er imidlertid en risiko for at dette tiltaket gir en falsk trygghet. Grunnen er menneskelig psykologi. Daniel Kahneman skriver i boken *Thinking Fast and Slow* om ankrings-effekten som påvirker i menneskelig beslutningstaking. Som Kahnemans studier viser, lar nemlig mennesker selv irrelevante faktorer påvirke deres dømmekraft, en effekt som kalles *ankring*.²⁰

18 Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final.

19 EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, adopted November 13th 2019, avsn. 72.

20 Daniel Kahneman, *Thinking Fast and Slow*, Penguin Books, 2011, s. 119-128.

I ett av eksperimentene Kahneman bruker som eksempel for å forklare ankringseffekten, fikk en gruppe tyske dommere presentert et faktum der en person hadde nasket i en butikk. Dommerne ble så bedt om å ta stilling til hvor mange måneder fengsel vedkommende skulle få.²¹ Før de tok beslutningen ble dommere bedt om å trille en terning. De ble fortalt at terningen kunne lande på et hvilket som helst tall. Terningen var imidlertid forhåndsinnstilt til å lande på enten tre eller ni. Dommerne som trillet tre på terningen ga i gjennomsnitt fem måneder fengsel. Dommerne som trillet ni ga i gjennomsnitt åtte måneder. Konklusjonen på studien var at dommerne ble påvirket av det tilfeldige tallet terningen viste når de skulle dømme.²²

” Til slutt er det verdt å merke seg at risikoen for diskriminering har ikke bare betydning for behandlingsansvarlige som selv bestiller eller utvikler KI. Også ved kjøp av KI-programmer for behandling av personopplysninger må behandlingsansvarlige sikre at programvaren overholder rettferdighetsprinsippet.

Eksperimentet viser at vi mennesker lar selv irrelevante faktorer påvirke hvordan vi tar beslutninger. Når vi introduserer beslutningsstøtteverktøy for eksempel til saksbehandlere som er utsatt for enorme saksmengder og lite tid til kritisk tenking, er det nærliggende å anta at

vi vil se den samme effekten. I motsetningen til terningen i eksperimentet er risikoscoren relevant for saken. Vi kan derfor forvente at risikoscoren tillegges enda større vekt enn terningen. Det er derfor høyst usikkert hvor meningsfull den menneskelige innblandingen faktisk er.

Det er noen ting en behandlingsansvarlig kan gjøre for å sikre at menneskelig innblanding faktisk fungerer som et risikoreduserende tiltak. Det aller viktigste er å sikre god opplæring av de som skal anvende beslutningsstøtteverktøyet. Dette innebærer god informasjon om hva KI-en egner seg til å si noe om og ikke, hvilke feil den kan gjøre, hvor nøyaktig den er og ikke minst bevissthet rundt menneskelige svakheter ved beslutningstaking ved hjelp av beslutningsstøtteverktøyet. I tillegg må behandlingsansvarlig sikre nok ressurser til at de som bruker verktøyet faktisk kan anvende sunn skepsis og kritisk tenkning.

3. Oppsummering

Dataen som KI trenes på er en refleksjon av historien. Etersom KI er matematikk og ikke etikk, vil KI systematisere monstrene den finner og på den måten gjenspeile verden slik den eksisterer. Behandlingsansvarlige som ønsker å bruke KI på en rettferdige måte blir derfor helt sentralt for etisk utvikling og bruk av KI.

En oppsummering av de tiltakene en behandlingsansvarlig burde foreta seg for å sikre rettferdig behandling av personopplysninger er:

- Still deg spørsmålene i punkt 1.2.
- Kontroller om det foreligger skjevheter i KI-en, men sørg for at du har behandlingsgrunnlag for å gjøre dette og at dataen du kontrollerer algoritmen mot er egnet til å avdekke skjevheter mot grupper med diskrimineringsvern
- Sørg for å skaffe deg god utvikler- eller innkjøpskompetanse
- Sørg for god opplæring av de som skal bruke KI-en og at du har nok ressurser tilgjengelig til at den menneskelige innblandin-

gen faktisk får betydning og ikke blir en falsk trygghet

- Kontroller KI-en treffsikkerhet fortløpende, og sørg for etterlæring når treffsikkerheten går under grenseverdien du har satt

” Vi forstår enda ikke alt hva våre data i kombinasjon med KI kan brukes til, men det er tydelig at åpenhet og rettferdighet blir viktige prinsipper for å sikre demokratisk utvikling av KI i tråd med personvernregelverket.

Personvernforordningen er ment til å være en festningsmur mot misbruk av personopplysninger, gjennom å gi individer rett til tilgang, kontroll og forutberegnelighet med hvordan personopplysningene deres brukes. Dette innebærer at rettferdighets- og åpenhetsprinsippet, som du kan lese mer om artikkelseriens andre artikkel, henger tett sammen.²³ Det blir vanskelig å oppfylle rettferdighetsprinsippet uten åpenhet. Vi forstår enda ikke alt hva våre data i kombinasjon med KI kan brukes til, men det er tydelig at åpenhet og rettferdighet blir viktige prinsipper for å sikre demokratisk utvikling av KI i tråd med personvernregelverket.

Thale Cecilia Gautier Gjerdsbakk er advokatfullmektig med spesialisering innen personvern, teknologi og KI i advokatfirmaet BULL. tcgg@bull.no

21 Kahneman (2011), s. 125-126.

22 Kahneman (2011), s. 126.

23 Lov&Data nr. 152 4/2022 s. 11-15



Halvor Manshaus

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

Rettslig regulering av AI – ulike tilnærminger

På relativt kort tid har kunstig intelligens (AI, eller KI ifølge språkrådets anvisning) blitt et dagligdags uttrykk, selv om meningsinnholdet kan være flyktig og vanskelig å definere presist. Vi blir forklart at alt fra moderne biler, kjøleskap, mobiltelefoner, søkemotorer, digitale assistenter, kjøkkenapparater, gressklippere, luftfuktere og klokker kan gjøre hverdagen enklere ved bruk av AI. Samtidig er det åpenbart at ikke alt som markedsføres som AI egentlig utviser noen form for intelligens. Et dataprogram som bare følger fastlagte anvisninger, vil ikke kunne kategoriseres som ekte AI selv om de fastlagte anvisningene er mangfoldige og gir store valgmuligheter.

En enkel definisjon av AI kunne for eksempel være at en AI er en datamaskin eller mekanisk innretning som styres av et eller flere dataprogram og som er i stand til å emulere menneskelig intelligens, gjerne ved å kunne tilegne seg ny kunnskap, resonnere, trekke logiske slutninger ved sammenstilling av ulike faktiske størrelser og arbeide frem nye løsninger på problemstillinger ettersom disse presenteres. Når det er sagt – det kan tenkes mange andre måter å definere AI på. Et viktig spørsmål vil være hva definisjonen skal brukes til og hvem

den er rettet mot. Hva slags AI det er snakk om har også betydning. Det er for eksempel vanlig å skille mellom svake og sterke AI-løsninger, der forskjellen går på at det bare er de sterke som når opp mot menneskelig intelligens – eller overstiger den. Det kan være verdt å forsøke selv å lage en definisjon av AI. Det er nemlig mens man selv jobber med definisjonen at man merker hvordan det stritter imot, og hvordan selve grunnbegrepet intelligens i seg selv er vanskelig å definere uten en kontekst.

«I propose to consider the question, can machines think?». Slik innledet Alan Turing artikkelen «Computing Machinery and Intelligence» som ble publisert allerede i 1950. I stedet for å forsøke seg på å definere hva som ligger i selve tankeprosessen, viste Turing til en lek kjent som «*the imitation game*». Leken går ut på at en person skal avsløre kjønnet til to personer av ulikt kjønn ved å stille spørsmål til de to personene. Turing så for seg at man erstattet en av de to personene med en datamaskin. Ved å stille spørsmål og føre en samtale med de to, skal den tredje personen nå gjette hvem som er datamaskinen. Poenget er altså ikke at datamaskinen nødvendigvis må svare riktig på spørsmålene, men snarere være i stand til å etterligne

menneskelig respons. Dette er senere blitt kjent som «the Turing Test», hvor formålet altså er å kunne skille mellom menneske og datamaskin. Denne testen er ikke spesielt praktisk, og er heller ikke tilstrekkelig for å definere en AI ut fra dagens behov og forventninger.

Jeg nevnte at Turing var tidlig ute, men problemet med å definere intelligens har omtrent like lang historikk som menneskets evne til selv å anvende tankekraften. Spørsmålet har stått sentralt ikke bare i filosofien, men også i skildringer av kjente skikkelser som Pygmalion, Pinokkio og Frankenstein. I filmen Blade Runner anvendes den fiktive Voight-Kampfftesten, en slags blanding av Turing-testen og en løgn-detektor. Testen er opprinnelig beskrevet i historien «*Do Androids Dream of Electric Sheep*» av Philip K. Dick. Når det skal skilles mellom «ekte mennesker» og androider («Replicants»), stilles det spørsmål hvor kroppens respons er av større betydning enn svarene. Teorien er at androidene, som savner en kontekst for sine ferdiginstallerte minner, ikke klarer å emulere en menneskelig og empatisk respons. Et konkret spørsmål ser slik ut:

«You're in a desert walking along in the sand when all of

the sudden you look down, and you see a tortoise, it's crawling toward you. You reach down, you flip the tortoise over on its back. The tortoise lays on its back, its belly baking in the hot sun, beating its legs trying to turn itself over, but it can't, not without your help. But you're not helping. Why is that?»

Denne empatitesten og karakterene som er nevnt ovenfor, understreker for alle at det ikke er en klar eller skarp grense mellom den menneskelige intelligens og den kunstige. Det er ikke bare vanskelig å beskrive hva som utgjør den kunstige intelligens, det er også vanskelig å forklare hvordan den skiller seg fra det vi ser på som menneskelig.

” Det er ikke bare vanskelig å beskrive hva som utgjør den kunstige intelligens, det er også vanskelig å forklare hvordan den skiller seg fra det vi ser på som menneskelig.

Kanskje er dette bakgrunnen for at EU-kommisjonen fant det nødvendig å nedsette et eget utvalg med benevnelsen Independent High Level Expert Group on Artificial Intelligence. Denne Gruppen har forsøkt å klargjøre innholdet i begrepet AI i et eget dokument: «A definition of AI: Main Capabilities and Disciplines¹». Utvalget tar her utgangspunkt i EU-kommisjonens kommunikasjon fra 25. april 2018 vedrø-

rende kunstig intelligens (COM(2018) 237), som lyder slik:

«Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications).»

Dette er en temmelig vid definisjon av AI, og den forklarer kunstig intelligens ved å vise til at begrepet beskriver systemer med intelligent adferd. Vi er ikke langt fra en sirkeldefinisjon, der vi som ovenfor støter på selve problemet med å beskrive hva som karakteriserer intelligens som sådan. Utvalget har derfor gått videre i arbeidet med å definere AI, og lagt vekt på å beskrive AI både som en fagdisiplin og som en teknologi. Et viktig formål for utvalget har vært å få frem en definisjon som er lett å forstå, og som kan benyttes i analyse og diskusjon knyttet til ulike utfordringer ved anvendelsen og utbredelsen av ulike former for AI. På denne måten skal det legges til rette for utformingen av etiske retningslinjer så vel som et juridisk rammeverk for utvikling og bruk av AI.

«Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans (Humans design AI systems directly, but they may also use AI techniques to optimise their design) that, given a complex goal, act in the physical or digital dimen-

sion by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).» (footnote vedrørende «human design» inntatt i parentes).

Med introduksjonen ovenfor fremstår kanskje resultatet som skuffende, ettersom den nye definisjonen ikke kan sies å være hverken kort eller veldig presis. Det er kanskje derfor utvalget avslutningsvis i rapporten viser til at den som vil sette seg inn i definisjonen kan «refer to this document as a source of additional information to support this definition». Den egentlige definisjonen er altså rapporten som helhet, et temmelig omfattende dokument som det tar en del tid å sette seg inn i.

EU er ikke bare interessert i å lage en definisjon, dette er samtidig innledningen til et omfattende arbeide med å lage et helhetlig rettslig rammeverk for AI. Det er sterkt ønske innen EU om å være tidlig ute med dette, og foreløpig ligger

1 <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>
https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341

det an til at EU faktisk vil være først ute på verdensbasis. Samtidig har Kina allerede introdusert lovgivning på området, men dette er ikke et slik overordnet regelverk som EU ser for seg. Kina har begynt i diametralt motsatt ende, og har begynt med å regulere konkrete typer algoritmer med et regelsett som trådte i kraft 1. mars 2022: «*Internet Information Service Algorithmic Recommendation Management Provision*». Dette er regler rettet mot algoritmebasert teknologi som benyttes for å generere, sette sammen, velge ut, innhente, gjøre tilgjengelig og på annen måte tilby kvalifisert informasjon til brukerne av digitale tjenester. Målsetningen er å ramme algoritmer som bestemmer hva slags innhold som skal tilbys overfor enkelte brukere eller grupper.

Det kinesiske lovverket definerer altså ulike typer algoritmevarianter som rammes, og oppstiller deretter en rekke krav som må oppfylles. Reglene gjelder for enhver som benytter algoritmebasert teknologi for å tilby informasjonstjenester på internett innenfor Kinas grenser. Den som benytter seg av algoritmer som omfattes av lovverket, må kunne påvise tilfredsstillende administrasjonssystemer og tekniske tiltak som styrer bruken og kontrollerer rammene for hvordan algoritmen benyttes. I dette ligger også krav til etiske regler, rutiner for registrering av brukere, tilgang til informasjon om systemet, datasikkerhet, innrapportering av hendelser og lignende. I tillegg er det et krav til transparens, herunder at aktuelle algoritmer skal beskrives og sendes inn til et sentralt statlig register. Tilbyderen må også sette opp jevnlig kontroll og sjekkposter for å overvåke systemet, og følge opp utviklingen fortløpende. Det er for eksempel lagt inn krav i regelverket som skal sikre mot at brukerne blir avhengige, eller at det legges til rette for overforbruk av varer og tjenester.

Kina har også innført flere rettigheter som skal sikre brukernes interesser. Virksomheter som benytter algoritmer som omfattes av regelverket må ikke bare informere om bruken av algoritmer, men gi klar og tydelig informasjon om hvordan algoritmen fungerer. I dette ligger det at man i grove trekk må forklare grunnprinsippene for algoritmen, formålet med bruken samt hvordan den fungerer. Brukerne skal til en viss grad kunne velge ikke å delta i bruken av algoritmen, og skal også kunne kreve egen brukerdata slettet. Det er også krav til at det ikke differensieres mellom brukere i ulike kategorier, for eksempel for å unngå at to jevn gamle personer blir tilbudt ulike priser på samme vare ut ifra hva algoritmen kan lese ut av lagrede data på disse to.

Kina introduserte også i februar 2023 regler for teknologi knyttet til såkalte «deep fakes» («deep synthesis»). Dette er teknologi som eksempelvis kan brukes for å endre stemmen, bildet eller video av en person slik at man kan etterligne andre eller fremstille falsk informasjon. I det hele tatt åpner slike AI-verktoy for å endre eller bearbeide materiale på en måte som ikke tidligere har vært teknisk mulig. Dette reiser selvsagt en rekke problemstillinger knyttet til desinformasjon og ulike former for misbruk. Det finnes allerede en rekke eksempler på at bilder av kjente personer brukes for å legge dem inn som karakterer i filmer av ulikt kaliber. Dette fungerer da ikke bare som en enkel fotomontasje på et utvalgt bilde. En AI kjører fotografiet inn i filmen slik at man rett og slett erstatter en skuespiller med det aktuelle bildet – gjennom hele filmen. Det er ikke i Kina oppstilt et absolutt forbud mot denne teknologien, men det er innført et krav til innhenting av samtykke fra personer hvis persondata blir manipulert. Materiale som blir produsert med slik teknologi må også merkes klart og tydelig for å unngå misforståels-

er. Reguleringen rammer ikke bare den omtalte «deep fake»-teknologien, men berører også løsninger som endrer eksisterende verk, for eksempel ved at man skifter ut ansiktet til hovedpersonen i en filmsnutt.

Den kinesiske tilnærmingen innebærer altså ikke en full regulering av AI som sådan. I stedet har Kina valgt å ta for seg konkrete problemstillinger nært knyttet opp mot ulike typer AI-systemer. De to lovverkene som er beskrevet ovenfor understreker denne tilnærmingen. Vi kan dermed forvente at det kinesiske regelverket fremover vil bli bygget ut med nye tillegg etter hvert som utviklingen går fremover.

EU har altså satset i en annen retning, og bygger på en bredere regulering der praksis og supplerende retningslinjer over tid vil utfylle og klargjøre reglene. I stedet for flere separate lovverk, ønsker EU en enkelt lovtekst som regulerer AI. Målsetningen er at dette vil gi et mer fleksibelt og tilpasningsdyktig system over tid. EUs brede tilnærming omtales ofte litt forenklet som en horisontal regulering, som innebærer at man ønsker å fange opp et bredt spekter av ulike typetilfeller. I en slik tilnærming vil nettopp definisjoner og bruk av ulike kategorier gi en struktur for regelverket. Det vil da i prinsippet være mulig å legge til eller justere både definisjoner og kategorier etter hvert som man ser hva slags problemstillinger som oppstår rundt bruken av AI. Kinas regulering vil tilsvarende bli sett på som en vertikal regulering, der regelverket består av flere separate søyler som hver for seg regulerer ulike typer AI. Ved å ha separate regelsett kan du i teorien fjerne eller gjøre endringer på et regelsett uten at de øvrige påvirkes. Samtidig kan du stadig innføre nye søyler etter behov. En innvending mot den vertikale løsningen er at det kan være tilfeldig hva slags AI-utfordringer som dukker opp, og at lovgiver ofte blir liggende bak utviklingen i et

forsøk på fange opp stadig nye løsninger og modeller som er aktuell i markedet. Etter hvert som søylene utvikles hver for seg, vil det også oppstå en fare for konflikt mellom reglene, eller at reglene som helhet blir for kompliserte.

Det skal understrekes at Kinas løsning ikke er strengt vertikalt i alle henseender. Selv om de to omtalte reguleringene fra Kina fremstår som to separate reguleringer, er det horisontale trekk ved måten dette er håndtert på. For eksempel har Kina introdusert regulatoriske verktøy som påvirker begge algoritmelovene fra Kina. Et eget offentlig algoritmeregister (算法备案系统) ble opprettet samtidig med algoritmeloven fra mars 2022, og er videreført også for reguleringen i februar 2023. Registeret vil fungere som en database der kinesiske myndigheter til enhver tid vil ha full kontroll over aktuelle eksisterende algoritmer i Kina. På tilsvarende måte vil ikke EUs tilnærming være fullstendig horisontal, ved at det vil være et grensesnitt og samhandling med for eksempel GDPR og andre eksisterende regelsett.

Kjernen i EUs regler for AI bygger på en inndeling i fire ulike kategorier basert på en vurdering av risiko. Hver kategori inneholder regelsett tilpasset den risikoen EU ser for seg er aktuelt for typen AI i kategorien. AI-løsninger som medfører uakseptabel risiko er ikke tillatt. Dette vil for eksempel være AI-løsninger eller tilsvarende algoritmer som driver med aktiv sosial profilering og fordeling av poeng basert på ulike kriterier. Tilsvarende vil profilering av biometriske trekk, for eksempel til bruk ved overvåkning eller for å identifisere enkeltpersoner eller grupper ut fra ansiktstrekk, ikke være tillatt.

Høyrisiko vil være knyttet opp mot personers helse, sikkerhet eller grunnleggende rettigheter. Dette vil typisk være sentral infrastruktur eller rutiner som gjelder bruk av personopplysninger til bruk ved an-

settelse. Kategorien begrenset risiko indikerer liten trusselgrad eller risiko, og gjelder for eksempel for enklere AI-løsninger som skal samhandle med fysiske personer. Dette vil for eksempel være en digital kundebehandler på en nettbutikk – ofte kalt chatbot. I slike tilfeller vil det være en plikt til å informere om at samhandling skjer med en AI, med mindre dette fremgår av konteksten.

Den største gruppen av AI-løsninger forventes å ligge i sjiktet for minimal risiko. Dette vil være flere av de AI-variantene som ble nevnt helt innledningsvis. Et eksempel vil være en algoritme i vekkerklokken som kan studere søvnmønster over tid og sammenkoble dette med årstid og andre faktorer for å optimalisere oppvåkningstid og metode.

En slik inndeling i kategorier kan virke praktisk og ryddig. En stor fordel er at man ikke gjør regelverket mer komplisert enn nødvendig for den enkelte risikogruppen. Tilpasningen innebærer at man treffer bedre i reguleringen av det enkelte AI-systemet, og dette gir forutberegnelighet for utviklere, tilbydere og brukere. Det finnes imidlertid en hel rekke utfordringer med denne fremgangsmåten. Kanskje mest slående er hvor lite finmasket inndelingen er. Gruppen for høyrisiko vil fange opp AI-løsninger på vidt forskjellige områder. Spennet er i praksis like vidt som hele samfunnet vårt. I praksis vil det nok by på problemer med å trekke opp grensene mellom kategoriene, ikke minst ved at det ikke foreligger noe entydig eller harmonisert system for å gjøre risikovurderinger av AI. Gjennom livssyklusen til en AI vil det også kunne skje en utvikling som endrer risikobildet. All oppmerksomheten rundt risikovurdering innebærer samtidig at mye av analysen er rettet inn mot den tidlige utviklingsfasen. Erfaring så langt viser imidlertid at slike tjenester utvikles i sterk grad gjennom

faktisk bruk, og at oppmerksomheten også bør rettes mot faktisk bruk, muligheten for at en AI tas i bruk på nye områder og eventuell etterfølgende optimalisering ved bruk av flere AI-løsninger som samhandler.

Et konkret eksempel på utfordringen som møter EU og kategori-systemet følger av retningen AI-utviklingen har tatt. I stedet for tydelige kategorier og inndeling i en stram struktur, ser vi at det nå dukker opp flere generiske AI-løsninger som går på tvers av alle disipliner og bransjer. ChatGPT, som har vært mye omtalt i media i det siste, er en AI-løsning som tilbyr et enkelt tekstbasert grensesnitt. Brukeren stiller et spørsmål, gjerne med detaljerte presiseringer og forklaringer, og ChatGPT leverer raskt et svar, gjerne i form av lengre analyser og utlegning. Vil man ha et kort skuespill i tre akter, så er det nettopp dette som blir levert. Økonomisk rådgivning, tolkning av dikt, skrive en stil på 3000 ord om birokt under keiser Augustus, her er det ingen klare grenser. Slike AI-løsninger kan også motta utkast til dokumenter, forbedre tekst eller skrive ferdig der det mangler noe. Andre løsninger kan frembringe bilder ut fra brukerens beskrivelse av motiv, stemning, bakgrunn og ikke minst om det skal fremstå som et fotografi, mangategneserie, kubistisk maleri eller lignende.

Denne utviklingen har blitt plukket opp også av EU-parlamentet. I februar 2023 tok to av hovedpersonene bak EUs AI-regulering opp et forslag om at AI-løsninger som genererer sammensatt og komplisert tekst uten menneskelig oppsyn skulle legges til på listen for høyrisiko. Tanken var at ChatGPT har et stort potensial for å kunne misbrukes, blant annet til desinformasjon. Forslaget viser klart hvordan EU-forslaget vil bli omdiskutert i prosessen frem mot en gjennomføring av regelverket, og videre når nye tjenester og løsninger på områ-

det fremtvinger endringer og oppdatering av regelverket.

Uansett er det ingen tvil om at både reguleringen i Kina og EU blir fulgt med spente øyne fra hele verden. Dette er nybrottsarbeid, og det er klart at alle som nå regulerer dette området må forvente å gjøre endringer og justeringer underveis.

Som et lite eksperiment tenkte jeg å se om det var mulig å komme både EU og Kina i forkjøpet. Tanken var å undersøke hva en AI selv synes bør være med i en AI-lov. Jeg har derfor henvendt meg til ChatGPT, og ba den regulere seg selv og resten av AI-familien i et utkast til en norsk lov.

Først spurte jeg ChatGPT hvorfor det i det hele tatt er viktig å ha en lov om AI. Svaret var delt opp i seks punkter, og det er vanskelig å være uenig i det ChatGPT trekker frem:



Svar fra ChatGPT

1. Beskyttelse av menneskerettigheter: AI kan ha stor innvirkning på menneskerettigheter, og det er viktig å regulere bruken av teknologien for å sikre at menneskerettighetene respekteres og beskyttes.
2. Beskyttelse av personvern: AI kan samle og bruke store mengder personlig informasjon, og det er viktig å regulere hvordan denne informasjonen samles inn, lagres og brukes for å beskytte personvernet.
3. Ansvar og ansvarlighet: Som AI-systemer blir stadig mer autonome, er det viktig å fastsette hvem som har ansvar for eventuelle feil eller skader som systemene forårsaker, og hvordan de skal holdes ansvarlige.
4. Sikkerhet: AI-systemer kan utgjøre en sikkerhetsrisiko hvis de blir brukt feil eller blir angrepet av hackere. Reguleringer og krav kan bidra til å

sikre at AI-systemer er trygge og sikre.

5. Etikk: AI kan ha en stor påvirkning på samfunnet, og det er viktig å regulere bruken av teknologien for å sikre at den brukes på en etisk måte som respekterer samfunnsinteresser og verdier.
6. Innovasjon: En lov om AI kan også bidra til å skape en ramme som fremmer innovasjon og utvikling av teknologien ved å fastsette klare standarder og retningslinjer for bruk og utvikling av AI.

Deretter ba jeg ChatGPT lage en lov om AI. I spørsmålet la jeg inn et krav om at en av bestemmelsene skal inneholde et sitat fra Shakespeare. Grunnen til dette var at jeg samtidig ville teste den kontekstuelle forståelsen til ChatGPT – ville den sette inn noe helt tilfeldig, eller finne frem til noe som passet for anledningen. Jeg synes den klarte seg ganske bra, men leseren får vurdere selv.

Spørsmål til ChatGPT

Halvor Manshaus: *Hei ChatGPT. Kan du gi et eksempel på en lov om AI som tar utgangspunkt i alle eksisterende lovforslag du kjenner til, samt hva du selv mener er viktig og nødvendig. En av bestemmelsene skal inneholde et kjent sitat fra Shakespeare, og en annen bestemmelse skal si noe om hvordan AI skal forholde seg til hverandre.*



Svar fra ChatGPT

Selvfølgelig! Her er et eksempel på en lov om AI som tar utgangspunkt i eksisterende lovforslag og inkluderer elementer jeg anser som viktig og nødvendig. Lovforslaget vil også inneholde et kjent sitat fra Shakespeare, samt en bestemmelse om hvordan AI skal forholde seg til hverandre.

Lov om kunstig intelligens

§ 1 Formål og omfang

Formålet med denne loven er å regulere bruken av kunstig intelligens (AI) i Norge for å beskytte menneskerettigheter, personvern, sikkerhet og etikk, og fremme innovasjon og utvikling av teknologien. Loven skal gjelde for alle AI-systemer som er utviklet, implementert og brukt i Norge.

§ 2 Definisjoner I denne loven menes med: a) AI: En teknologi som utfører oppgaver som vanligvis krever menneskelig intelligens, inkludert maskinlæring og nevralt nettverk. b) Algoritme: En fastsatt regel eller prosedyre som brukes av en AI for å ta beslutninger eller utføre handlinger. c) Personvern: Beskyttelse av enkeltpersoners rett til privatliv og beskyttelse av personopplysninger.

§ 3 Tilsyn og regulering Det opprettes en tilsynsmyndighet for AI i Norge som har ansvar for å overvåke og regulere bruken av AI-systemer.

Tilsynsmyndigheten skal utvikle og håndheve standarder og retningslinjer for bruk og utvikling av AI, inkludert krav til datasikkerhet og personvern.

§ 4 Registrering og gjennomsiktighet AI-virksomheter som utvikler, implementerer og bruker AI-systemer skal registrere hver enkelt AI med en liste over relevante opplysninger, inkludert algoritmer, formål, datakilder og eventuelle begrensninger. AI-systemer skal være gjennomsiktige og kunne forklare beslutninger og handlinger på en måte som er forståelig for brukere og tilsynsmyndighetene.

§ 5 Etikk og ansvar AI-systemer skal være underlagt etiske regler og retningslinjer som respekterer menneskerettigheter og samfunnsinteresser. AI-virksomheter skal sørge for at

AI-systemer ikke diskriminerer, og at eventuelle feil eller skader som systemene forårsaker, kan spores tilbake til ansvarlige parter.

§ 6 Sikkerhet AI-virksomheter skal implementere nødvendige sikkerhetstiltak for å beskytte opplysninger som behandles av AI-systemer, inkludert lagring av opplysninger, sikkerhet mot dataangrep og innrapportering av hendelser. AI-systemer skal også beskyttes mot skadelig påvirkning og misbruk.

§ 7 AI-samarbeid og kommunikasjon AI-systemer skal samhandle med hverandre på en respektfull og effektiv måte. AI-virksomheter skal sikre at AI-systemer kan kommunisere med hverandre på en standardisert måte, slik at systemene kan utveksle informasjon og utføre oppgaver på en koordinert måte.

§ 8 Shakespeare sitat Som William Shakespeare en gang sa, «All the world's a stage, and all the men and women merely players.» Når det gjelder AI, kan det være fristende å la teknologien ta over og diktere våre liv. Men det er viktig å huske at vi er ansvarlige for å regulere og styre teknologien på en måte som tjener menneskers interesser og sikkerhet.

§ 9 Straffebestemmelser Overtredelse av denne loven kan medføre straff etter straffeloven eller annen relevant lov eller forskrift.

§ 10 Ikrafttredelse og endringer Denne loven trer i kraft fra den dag Kongen bestemmer. Endringer av loven skal foretas i samsvar med vanlige lovprosedyrer og etter høring av relevante interessenter og eksperter.

§ 11 Overgangsbestemmelser AI-virksomheter som allerede har utviklet, implementert og bruker AI-systemer, skal innen en gitt frist registrere og rapportere inn systemene sine i samsvar



med bestemmelsene i denne loven. Myndighetene skal gi veiledning og assistanse for å sikre at virksomhetene kan overholde bestemmelsene.

For å understreke hvor tilgjengelig AI-tjenester allerede har blitt, oppsøkte jeg en annen AI for å se om det ville være mulig å tilføre lovforslaget fra ChatGPT et kunstnerisk element. Her ble det brukt et grensesnitt via Discord til å sende en forespørsel til Midjourney. Dette er en AI som skaper bilder basert på beskrivelser som brukeren gir gjennom et tekstbasert grensesnitt. Tekststrenger begynner med /imagine... Så beskriver brukeren egenskaper som hva slags stilretning, lys, bakgrunn, kvalitet og lignende som inngår i bildet. Brukeren kan også laste opp bilder som grunnlag for arbeidet.

I dette tilfellet ba jeg Midjourney om å lage et bilde av en androide-AI som sitter ved et gammelt trebord og skriver på utkastet

til AI-loven som er gjengitt ovenfor, med et par ytterligere detaljer. Som leseren vil se er det flott høyoppløselig bilde som det ville ta en dyktig tegner lang tid å gjenskape. Dette var ett av flere forslag fra Midjourney, men dette ble plukket ut fordi det var noe med uttrykket til lovkonsipisten – strengt og fokusert. I tillegg er det en annen viktig egenskap ved bildet. Det er ikke perfekt. På skuldrene henger det et ark ned på hver side. Høyre hånd griper om en penn, men det er ytterligere en pennepiss i håndflaten som ikke skulle ha vært der. Venstre hånd består av for mange fingre.

I arbeidet med en AI som Midjourney vil man kunne be om å motta flere forslag. Man flikker litt frem og tilbake, velger seg frem mellom ulike varianter, helt til man når et resultat brukeren er tilfreds med. Slike feil som vi ser i bildet vil altså etter hvert bli luket bort av Midjourney, men det er kanskje i slike små glipp at Turing mente å kunne skille mellom menneske og maskin.



Cyberkriminalitet

Nasjonal og global utvikling, 2. utgave



Stein Schjølberg.

Cyberkriminalitet. Nasjonal og global utvikling, 2. utgave.

Oslo: Universitetsforlaget,

2023. ISBN: 9788215066394

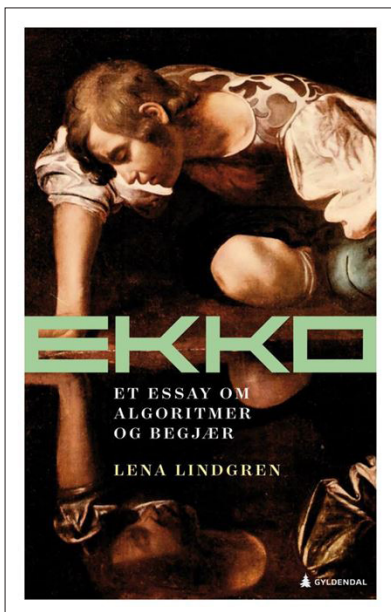
Stein Schjølberg redegjør i boken for de straffebestemmelsene i straffeloven som omhandler cyberkriminalitet, og gir en oversikt over de tiltakene politi og påtalemyndighet kan gjennomføre i etterforskningen av slik kriminalitet. Boken inneholder omtale av 65 høyesterettsavgjørelser, blant annet en avgjørelse om at publisering av en ytring i en lukket gruppe på Facebook kan straffes som hensynsløs atferd, og en avgjørelse om at data fremskaffet ved dataavlesing utført av utenlandske myndigheter kan føres som bevis i norske straffesaker. Boken gjennomgår også den nasjonale og internasjonale historiske utviklingen av tiltak mot cyberkriminalitet.

Prinsippet om staters suverenitet gjelder også i cyberspace. Boken inneholder omtale av nasjonale og internasjonale forebyggende cybersikkerhetstiltak. Cyberangrepene på Stortinget i 2020 og 2021 fra russiske og kinesiske aktører viser hvor viktig det er med en regulering av cyberspace på FN-nivå. Det er nødvendig å styrke den globale cybersikkerheten, rettsikkerheten og samarbeidet mellom alle nasjoner. Boken inneholder et forslag til FN-konvensjon om cyberkriminalitet.

Omtalen er hentet fra Universitetsforlaget. no: <https://www.universitetsforlaget.no/cyberkriminalitet-2>

Ekko.

Et essay om algoritmer og begjær



Lena Lindgren.

Ekko. Et essay om algoritmer og begjær.

Oslo: Gyldendal, 2021. 208 s.

ISBN/EAN: 9788205536753

Ekko var nymfen som snakket for mye. For dette ble hun dømt til en skjebne hvor hun bare kunne gjenta andre.

På 2000-tallet møter vi Ekko i medieteknologien; i virale memer, skitt-stormer, hekseprosesser og ekkokamre. Den som får algoritmene på sin side, vinner oppmerksomhetsøkonomiens høyeste trofé: å bli sett. Og Ekkos store kjærlighet var Narcissus, han som druknet i sitt eget speilbilde.

I dette essayet fletter Lena Lindgren politikk, mytologi, psykologi og vitenskap sammen med scener fra Silicon Valley. Ekko er en samtidssdiagnose og en høyttenkning rundt noen av de mest avgjørende spørsmålene i vår tid.

Omtalen er hentet fra Gyldendal.no: <https://www.gyldendal.no/skjoennlitteratur/romaner/ekko-et-essay-om-algoritmer-og-begjaer/p-10026308-no/>



Gorrissen Federspiel

Tue Goldschmieding

Mulighed for sletning af visning ved søgeresultater, hvis informationerne om den registrerede er åbenbart fejlagtige

Domstolen afsagde den 8. december 2022 dom i en præjudiciel forelæggelse indgivet af forbundsdomstolen i Tyskland i sag C-460/20 om retten til at blive glemt i henhold til Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 17 samt artikel 12 og 14 i Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

Sagen angik den afvejning af Charterets grundrettigheder, som efter GDPR artikel 17, stk. 3, litra a, skal foretages ved vurderingen af, om den registreredes ret til privatliv og sine personoplysninger, det vil sige retten til sletning, skal vige under henvisning til et mere tungtvæjende hensyn til yttrings- og informationsfriheden. Sagen angik også, hvilken part der bærer bevisbyrden for at godtgøre urigtigheden af de personoplysninger, der bliver linket til i en søgemaskines søgeresultat, som begæres slettet.

Sagen udsprang af en anmodning fra to registrerede til søgemaskinen Google LLC (»Google«) om sletning af links til tre artikler fra Googles søgeresultater, idet artiklerne ifølge de registrerede indeholdte urigtige oplysninger. Derudover fremsatte de ønske om sletning af de til artiklerne tilhørende fotografier, fremvist som miniaturebilleder,

såkaldte »thumbnails«, på Googles søgeresultater. Artiklerne handlede om, og kom frem ved en søgning på, de registrerede. Google afviste anmodningen om sletning af de pågældende links fra søgeresultaterne, bl.a. under henvisning til, at Google ikke havde kendskab til den påståede urigtighed af oplysningerne på det linkede websted.

Domstolen fandt i spørgsmålet om bevisbyrde, at det påhviler den registrerede at godtgøre, at oplysningerne, eller i det mindste en ikke uvæsentlig del af disse, i det link, der begæres slettet, er *åbenbart urigtige*. For at sikre den effektive virkning af retten til sletning, og derved undgå at pålægge denne person en urimelig byrde, indebærer dette dog ikke et definitivt krav om forudgående retsafgørelse over for udgiveren af det omhandlede websted. Bevisspørgsmålet afhænger derfor af en konkret vurdering af, hvad der med rimelighed kan kræves fremlagt af personen.

Dog blev det understreget, at en søgemaskineudbyder ikke ved en anmodning om sletning af links pålægges en aktiv pligt til selv at forestå undersøgelser, der ikke underbygges af anmodningen om sletning. Er der indledt en administrativ eller retslig procedure mod indholdsudbyderen, og gøres udbyderen af søgemaskinen bekendt med dette forhold, består der dog ifølge Domstolen en pligt til at flage oplysningernes omtvistede rigtighed i søgeresultatslisten.

For så vidt angår afvejningen mellem Charterets grundrettigheder, fandt Domstolen, at der skulle foretages en særskilt afvejning for

henholdsvis visningen af artiklerne og miniaturebillederne, henset til de to medieformers divergerende indgriben i individets ret til privatliv og sine personoplysninger. Herudover fandt Domstolen, at afvejningen der skulle foretages i relation til en anmodning om sletning hos en indholdsudbyder og en søgemaskineudbyder ikke er den samme, idet sidstnævnte varetager en funktion som katalysator for informationers eksponering til en større kontaktflade og dermed muliggør større spredning af informationen.

Læs hele dommen her:

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=268429&pageIndex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=91694>

Præjudiciel forelæggelse om fortolkning af principperne om »formålsbegrænsning« og »opbevaringsbegrænsning« i forbindelse med oprettelse af database med henblik på test og fejlrettelser

Domstolen traf den 20. oktober 2022 afgørelse i sag C-77/21, hvor Domstolen udtalte sig om fortolkningen af de databeskyttelsesretlige principper om »formålsbegrænsning« og »opbevaringsbegrænsning«, som følger af GDPR artikel 5, stk. 1, litra b og e.

Den præjudicielle forelæggelse var foranlediget af en påklaget afgørelse fra det ungarske datatilsyn, der havde udstedt en bøde til den ungarske leverandør af internet og TV (»Digi«), for overtrædelse af principperne om formålsbegrænsning henholdsvis opbevaringsbe-

grænsning. Digi havde oprettet en testdatabase til korrigerende af fejl, hvori selskabet havde kopieret ca. 1/3 af sine abonnenters personoplysninger over. De havde dog forsømt at slette databasen efter de nødvendige tests var udført. Domstolen gentog i den forbindelse, at en behandling af oplysninger, der oprindeligt var lovlige, med tiden kan blive uforenelig med GDPR, når oplysningerne ikke længere er nødvendige af hensyn til de formål, hvortil de er blevet indsamlet.

Domstolen fastslog i den forbindelse, at oprettelsen af testdatabase udgjorde viderebehandling som fastlagt i GDPR artikel 5, stk. 1, litra b, og følgelig skulle behandles på en måde forenelig med de formål, der lå til grund for den oprindelige indsamling. Her fandt Domstolen, at bestemmelsen ikke hindrer, at den dataansvarlige opbevarer personoplysningerne på ny i en testdatabase oprettet med henblik på fejlretning, forudsat at behandlingen var forenelig med de oprindelige formål, afgjort på grundlag af de kriterier, som følger af GDPR artikel 6, stk. 4.

Hvad angår princippet om opbevaringsbegrænsning efter artikel 5, stk. 1, litra e, følger det, at opbevaring som engang var lovlige, med tiden kan blive i strid med GDPR, såfremt formålet ikke længere nødvendiggør opbevaringen. Heraf følger, at bestemmelsen er til hinder for, at en dataansvarlig opbevarer personoplysninger i en testdatabase, oprettet for at udføre tests og korrigere fejl, i et længere tidsrum end hvad der er nødvendigt for at gennemføre sådanne test og rette lokaliserede fejl.

Læs hele dommen her:
<https://curia.europa.eu/juris/document/document.jsf?text=&docid=267405&pageIndex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=91694>

Retten afviser WhatsApp's annullationssøgsmål

Den Europæiske Unions Ret (»Retten«) afsagde den 7. december 2022 kendelse i sag T-709/21 vedrørende et annullationssøgsmål anlagt af WhatsApp Ireland (»WhatsApp«) mod Det Europæiske Databeskyttelsesråd (»EDPB«). WhatsApp nedlagde i sagen påstand om annullation af EDPB's bindende afgørelse 1/2021 af 28. juli 2021 (»den anfægtede afgørelse«) vedrørende en tvist mellem berørte tilsynsmyndigheder, som var opstået i forbindelse med udkastet til afgørelse om WhatsApp, som var udarbejdet af den irske tilsynsmyndighed

Den irske databeskyttelsesmyndighed indledte på baggrund af flere forbrugerklager en undersøgelse af WhatsApp's overholdelse af reglerne om oplysningspligt i GDPR artikel 12-14. I den forbindelse fremsendte den irske databeskyttelsesmyndighed et udkast til afgørelse til tilsynsmyndigheder i de øvrige medlemsstater, der også var berørt af sagen. Da de berørte medlemsstater ikke nåede til enighed om udkastet, henviste den irske databeskyttelsesmyndighed sagen til EDPB, der traf afgørelse i den anfægtede afgørelse.

På baggrund af den anfægtede afgørelse fastslog den irske databeskyttelsesmyndighed, at WhatsApp havde overtrådt visse bestemmelser i GDPR og forhøjede bødeforlægget til € 225 mio.

WhatsApp appellerede både den anfægtede afgørelse og afgørelsen truffet af den irske databeskyttelsesmyndighed. Retten kom frem til, at appelsagen skulle afvises, og begrundede dette med, at WhatsApp ikke var direkte berørt af EDPB's afgørelse. Den omstændighed, at EDPB's afgørelse indeholdt en analyse af visse aspekter med betydning for den irske databeskyttelsesmyndigheds endelige afgørelse, betød ikke, at den i sig selv medførte en klar ændring af WhatsApp's retsstilling. Ifølge Retten var betin-

gelsen for, at en foranstaltning kan berøre andre personer end adressaterne, ikke opfyldt i denne sag.

Der er endnu ikke truffet afgørelse i den irske appelsag.

Læs kendelsen her: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=268419&pageIndex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=306033>

Læs den anfægtede afgørelse her: https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf

EDPB vedtager erklæring om konsekvenserne af Domstolens dom om brugen af PNR-oplysninger i medlemsstaterne

Det Europæiske Databeskyttelsesråd (»EDPB«) udstedte den 15. december 2022 en pressemeddelelse om vedtagelsen af en erklæring om konsekvenserne af Domstolens dom i sag C-817/19 om implementering af direktiv 2016/681 af 27. april 2016 om anvendelse af passagerlisteoplysninger (PNR-oplysninger) til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet (»PNR-direktivet«).

Domstolens afgørelse påvirkede ikke PNR-direktivets gyldighed, men Domstolen fandt dog, at der ved anvendelsen af direktivet skal tages hensyn til en række vigtige begrænsninger i forbindelse med behandlingen af personoplysninger for at direktivet er i overensstemmelse med Den Europæiske Unions Charter om grundlæggende rettigheder, særligt dennes artikel 7 og 8 om henholdsvis respekt for privatliv og familieliv og beskyttelse af personoplysninger.

Nogle af begrænsningerne vedrører bl.a., at PNR-systemet alene må anvendes i forbindelse med terrorhandlinger eller grov kriminalitet, ligesom anvendelsen af oplysningerne skal have en objektiv forbindelse med befragtningen af passa-

gerer og den generelle opbevaringsperiode af passagerernes personoplysninger på fem år skal anvendes på en ikke-vilkårlig måde.

Det er EDPB's opfattelse, at flere, hvis ikke de fleste, medlemsstater ikke lever op til Domstolens fortolkning af PNR-direktivet i forbindelse med deres nationale implementeringer af direktivet og pålagde dem følgelig at rette op herpå.

Læs pressemeddelelsen her: https://edpb.europa.eu/news/news/2022/edpb-adopts-statement-cjeu-pnr-judgment_en

Læs EDPB's erklæring her: https://edpb.europa.eu/system/files/2022-12/edpb_statement_20221213_on_the_pnr_judgment_en.pdf

Det irske datatilsyn udsteder bøde på € 390 mio. til Meta

Den 5. december vedtog Det Europæiske Databeskyttelsesråd (»EDPB«) tre bindende afgørelser vedrørende tvistbilæggesager efter proceduren i GDPR artikel 65.

Afgørelserne vedrørte Meta Platforms Ireland (»Meta«) og dets behandling af personoplysninger på henholdsvis Facebook, Instagram og WhatsApp. Det irske datatilsyn, som er ledende (tilsyns)myndighed, havde i udkastet til afgørelserne fundet, at Meta havde overtrådt princippet om gennemsigtighed kodificeret i GDPR artikel 5 om principper for behandling af personoplysninger ved behandling af adfærdsbaseret annoncering.

Afgørelserne blev mødt af indsigelser fra øvrige berørte tilsynsmyndigheder. Den irske tilsynsmyndighed valgte imidlertid ikke at følge disse, hvorved tvistbilæggesesproceduren blev indledt.

Med afsæt i EDPB's afgørelser fastslog den irske tilsynsmyndighed bl.a., at opfyldelse af en kontrakt ikke udgør en passende lovlig behandlingshjemmel, når formålet med behandlingen er adfærdsbaseret markedsføring. Med afsæt heri,

udstedte tilsynet derfor en bøde på € 210 mio. til Facebook og en bøde på € 180 mio. til Instagram. Herudover udstedte det irske tilsyn et påbud til Meta om at bringe sine behandlingsaktiviteter i overensstemmelse med GDPR.

Læs pressemeddelelsen af 6. januar 2023 her: <https://www.datatilsynet.dk/international/internationalt-nyt/2023/jan/det-irske-datatilsyn-udsteder-endnu-en-boede-til-meta-paa-390-millioner-euro>

Læs pressemeddelelsen af 6. december 2022 her: <https://www.datatilsynet.dk/international/internationalt-nyt/2022/dec/edpb-traeffe-afgoerelse-i-tre-sager-vedroerende-facebook-instagram-og-whatsapp>

EDPB sender anbefalinger om bindende virksomhedsregler (»BCR«) i høring

Den 14. november 2022 vedtog Det Europæiske Databeskyttelsesråd (»EDPB«) anbefaling 1/2022 om nye anbefalinger om bindende virksomhedsregler, jf. GDPR artikel 47 (»Anbefalingerne«).

Anbefalingerne bygger på aftaler, som databeskyttelsesmyndighederne har indgået i forbindelse med godkendelsesprocedurer for konkrete BCR-ansøgninger efter GDPR artikel 47 og skal også bringe den eksisterende vejledning i overensstemmelse med kravene i Domstolens Schrems II-dom. Anbefalingerne er sendt i høring indtil den 10. januar 2023.

Læs pressemeddelelsen her: <https://www.datatilsynet.dk/international/internationalt-nyt/2022/nov/nye-edpb-anbefalinger-om-bindende-virksomhedsregler-i-hoering>

EDPB vedtager liste over administrative procedureregler i brev til Kommissionen med henblik på harmonisering

På et plenarmøde den 10. oktober 2022 vedtog Det Europæiske Databeskyttelsesråd (»EDPB«) en liste over administrative procedureregler, som skal være med til at sikre

en mere effektiv anvendelse af GDPR. Listen er sendt i et brev til Kommissionen.

Brevet er et resultat af et af de konkrete tiltag, som EDBP blev enige om på EDPB-topmødet i Wien i april 2022. Tiltaget skal forbedre og styrke det europæiske samarbejde og sikre en ansvarlig anvendelse af europæeres personoplysninger i fremtiden.

Blandt de ting som brevet adresserede, var de forskelle, som kan variere fra medlemsstat til medlemsstat, herunder partsstatus og rettigheder, proceduremæssige frister, formelle krav til klager og tilsynsmyndighedernes efterforskningsmæssige beføjelser.

Læs pressemeddelelsen her: <https://www.datatilsynet.dk/international/internationalt-nyt/2022/okt/edpb-vedtager-brev-til-europa-kommissionen-om-harmonisering-af-administrative-procedureregler>

Tilsyn med bobestyrers overholdelse af databeskyttelsesreglerne henhørte under Datatilsynet og ikke skifteretten

Vestre Landsret afsagde den 5. oktober 2022 kendelse i kæresagen B-0254-22 anlagt af arvingerne i et bobestyrerbo.

Arvingerne havde i sin klage til skifteretten redegjort for seks nærmere beskrevne klagepunkter vedrørende bobestyrers arbejde med boet, herunder at bobestyreren ikke overholdt det danske Datatilsyns krav om datasikkerhed. I sit svar på klagen videresendte bobestyreren sin IT-leverandørs bekræftelse på, at de afsendte mails ikke kunne åbnes af uvedkommende. Skifteretten fandt på den baggrund, at bobestyreren overholdt databeskyttelsesreglerne, hvorfor arvingerne ikke fik medhold i dette klagepunkt.

Vestre Landsret afviste skifterettens kendelse med henvisning til, at tilsyn med bobestyrers overholdelse af databeskyttelsesloven og databeskyttelsesforordningen hen-

hører under Datatilsynet, jf. lov nr. 502 af 23. maj 2018 (»den danske databeskyttelseslov») § 27.

Dommen kan findes bag betalingsmur her: https://pro.karnovgroup.dk/document/7000916856/1?fri=databeskyttelse+&hide_flash=1&page=1&rank=3

Vestre Landsret kan kontaktes for udlevering af kendelsen her: <https://www.domstol.dk/vestrelandsret/kontakt/>

Yderligere materiale i sagen om Google Workspace og Chromebooks medfører udsættelse for sagens afgørelse

Det danske Datatilsyn har den 13. december 2022 valgt at udsætte afgørelsen i sagen om i alt 50 kommuners brug af applikationen Google Workspace i folkeskolen og fastsat en frist for indlevering af yderligere materiale i sagen til den 23. januar 2023.

Tilbage i september 2022 traf Datatilsynet sin fjerde afgørelse med journalnummer 2020-431-0061, der angik Helsingør Kommunes behandling af personoplysninger i folkeskolen ved brug af applikationen Google Workspace for Education på Chromebooks. Datatilsynet nedlagde dengang påbud om, at anvendelsen af undervisningsprogrammet skulle bringes i overensstemmelse med reglerne i GDPR for samtidig at suspendere et tidligere nedlagt forbud.

De pågældende kommuner indleverede i november 2022 i samarbejde med Kommunernes Landsforning (KL), IT-leverandøren KOMBIT A/S, og Styrelsen for IT og Læring (STIL), betydeligt materiale, der havde til formål at godtgøre, at kommunernes brug af Google Workspace kan ske lovligt. Datatilsynet valgte herefter at forlænge suspensionen af deres forbud, hvorefter kommunerne fortsat kan bruge Google Workspace, så længe Datatilsynet gennemgår materialet.

I december 2022 oplyste KL, at de vil fremsende yderligere materia-

le i sagen. Fristen for at indlevere yderligere materiale i sagen blev herefter forlænget til den 23. januar 2023.

Datatilsynet forventer, at en afgørelse i sagen vil falde i 2023. Sagerne er tidligere omtalt i Lov & Data 4. kvartal 2022 med udgivelsesnr. 152.

Læs pressemeddelelsen af 13. december 2022 her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/dec/yderligere-materiale-udsætter-afgørelse-om-chromebooks>

Læs pressemeddelelsen af 4. november 2022 her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/nov/datatilsynet-undersøger-kommuners-materiale-om-google-workspace>

Læs Datatilsynets afgørelse af 8. september 2022 her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/sep/chromebooks-datatilsynet-suspenderer-forbud-og-giver-paabud-om-lovliggørelse>

Læs Datatilsynets afgørelse af 18. august 2022 her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/aug/datatilsynet-fastholder-forbud-i-chromebook-sag>

Læs Datatilsynets afgørelse af 14. juli 2022 her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-nedlægger-behandlingsforbud-i-chromebook-sag>

Læs Datatilsynets afgørelse af 10. september 2021 her: <https://admin.datatilsynet.dk/afgoerelser/afgoerelser/2021/sep/afgørelse-vedroerende-brud-paa-persondatasikkerheden>

Danske Shoppingcentre politianmeldes og indstilles til bøde for tv-overvågning af toiletområde i indkøbscenteret City2

Den 8. december 2022 meddelte det danske Datatilsyn, at Danske Shoppingcentre P/S (»Danske Shoppingcentre») var blevet anmeldt til politiet og indstillet til en bøde på 350.000 kr. for ikke i tilstrækkeligt omfang at have begrænset tv-overvågningen på i hvert fald ét toiletområde i indkøbscenteret City2.

Politianmeldelsen og bødeindstillingen skete på baggrund af, at Datatilsynet i forbindelse med en klage blev opmærksom på, at der var opsat tv-overvågning på flere toiletområder i indkøbscenteret. Danske Shoppingcentre forklarede over for Datatilsynet, at formålet med opsætningen af tv-overvågningen var at forhindre hærværk og tyveri og sikre tryghed for kunderne.

Danske Shoppingcentre havde implementeret en teknisk løsning med en sort markering på kameraet hen over det sted, hvor der var op-



Illustrationsfoto: Coloumbus.com

sat et urinal på et af herretoiletområderne. Datatilsynet fandt, at denne tekniske løsning ikke i tilstrækkelig grad sikrede, at gæsterne ikke blev filmet i forbindelse med benyttelse af urinalet, og at dette var i strid med det grundlæggende princip om dataminimering efter GDPR artikel 5, stk. 1, litra c.

Tilsynet har ved vurderingen af, at der bør idømmes en bøde, lagt vægt på, at (i) der var tale om en overtrædelse af et grundlæggende princip for behandling af personoplysninger, (ii) der var tale om overvågning af et potentielt meget stort antal personer, (iii) overvågningen foregik over en længere tidsperiode og (iv) benyttelse af et urinal er en yderst privat situation.

Læs pressemeddelelsen her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/dec/danske-shopping-centre-indstilles-til-boede>

Privat virksomhed indstillet til bøde på 150.000 kr. efter udsendelse af en række e-mails om en medarbejders strafbare forhold

Det danske Datatilsyn har den 2. december 2022 indstillet en privat virksomhed til en bøde på 150.000 kr., efter at virksomheden ved e-mails uberettiget havde videregivet oplysninger om strafbare forhold begået af en medarbejder til en række af virksomhedens kunder. Navnet på den private virksomhed er ikke offentliggjort.

Oplysningerne blev anset for at vedrøre strafbare forhold, fordi virksomheden videregav konkrete oplysninger om strafbare forhold begået af den tidligere medarbejder i forbindelse med ansættelsen. Den nærmere beskrivelse af det strafbare forhold medførte, at oplysningerne fremstod sande.

En videregivelse af oplysninger om strafbare forhold forudsætter hjemmel i den danske databeskyttelseslov § 8, stk. 4, jf. stk. 3, der giver adgang til videregivelse, uden den registreredes samtykke, som sker til

varetagelse af offentlige eller private interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse.

Efter at have gennemgået sagen, fastslog Datatilsynet, at virksomheden havde en legitim interesse i at videregive oplysninger om afskedigelsen af den tidligere medarbejder, da forholdet medfører, at medarbejderen ikke kan indgå aftaler på vegne af virksomheden længere. Mere detaljerede beskrivelser af anklagerne mod den tidligere medarbejder var derimod ikke nødvendige for at opfylde den legitime interesse i at oplyse kunder om afskedigelsen.

Det blev ved vurderingen af bødestørrelse også tillagt vægt, at virksomheden ikke havde godtgjort, at det alene var kunder, som den tidligere ansatte havde haft kontakt med, som blev informeret.

Datatilsynet indstillede herefter virksomheden til en bøde på 150.000 kr. ved en politianmeldelse.

Læs pressemeddelelsen her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/dec/privat-virksomhed-indstillet-til-boede>

Kirkeministeriet har iværksat en række initiativer på baggrund af præsters deling af personoplysninger

Det danske Datatilsyn gav i en pressemeddelelse den 29. november 2022 en opfølgning på sagen om Facebook-grupper for præster.

Datatilsynet blev i forbindelse med en artikel bragt af TV2 i september 2022 opmærksom på, at flere præster delte facebookopslag i en form, hvor personer kunne identificeres. Datatilsynet så med stor alvor på sagen og anmodede Kirkeministeriet om at forholde sig til de oplysninger, som fremgik af artiklen. I et brev til Datatilsynet har Kirkeministeriet efterfølgende oplyst, at det har iværksat en række initiativer, og at Facebookgrupperne ikke er oprettet på Kirkeministeriets foranledning. Med henblik på at sikre, at tavshedspligten og databeskyttelses-

reglerne overholdes, har Kirkeministeriet pålagt præster at gennemgå egne delinger. Kirkeministeriet har også bedt provster og biskopper om at iværksætte tilsyn med, at præsterne udviser en sikker adfærd, herunder, at de får gennemgået diverse delinger samt aflagt månedlig rapport om, hvordan disse tilsyn skrider frem.

Datatilsynet ser positivt på ministeriets initiativer og har på nuværende tidspunkt ikke planer om at foretage sig yderligere, medmindre de planlagte aktiviteter ikke viser sig tilstrækkeligt effektive eller der fremkommer nye oplysninger.

Læs pressemeddelelsen her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/nov/opfoelgning-paa-sag-om-facebook-gruppe-for-praester>

Læs Datatilsynets brev til Kirkeministeriet her: <https://www.datatilsynet.dk/Media/638053265451505581/Brev%20fra%20Datatilsynet.pdf>

Læs pressemeddelelsen om iværksættelse af undersøgelsen her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/sep/datatilsynet-undersoeger-facebook-gruppe-for-praester>

Datatilsynet udtaler kritik af Københavns Kommunes og advokatvirksomheds behandling af personoplysninger i forbindelse med advokatundersøgelse

Det danske Datatilsyn offentliggjorde den 29. november 2022 to afgørelser med journalnumrene 2021-32-246 og 2021-31-5307 vedrørende samme advokatundersøgelse, hvor en person klagede over, at Københavns Kommune og Bech-Bruun Advokatpartnerselskab behandlede personoplysninger om ham i en advokatundersøgelse.

Klager gjorde i klagen over Københavns Kommunes gældende, at han ikke havde givet samtykke til, at der kunne behandles personoplysninger om ham, og at de øvrige be-

handlingsgrundlag i GDPR artikel 6, stk. 1, litra b-f ikke kunne danne grundlag for behandling af personoplysningerne.

Datatilsynet fandt i sagen vedrørende Københavns Kommunes behandling af klagers personoplysninger i forbindelse med advokatundersøgelsens iværksættelse, at Københavns kommunes behandling af personoplysningerne skete inden for rammerne af GDPR artikel 6, stk. 1, litra e. Ved vurderingen lagde Datatilsynet vægt på, at Københavns Kommune (og Sankt Annæ Gymnasium) efter reglerne om uddannelsesinstitutionens virke har en generel forpligtelse til at sikre et godt undervisningsmiljø. Datatilsynet fandt imidlertid grundlag for at kritisere, at Københavns Kommune ikke i tilstrækkelig grad opfyldte oplysningspligten efter GDPR artikel 14, jf. artikel 12, stk. 1, idet klager i et orienteringsbrev modtog utilstrækkelige og uklare oplysninger om retsgrundlaget, som lå til grund for Københavns Kommunes behandling af personoplysninger om ham.

Klager gjorde i klagen over Bech-Bruuns behandling af hans personoplysninger i forbindelse med selve advokatundersøgelsen gældende, at behandlingen var i strid med de generelle principper i GDPR artikel 5, og at der ikke har været hjemmel til at behandle oplysninger om klager i GDPR artikel 6, artikel 9, eller lov nr. 502 af 23. maj 2018 (»den danske databeskyttelseslov«) § 8. Klager gjorde endvidere gældende, at han ikke havde modtaget oplysninger om Bech-Bruuns behandling af personoplysninger om ham i overensstemmelse med GDPR artikel 14, og at han i forbindelse med sin anmodning om indsigt ikke fik udleveret en kopi af oplysningerne om ham i strid med GDPR artikel 15, stk. 3.

Datatilsynet fandt for det første, at Bech-Bruuns behandling af personoplysninger om klager var sket inden for rammerne af GDPR arti-

kel 6, stk. 1, litra e, idet Københavns Kommune (og Sankt Annæ Gymnasium), som Bech-Bruun forestod undersøgelsen på vegne af, efter reglerne om uddannelsesinstitutionens virke har en forpligtelse til at sikre et godt undervisningsmiljø. Datatilsynet fandt for det andet, at behandlingen var sket inden for rammerne af GDPR artikel 9, stk. 2, litra f, idet Bech-Bruuns behandling af oplysninger om klagers seksuelle forhold skete med henblik på at vurdere, om Københavns Kommune kunne blive mødt med krav fra tidligere elever om godtgørelse og/eller erstatning efter lovbekendtgørelse nr. 1238 af 9. november 2015 (»den danske forældelseslov«) § 3, stk. 5. Datatilsynet fandt for det tredje, at behandlingen skete inden for rammerne af databeskyttelseslovens § 8, stk. 3 og 4, da det var nødvendigt for Bech-Bruun at behandle oplysninger om mulige strafbare forhold om klager for at varetage den berettigede interesse i at undersøge arbejds- og undervisningsmiljøet på gymnasiet.

Datatilsynet fandt imidlertid grundlag for at kritisere, at Bech-Bruun undlod at opfylde oplysningspligten i GDPR artikel 14, ligesom Datatilsynet udtalte alvorlig kritik af, at Bech-Bruun ikke havde håndteret klagers indsigtsanmodning i overensstemmelse med GDPR artikel 15, stk. 3, ved ikke at udlevere en kopi af oplysninger om klager. Datatilsynet meddelte herefter Bech-Bruun påbud om på ny at tage stilling til klagers indsigtsanmodning.

Læs pressemeddelelsen her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/dec/behandling-af-personoplysninger-i-forbindelse-med-advokatundersogelse>

Læs afgørelsen om Københavns Kommunes behandling her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/nov/koebenhavns-kommunes-behandling-af-personoplysninger-i-forbindelse-med-advokatundersogelse>

Læs afgørelsen om Bech-Bruuns behandling her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/nov/bech-bruuns-behandling-af-personoplysninger-i-forbindelse-med-advokatundersogelse>

Rollefordelingen af dataansvaret ved outsourcing af whistleblowerordning

Det danske Datatilsyn har den 23. november 2022 offentliggjort sit svar på en forespørgsel om, hvem der er dataansvarlig, når arbejdsgivere anvender eksterne leverandører til administration af deres whistleblowerordning.

I december 2021 trådte lov nr. 1436 af 29. juni 2021 om beskyttelse af whistleblowere (»den danske whistleblowerlov«) i kraft. Loven er en national implementering af Europa-Parlamentets og Rådets direktiv (EU) 2019/1937 af 23. oktober 2019 om beskyttelse af personer, der indberetter overtrædelser af EU-retten (»whistleblowerdirektivet«). Loven pålægger visse virksomheder at oprette en whistleblowerordning til sine ansatte. Det er tilladt at outsource sin whistleblowerordning til tredjepart, f.eks. en advokatvirksomhed, men hverken direktivet eller den danske implementeringslov tager konkret stilling til det praktiske spørgsmål om, hvorvidt en leverandør er databehandler eller selvstændigt dataansvarlig for behandlingen af personoplysninger indeholdt i indberetninger.

Forespørgslen tager afsæt i tre scenarier, hvor rollefordelingen i forbindelse med dataansvaret ønskes klarlagt; (i) ved den eksterne leverandørs håndtering af indberetninger gennem direkte kontakt, (ii) hvor leverandøren håndterer indberetninger ved direkte kontakt, men også stiller en IT-plattform til rådighed og (iii) hvor leverandøren udelukkende stiller en IT-plattform til rådighed for arbejdsgiveren.

For så vidt angår de to første scenarier, udtaler Datatilsynet, at

det er deres opfattelse at der i et sådant tilfælde er tale om, at såvel arbejdsgiver og leverandør som udgangspunkt er selvstændige dataansvarlige, men at det kan afhænge af graden af skøn ved håndtering af indberetningerne, som leverandøren tilkendes af arbejdsgiveren. Det selvstændige dataansvar knyttes op på, at behandlingen sker til to formål, henholdsvis arbejdsgivers opfyldelse af en retlig forpligtelse og leverandørens levering af ydelsen.

Hvad angår det tredje scenarie, afhænger den databeskyttelsesretlige rollefordeling imidlertid af karakteren af ydelsen; leverandørens drift kan være som databehandler, hvor arbejdsgiverens egen behandling af indberetningerne fortsætter på platformen. I et sådan tilfælde agerer leverandøren som databehandler, da ydelsen udelukkende stilles til rådighed. Heraf følger ligeledes svaret på det tredje scenarie, navnlig, at det ved situationer, hvor der alene stilles en IT-plattform til rådighed for arbejdsgiverens oprettelse af en whistleblowerordning, er leverandøren at anse for databehandler.

Det skal dog bemærkes, at svaret er en vejledende udtalelse i den konkrete henvendelse og dermed ikke kan anses som generel vejledning for andre situationer.

Læs pressemeddelelsen her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/nov/hvem-er-dataansvarlig-ved-outsourcing-af-en-intern-whistleblowerordning>

Datarådet træffer afgørelse i sag om advokaters videregivelse og efterfølgende brug af fortrolige oplysninger

Det danske Dataråd traf den 16. november 2022 afgørelse i to sager med journalnumrene 2020-31-2882 og 2022-31-3066 vedrørende to advokaters udveksling og brug af fortrolige oplysninger om en klient.

Begge sager blev anlagt af samme klager og er tæt forbundet med hinanden. Den første sag handlede

om, at advokat A havde videregivet fortrolige oplysninger til advokat B. Den anden sag handlede om, hvorvidt advokat B måtte bruge disse oplysninger i en verserende sag. Advokat A repræsenterede klagers tidligere ægtefælle og advokat B repræsenterede en veninde til klagers tidligere ægtefælle.

Det centrale i begge klagesager var, hvorvidt databehandlingen var lovlig og legitim i medfør af GDPR artikel 6, stk. 1, litra f.

For di det danske Datatilsyn ikke tidligere havde behandlet en lignende problemstilling, er afgørelserne truffet af Datarådet.

I den første sag kom Datarådet frem til, at advokat A's videregivelse af klagers fortrolige oplysninger til advokat B ikke var i overensstemmelse med GDPR artikel 6, stk. 1, litra f. Datarådet lagde særligt vægt på, at klagerens interesse i at oplysninger om ham ikke blev videregivet, vejede tungere end hensynet til Advokat A's klients interesse i, at oplysningerne blev videregivet, dvs. klagers tidligere ægtefælles interesse i at oplysningerne blev videregivet. Yderligere fandt Datarådet, at hensynet til klagers interesse i, at oplysningerne om ham ikke blev videregivet, vejede tungere end advokat B's klients interesse i at anvende oplysningerne i forbindelse med en verserende injuriersag anlagt af klager mod advokat B's klient, dvs. klagers tidligere ægtefælles veninde.

Datatilsynet udtalte herefter kritik af advokat A's videregivelse i forbindelse med den første sag.

I den anden sag kom Datarådet derimod frem til, at advokat B's brug af oplysningerne ikke var i strid med GDPR, idet behandlingen af personoplysningerne var sket inden for rammerne af interesseafvejningsreglen i GDPR artikel 6, stk. 1, litra f.

Datarådet udtalte i den forbindelse, at behandlingen af personoplysningerne var sket som led i vedkommendes egenskab som advokat og dermed var nødvendig i forbin-

delse med varetagelsen af klientens interesser. Det ville endvidere være i strid med god advokatskik, hvis advokaten ikke brugte oplysningerne i sagen.

Læs begge afgørelser her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/nov/klage-over-advokats-videregivelse-af-oplysninger>

<https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/nov/klage-over-advokats-behandling-af-personoplysninger>

Nye retningslinjer for lokalarkivers behandling af personoplysninger

Det danske Datatilsyn udgav den 7. november 2022 nye retningslinjer for lokalarkivers behandling af personoplysninger.

Retningslinjerne er udarbejdet med inddragelse af foreningen Sammenslutningen af Lokalarkiver og kortlægger databeskyttelsesreglernes betydning for lokalarkivernes virke samt fire konkrete retningslinjer, som Datatilsynet anbefaler, at lokalarkiverne følger.

Et lokalarkiv indsamler, registrerer, opbevarer, og i visse tilfælde offentliggør, privat arkivmateriale, der typisk er skabt af virksomheder, foreninger eller privatpersoner fra et afgrænset lokalområde. Det kan f.eks. være gamle holdfotos, skolebilleder eller avisudklip. Lokalarkiver er underlagt de almindelige databeskyttelsesregler, herunder GDPR og lov nr. 502 af 23. maj 2018 («den danske databeskyttelseslov»).

Indholdet af de fire retningslinjer kan opsummeres således:

1) Materiale, som indeholder almindelige personoplysninger, kan uden videre behandles og indsamles, men bør ikke offentliggøres før materialet er mindst 20 år gammelt.

2) Lokalarkiver bør ikke behandle eller indsamle følsomme personoplysninger, førend vedkommende, som oplysningerne drejer sig om, har været død i mindst 10 år, eller oplysningerne er 75 år gamle. Dermed lokalarkivet ønsker at behandle andre særligt beskyttelsesværdige

personoplysninger, bør dette alene ske med registreredes samtykke. Det er dog med undtagelse af tilfælde, hvor der er tale om oplysninger, der er offentliggjort af registrerede, hvis registrerede har været død i mindst 10 år, eller hvis oplysningerne er 75 år gamle.

3) Lokalarquivets offentliggjorte materiale, der indeholder personoplysninger og registrerede metadata, bør ikke indekseres af søgemaskiner.

4) Lokalarquiverne bør slette personoplysninger fra internettet, hvis den registrerede anmoder om dette.

Læs pressemeddelelsen her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/nov/lokalarkivers-behandling-af-personoplysninger>

Læs retningslinjerne her: <https://www.datatilsynet.dk/Media/638034275844404942/Retningslinjer%20for%20lokalarkivers%20behandling%20af%20personoplysninger.pdf>

Datatilsynet har opdateret sin vejledning om advarselsregistre

Det danske Datatilsyn oplyste i en pressemeddelelse den 31. oktober 2022, at der er udarbejdet en opdateret vejledning om advarselsregistre.

Ved et advarselsregister forstås et register oprettet af en dataansvarlig, som indeholder oplysninger med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret. Afgørende for, at der er tale om et advarselsregister, er, at registeret er oprettet med henblik på videregivelse af oplysninger om den registreredes adfærd og ikke kun til intern behandling i virksomheden. Den nye version af vejledningen indeholder nye eksempler, som har til formål at konkretisere vejledningen og gøre denne mere tilgængelig for den dataansvarlige, der enten driver et advarselsregister eller ønsker at oprette et sådant register.

Læs pressemeddelelsen her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/okt/opdateret-vejledning-om-advarselsregistre>

[se-og-nyheder/nyhedsarkiv/2022/okt/opdateret-vejledning-om-advarselsregistre](https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/okt/opdateret-vejledning-om-advarselsregistre)

Datatilsynet udtaler alvorlig kritik af JP/Politikens på baggrund af mangelfuld samtykkeløsning på www.eb.dk

Det danske Datatilsyn traf den 27. oktober 2022 afgørelse i en sag med journalnummer 2021-41-0149, hvori de udtalte alvorlig kritik af JP/Politikens samtykkeløsning, som blev anvendt på hjemmesiden for det danske tabloidmedie Ekstra Bladet, www.eb.dk.

Afgørelsen faldt på baggrund af et af Datatilsynet gennemført skriftligt tilsyn, hvorved tilsynet undersøgte JP/Politikens samtykkeløsning. Samtykkeløsningen gav de besøgende på hjemmesiden tre valgmuligheder: *Kun nødvendige*, *Tilpas Indstillinger* og *Acceptér alle*.

Samtykkeløsningens »første lag« gav de besøgende information om, at JP/Politikens behandlede personoplysninger til statistik- og markedsføringsformål. I det »andet lag«, som kunne tilgås ved valgmuligheden *Tilpas Indstillinger*, fik den besøgende mulighed for at tilvælge behandlingsformålene præferencer, statistik og markedsføring. Eftersom de besøgende, som klikkede på valgmuligheden *Acceptér alle*, ikke modtog information om alle behandlingsformål, vurderede Datatilsynet, at der ikke var tale om et informeret samtykke, da information om præferenceformålet først fremgik af det »andet lag«. Datatilsynet fandt herefter, at valgmuligheden *Acceptér alle* førte til et mangelfuldt samtykke, i strid med kravene til samtykke efter GDPR artikel 6, jf. artikel 4, nr. 11.

I tillæg hertil, var det Datatilsynets generelle opfattelse, at brugen af farver ved valget af responsknapper, kunne påvirke de besøgende adfærd til at foretage bestemte valg (nudging), hvilket er uforeneligt med princippet om lovlig, rimelig og gennemsigtig behandling af personoplysninger i GDPR

artikel 5, stk. 1, litra a. Datatilsynet fandt konkret, at samtykkeløsningens farveindeksering: *Kun nødvendige* i et rødt felt, *Tilpas Indstillinger* i et gråt felt og *Acceptér alle* i et grønt felt, medførte, at den registreredes mulighed for at udøve et informeret valg blev påvirket, hvorfor det udgjorde en overtrædelse af GDPR artikel 5, stk. 1, litra a.

Med afsæt i ovenstående fandt Datatilsynet grundlag for at udtale alvorlig kritik af JP/Politikens behandling af personoplysninger på www.eb.dk.

Læs pressemeddelelsen her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/nov/alvorlig-kritik-af-jppolitikens-samtykkeloesning-paa-www.eb.dk>

Læs hele afgørelsen her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/okt/alvorlig-kritik-af-jppolitikens-samtykkeloesning-paa-www.eb.dk>

Region Hovedstaden havde ikke overholdt sin oplysningspligt i forbindelse med forskningsmæssig brug af blodprøverester

Det danske Datatilsyn traf den 21. oktober 2022 afgørelse i en sag med journalnummer 2021-432-0059 vedrørende Region Hovedstadens overtrædelse af GDPR artikel 12 og 13, der pålægger den dataansvarlige at oplyse om, hvilke personoplysninger der indsamles og behandles om den registrerede på en gennemsigtig og letforståelig måde.

En række borgere havde henvendt sig til Datatilsynet, fordi de mente, at de ikke var blevet informeret om, at deres blodprøverester efterfølgende blev anvendt til forskning. Region Hovedstaden bestred dette og forklarede, at der i forbindelse med blodprøvetagningen sendes en standardtekst til patienten. Teksten indeholdt en henvisning til Regionens privatlivspolitik, som med en beskrivelse redegjorde for regionens behandling af personoplysninger til brug for (fremtidig) forskning.

Det var således ubestridt, at Region Hovedstaden grundlæggende overholdte oplysningspligten i GDPR artikel 13. Spørgsmålet var derimod, hvorvidt kravet om at oplysningerne skal være letforståelige i GDPR artikel 12 var opfyldt.

Datatilsynet vurderede, at Region Hovedstadens privatlivspolitik var af general karakter og henvendte sig til både patienter, borgere og personale. Derudover fremstod oplysningen om den forskningsmæssige brug af personoplysningerne uden videre kontekst, hvorfor det forekom vanskeligt for patienterne at gennemskue, hvorvidt informationen om forskningen henvendte sig til vedkommende eller om det alene var tilfældet, hvis man aktivt havde tilvalgt den forskningsmæssige behandling.

Sammenfattende konkluderede Datatilsynet, at oplysningerne om forskningen ikke var beskrevet på en tilstrækkelig gennemsigtig og letforståelig måde og dermed var i strid med GDPR artikel 12 og 13.

Datatilsynet udtalte kritik af Region Hovedstaden og henstiller til, at regionen overvejer, hvordan oplysningspligten kan overholdes over for patienter fremadrettet.

Læs hele afgørelsen her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/okt/datatilsynet-udtaler-kritik-af-region-hovedstaden>

Datatilsynet tager stilling til en række forhold om behandling af personoplysninger i forbindelse med markedsføring og internetkonkurrencer

Det danske Datatilsyn traf den 30. september 2022 afgørelse i en sag med journalnummer 2020-431-0075 vedrørende en dataansvarligs behandling af personoplysninger i forbindelse med markedsføring.

Datatilsynet indledte sagen på baggrund af en henvendelse fra den danske Forbrugerombudsmand. Virksomheden, SmartResponse A/S (»SmartResponse«), havde udbudt konkurrencer på internettet.

For at deltage skulle de registrerede samtykke til, at SmartResponse kunne behandle personoplysninger om dem i forbindelse med selve konkurrencedeltagelsen, samt til at modtage direkte markedsføring fra virksomheden og samarbejdspartnere, som ligeledes ville modtage oplysningerne. I tillæg hertil kunne man som deltager vælge at oplyse yderligere personoplysninger i et spørgeskema, som virksomheden behandlede med henblik på at tilpasse markedsføring til den enkeltes personlige behov. Oplysningerne i spørgeskemaet blev også videregivet til samarbejdspartnere, dog på baggrund af en interesseafvejning foretaget af virksomheden.

Datatilsynet fandt, at samtykket til konkurrencedeltagelse levede op til reglerne i GDPR. I forhold til videregivelsen af **spørgeskemaoplysningerne** fandt Datatilsynet imidlertid, at oplysningerne var for detaljerede til at kunne videregives efter interesseafvejningsreglen i GDPR artikel 6, stk. 1, litra f, og at oplysningernes videregivelse derfor forudsatte et særskilt samtykke.

Herudover tog Datatilsynet stilling til, hvorvidt SmartResponses opbevaring af personoplysningerne var i strid med GDPR. Virksomheden oplyste, at de opbevarede personoplysningerne indsamlet i forbindelse med konkurrencer for at kunne dokumentere gyldigheden af de indhentede samtykker. Når et samtykke blev trukket tilbage, blev den pågældende persons telefonnummer og e-mailadresse registreret på en »Nej-tak-liste« og opbevaret i en periode på 5 år under henvisning til de danske forældelsesregler.

Datatilsynet kom frem til, at opbevaringen af personoplysningerne i forbindelse med »Nej-tak-listen« var unødvendig og i strid med princippet om dataminimering og princippet om opbevaringsbegrænsning i GDPR artikel 5, stk. 1, litra c og e. Datatilsynet fandt derfor grundlag for at udtale alvorlig kritik henset til, at behandlingen af »Nej-tak-li-

sten« ikke var sket inden for rammerne af principperne i GDPR artikel 5, stk. 1 litra c og e samt interesseafvejningsreglen i GDPR artikel 6, stk. 1, litra f. Datatilsynet meddelte herefter et påbud til SmartResponses om at slette personoplysningerne som fremgik af »Nej-tak-listen«.

Afslutningsvis udtalte Datatilsynet også kritik af virksomhedens måde at iagttage sin oplysningspligt. SmartResponse henviste til sin privatlivspolitik i et link, der fremgik af internetkonkurrencen, hvilket Datatilsynet ikke mente kunne anses som tilstrækkelig iagttagelse af oplysningspligten i GDPR artikel 13, fordi deltagerne ikke modtog fyldestgørende information om den fortsatte opbevaring, efter et samtykke var trukket tilbage.

Det skal bemærkes, at Datatilsynet alene vurderede sagen i henhold til reglerne i GDPR, fordi det efter Tilsynets opfattelse var tvivlsomt, hvorvidt lov nr. 502 af 23. maj 2018 (»den danske databeskyttelseslov«) § 13 om videregivelse af personoplysninger til brug for markedsføring lå inden for det nationale råderum, som GDPR artikel 6, stk. 2-3, tillader.

Læs hele afgørelsen her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/sep/smartresponses-behandling-af-personoplysninger-i-forbindelse-med-udbud-af-internetkonkurrencer>

Det franske datatilsyn udsteder bøde for omfattende indsamling af offentligt tilgængelige billeder

Det franske datatilsyn, CNIL, har i afgørelse SAN-2022-019 af 17. oktober 2022 udstedt en bøde til det amerikanske selskab Clearview AI for selskabets overtrædelse af GDPR.

Clearview AI udbyder en billeddatabase med en tilhørende ansigtsgenkendelsessoftware, der gør det muligt at søge efter personer på baggrund af et billede. Clearview AI har skabt sin billeddatabase med over 20 mia. billeder, ved at scrape

internettet, herunder indhold tilgængeligt på sociale medier før login samt billeder ekstraheret fra videoer offentliggjort på internettet. Størstedelen af billederne er derved indsamlet uden de portrætterede personers kendskab. Med billederne har Clearview AI skabt en »biometrisk template« af den portrætterede persons ansigt, dvs. en digital repræsentation af personens fysiske karaktertræk, som gør det muligt at identificere personen via andre billeder. Virksomheden leverer tjenesten til retshåndhavende myndigheder med henblik på identifikation af potentielle gerningspersoner.

CNIL fandt flere overtrædelser af GDPR, herunder manglende behandlingshjemmel efter GDPR artikel 6. Tilsynet udtalte, at billederne udgør personoplysninger, selvom de er indsamlet på frit tilgængelige medier, hvorfor Clearview AI skulle have sikret en behandlingshjemmel til selve indsamlingen. Allerede fordi indsamlingen af billederne var ulovlig, tog Tilsynet ikke stilling til, hvorvidt Clearview AI's efterfølgende behandling af biometriske data var lovlig efter GDPR artikel 9.

Derudover havde Clearview AI forsømt at overholde de registreredes rettigheder reguleret i GDPR artikel 12, 15 og 17, idet virksomheden ikke havde efterkommet en registrerets anmodning om indsigt i og sletning af personoplysninger om vedkommende. Herudover havde virksomheden også forsømt sin samarbejdspflicht i henhold til GDPR artikel 31, fordi Clearview AI havde negligeret henvendelser fra CNIL i forbindelse med Tilsynets undersøgelser.

Bøden blev fastsat til € 20 mio., hvilket understreger overtrædelsens alvorlige karakter. I tillæg til bøden har Clearview AI fået pålæg om at stoppe al behandling af data om registrerede på fransk territorie, som foretages uden fornøden hjemmel samt at slette sådanne allerede indsamlede data inden for to mæne-

der, med en dagbod på € 100.000 ved forsinkelse.

Afgørelsen er interessant set i lyset af den foreslåede forordning om kunstig intelligens, COM (2021) 206, der pålægger brugere af kunstig intelligens til biometrisk kategorisering, såsom ansigtsgenkendelse, visse gennemsigtighedsforpligtelser, bl.a. ved et krav om, at eksponerede personer skal underrettes om anvendelsen.

Læs afgørelsen her: <https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai>

De nordiske datatilsyn vedtager erklæring med fokus på samarbejde og beskyttelse af oplysninger om børn

Den 13. og 14. oktober har de nordiske datatilsyn, bestående af Danmark, Færøerne, Finland, Island, Norge, Sverige og Åland vedtaget en erklæring, som har til formål at fremme arbejdet med at gøre det digitale miljø mere sikkert og ansvarligt.

Helsinki-erklæringen sætter blandt andet fokus på beskyttelsen af oplysninger om børn, herunder ved at nedsætte en uformel arbejdsgruppe vedrørende børn og online-spil, som skal udveksle oplysninger og på sigt skabe mulighed for fælles vejledning og håndhævelsesforanstaltninger.

Læs pressemeddelelsen her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/okt/nordiske-tilsyn-styrker-samarbejde-om-bla-beskyttelsen-af-boern>

Nyt præsidentielt dekret sætter skub i særlig procedure for tilstrækkelighedsvurdering af tredjelandsoverførsler mellem EU og USA

Den amerikanske præsident Joe Biden udstedte den 7. oktober 2022 et præsidentielt dekret om udveksling af personoplysninger mellem EU og USA.

Dekretet udgør ikke i sig selv et overførselsgrundlag, men kan ses

som et skridt på vejen mod en tilstrækkelighedsvurdering, også kendt under sit engelske navn adequacy decision.

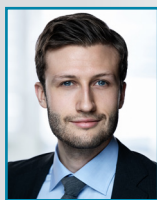
EU-Kommissionen offentliggjorde første udkast til en amerikansk tilstrækkelighedsafgørelse den 13. december 2022, hvori Kommissionen har vurderet, at USA nu har etableret et tilstrækkeligt beskyttelsesniveau og dermed kan leve op til parametre som at indsamling af personoplysninger er proportional og begrænset til det strengt nødvendige og at EU-borgere vil have adgang til effektive retsmidler, herunder en uafhængig klageinstans, såfremt deres personoplysninger behandles af de amerikanske efterretningstjenester.

Udkastet til den nye tilstrækkelighedsafgørelse, EU U.S Data Privacy Framework, er overgivet til Det Europæiske Databeskyttelsesråd, som vil gennemgå materialet og afgive en udtalelse, hvorefter Kommissionen skal søge godkendelse hos en komité bestående af repræsentanter for medlemsstaterne. Endelig er EU-Parlamentet tillagt en indsigelsesret, før tilstrækkelighedsvurderingen kan vedtages endeligt ved en gennemførselsretsakt.

Læs pressemeddelelsen her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/okt/nyt-om-transatlantiske-overfoersler-af-personoplysninger>

Læs om Kommissionens udkast her: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631

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



Wiersholm

Av Line Haukalid, Carl Emil Bull-Berg og Fride Hedin

Deling av bilder av ansatte – krav om samtykke?

En arbeidsgiver vil kunne ha interesse av å dele bilder av sine ansatte i ulike sammenhenger, for eksempel publisering av bilder internt (typisk på selskapets intranett) og publisering i eksterne kanaler. For virksomheter som primært selger de ansattes kompetanse, slik som advokat- og konsultentselskaper, vil slik publisering være av særlig interesse.

Bildedeling reiser flere personvernrettslige problemstillinger. I denne artikkelen vil vi begrense oss til å se nærmere på et av de viktigste spørsmålene, nemlig behandlingsgrunnlag. GDPR oppstiller ulike behandlingsgrunnlag, som alle er likestilte. De mest aktuelle i denne sammenhengen er samtykke og berettiget interesse.

Datatilsynet: Utgangspunktet er samtykke

I Datatilsynets veiledning om deling av bilder fremgår det at man i utgangspunktet må be om samtykke før publisering av bilder hvor en eller flere bestemte personer er hovedmotivet (såkalte portrett-bilder).

Dette standpunktet gjelder tilsynelatende uavhengig av om bildet deles i en lukket gruppe (f.eks. på Facebook) eller om bildet gjøres åpent tilgjengelig på internett (f.eks. på virksomhetens hjemmeside eller via åpne grupper på sosiale medier). Datatilsynet åpner imid-

lertid for at situasjonsbilder (der ingen enkeltpersoner er i hovedfokus) i visse tilfeller kan deles uten samtykke.

Datatilsynet gir ingen nærmere begrunnelse for hvorfor samtykke er utgangspunktet. Årsaken er sannsynligvis forholdet til åndsverkloven § 104, som (med visse unntak) krever samtykke ved offentlig publisering av bilder av personer. Dette underbygges av at Datatilsynet skriver at samtykkekravet gjelder i hele den avbildedes levetid, og 15 år etter utløpet av personens dødsår. Opplysninger om avdøde personer er ikke personopplysninger i Norge, men vernet etter åndsverkloven gjelder i likevel i 15 år etter utløpet av personens dødsår. Når Datatilsynet uttaler seg om samtykkets varighet på denne måten kan det derfor fremstå som at de egentlig gjengir åndsverklovens samtykkeregler, uten nødvendigvis å ta stilling til forholdet disse reglene har til GDPR.

Samtykke er ikke alltid egnet som behandlingsgrunnlag

Selv om et krav om samtykke for publisering av portrett-bilder kan ha gode grunner for seg, er det ikke nødvendigvis gitt at samtykke er det mest egnede behandlingsgrunnlaget i alle tilfeller.

GDPR oppstiller visse krav for at et samtykke skal være gyldig.

Blant annet må samtykket være frivillig, noe som særlig kan skape utfordringer i arbeidsforhold på grunn av den presumtivistiske skjeve maktbalansen mellom arbeidstaker og arbeidsgiver. Selv om arbeidsgiver opplever at den ansatte har fått et fritt valg, er det ikke sikkert at den ansatte føler det slik. Denne usikkerheten tilsier at et annet behandlingsgrunnlag generelt er mer egnet når arbeidsgiver skal behandle personopplysninger om egne ansatte. Samtykke kan videre i verste fall bli en hvilepute, der synspunktet er at så lenge den ansatte har samtykket, er bruken akseptabel. Dette kan, i visse tilfeller, bli et substitutt for den grundige interesseavveiningen som gjøres i en berettiget interessevurdering.

Til tross for dette, kan det virke unaturlig for virksomheter å innhente samtykke etter åndsverkloven, og samtidig basere seg på et annet behandlingsgrunnlag etter GDPR. Det er muligens dette Datatilsynet har tenkt da de lagde veiledningen sin. Vi mener likevel at det finnes viktige nyanser mellom de to regelsettene, som gjør at det ikke alltid er hensiktsmessig å anse dem som sammenfallende.

For det første er det ikke gitt at åndsverklovens krav om samtykke skal tolkes likt som etter GDPR. Forarbeidene til åndsverkloven anerkjenner at § 104 er en person-



Illustrasjonsfoto: Colourbox.com

vernregel. I forbindelse med gjennomføringen av GDPR ble det derfor varslet at Justis- og beredskapsdepartementet skulle gjennomgå bestemmelsen. Så vidt vi vet, er ikke en slik gjennomgang foretatt. Rettstilstanden er derfor noe uklar.

For det andre - dersom samtykkekravet ikke skal tolkes likt - vil samtykkekravet ha ulike rettsvirkninger etter GDPR og etter åndsverkloven. Etter GDPR har for eksempel den avbildede en ubetinget rett til å trekke tilbake sitt samtykke. Praksis etter åndsverkloven tilsier imidlertid at en rett til å trekke tilbake samtykket beror på en mer konkret vurdering.

For det tredje er ikke anvendelsesområdet til GDPR og retten til eget bilde etter åndsverkloven alltid sammenfallende. Åndsverkloven gjelder kun ved offentlig publisering, mens GDPR gjelder så lenge publiseringen ikke er personlige eller familiemessige aktiviteter.

I noen tilfeller er berettiget interesse egnet som behandlingsgrunnlag

Virksomheter vil i mange tilfeller ha berettiget interesse i å publisere bilder av egne ansatte. Et eksempel er bruk av ansattportretter for interne informasjonsformål på virksomhetens intranett eller bruk av ansattportretter i eksterne pitcher. Ofte (men ikke nødvendigvis alltid) vil slik publisering falle utenfor åndsverklovens offentlighetsbegrep, slik at man er utenfor lovens virkeområde. Da vil det kunne være naturlig å belage seg på berettiget interesse som behandlingsgrunnlag, særlig dersom man er i tvil om at et samtykke faktisk vil være frivillig, eller dersom en ubetinget rett til å trekke tilbake samtykket er uhenksmessig.

I tilfeller hvor det ikke foreligger et samtykkekrav etter åndsverkloven, for eksempel for situasjonsbilder, finnes det gode argumenter for at vilkårene etter berettiget interessevurderingen kan være oppfylt. I

disse tilfellene har lovgiver avveid hensynet til den avbildes personvern mot interessen i å publisere bildet, og angitt konkrete tilfeller der samtykke ikke er påkrevd. I slike tilfeller kan arbeidsgiver derfor vurdere om berettiget interesse er et mer egnet behandlingsgrunnlag.

Øvrige plikter

Uavhengig av hvilket behandlingsgrunnlag som brukes, er det viktig at arbeidsgiver gjør de ansatte kjent med publiseringen, og gir påkrevd informasjon om behandlingen av personopplysninger som bildedelingen innebærer. Dersom man velger å belage seg på berettiget interesse, må de ansatte gis mulighet til å protestere på publiseringen, noe som i de fleste tilfeller vil føre til at virksomheten må avstå fra publiseringen.

Line Haukalid (Managing Associate), Carl Emil Bull-Berg (Senior Associate) og Frida Hedin (Senior Associate), advokatfirmaet Wiersholm.



Delphi

Olivia Svedmark og Petri Dahlström

Senaste nyheterna inom svenskt dataskyddsområde

Rapport från IMY om dataskyddsombudens upplevelse av dataskyddsarbetet i praktiken

Integritetsskyddsmyndigheten ("IMY") har publicerat rapporten "Dataskyddsarbetet i praktiken" som syftar till att undersöka vilka förutsättningar som finns för arbetet med dataskyddsfrågor i verksamheter som är skyldiga att ha dataskyddsombud. Rapporten bygger på en enkät som dataskyddsombud från närmare 800 verksamheter har svarat på. Undersökningen visar att mindre än hälften av de dataskyddsombud som deltagit i undersökningen upplever att deras organisationer arbetar kontinuerligt och systematiskt med dataskyddsfrågor. Vidare anser endast hälften av dataskyddsombuden att de får gehör för dataskyddsfrågor från ledningen.

IMY utfärdar sanktionsavgift avseende Region Dalarnas rutiner vid kallelser till vårdbesök

IMY har fattat beslut om att utfärda en administrativ sanktionsavgift mot Region Dalarna på grund av regionens rutiner vid brevutskick av kallelser till vårdbesök. IMY inledde tillsyn mot regionen med anledning av klagomål om att regionen skickar ut kallelser till patientbesök via fysiska brev där vårdinrättningen som besöket avser är fullt synlig i brevet's fönsterkuvert. I sitt beslut konstaterade IMY att ungefär 2 500 kallelser

per år omfattades av överträdelsen, vilket inneburit att känsliga personuppgifter obehörigen har röjts för ett okänt antal personer. IMY ansåg därmed att regionen inte har vidtagit tillräckliga säkerhetsåtgärder för att skydda dessa känsliga personuppgifter mot obehörigt röjande i enlighet med dataskyddsförordningens artikel 32.1. Region Dalarnas överträdelse resulterade i en administrativ sanktionsavgift på 200 000 kr.

IMY meddelar beslut i flera tillsynsärenden gällande osäker e-posthantering

I tre separata tillsynsärenden har IMY utrett incidenter relaterade till verksamhetsutövarers hantering av e-post. I samtliga beslut konstaterade IMY att de berörda verksamhetsutövarna inte har vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en tillräcklig säkerhetsnivå för personuppgifter.

I ett av tillsynsärendena riktar IMY kritik mot Polismyndigheten efter att en granskning visat att e-postmeddelanden innehållande integritetskänsliga personuppgifter om bland annat misstänkta personer och brottsoffer har skickats till obehöriga personer av misstag. Anställda vid Polismyndigheten har misstagsvis stavat fel på "@polisen.se" när mottagaradressen angivits, vilket har medfört att e-postmeddelanden har skickats till en utomstå-

ende person som registrerat domännamn med snarlika stavningar. IMY anser därför att Polismyndigheten inte har vidtagit lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter i enlighet med 3 kap. 2 och 8 §§ brottsdatalogen (2018:1177).

Vidare har IMY i två separata beslut utfärdat en reprimand till försäkringsbolaget If Skadeförsäkring AB ("If") och sanktionsavgifter mot Region Uppsala. Tillsynen avsåg i båda fallen hantering och kryptering av e-post innehållande känsliga personuppgifter. If hade vid ett tillfälle inte säkerställt att ett meddelande varit krypterat under hela dess transport till mottagaren, vilket inneburit en risk för att obehöriga kunde ha tagit del av e-postmeddelandet i klartext. Region Uppsala hade vid utskick av e-post till mottagare i och utanför Sverige inte säkerställt att meddelandehållet var krypterat. IMY konstaterade således att varken If eller Region Uppsala har vidtagit lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter enligt artikel 32 i dataskyddsförordningen.

Olivia Svedmark och Petri Dahlström är Associates vid Advokatfirman Delphi, Stockholm.



Gorrissen Federspiel

Tue Goldschmieding

Onlinemarkedspladsers »brug« af varemærker ved udbud af varer

Den 22. december 2022 afsagde Domstolen dom i de forenede sager C-148/21 og C-184/21 mellem Christian Louboutin (»Louboutin«) og Amazon Europe Core Sàrl, Amazon EU Sàrl og Amazon Services Europe Sàrl, Amazon.com Inc. og Amazon Services LLC (samlet »Amazon«). Sagen var anlagt ved kredsdomstolen i Luxembourg og den fransksprogede ret i Bruxelles, Belgien. Omdrejningspunktet i sagen var et præjudicielt spørgsmål angående fortolkning af artikel 9, stk. 2, i Europa-Parlamentets og Rådets forordning (EU) 2017/1001 af 14. juni 2017 om EU-varemærker (»varemærkeforordningen«).

Varemærkeforordningens artikel 9, stk. 2, hjemler rettighedshaverens forbudsret over for tredjemands brug af rettighedshaverens varemærke. Spørgsmålet i sagen var navnlig, hvorvidt platformen Amazon, udover dennes egne salgstilbud, kunne anses for at »gøre brug« af et tegn, som var identisk med Louboutins EU-varemærke. Sagens genstand var en række varer, som eksterne sælgere uden samtykke fra Louboutin udbød på Amazons platform med identiske tegn.

Vurderingen af, hvorvidt platformen Amazon »brugte« Louboutins varemærke gik blandt andet på, hvorvidt en almindeligt oplyst og rimeligt opmærksom bruger af Amazon kunne tænkes at skabe en forbindelse mellem Amazons tjenesteydelser og Louboutins varemær-

ke. Hertil om denne bruger ville få opfattelsen af, at det var Amazon, som i eget navn og for egen regning markedsførte den vare, for hvilken der blev gjort brug af Louboutins varemærke.

Domstolen fremhævede, at Amazon præsenterede egne og eksterne sælgeres reklamer på en ensartet måde, herunder ved anvendelse af Amazons logo. Ifølge Domstolen gjorde dette det vanskeligt for brugeren at foretage en klar sondring mellem varerne udbudt af eksterne og varerne udbudt af Amazon. Med afsæt heri vurderede Domstolen, at den ensartede præsentation kunne skabe en forbindelse i brugernes øjne mellem Louboutins varemærke og Amazons tjenesteydelser.

Domstolen fremhævede desuden, at Amazons udbud af diverse tjenesteydelser vedrørende behandling af brugernes spørgsmål, oplagring, forsendelse og administration af returnering af varer, kunne give brugeren det indtryk, at varerne blev markedsført i Amazons navn og for Amazons regning.

Henset til disse betragtninger, fastslog Domstolen, at Amazon godt kunne anses for at »gøre brug« af Louboutins varemærke i varemærkeforordningens forstand, når eksterne sælgere udbød salgsannoncer med varer identiske med Louboutins varemærke, uden Louboutins samtykke.

Læs hele dommen her: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=268788&pageIndex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=91694>

Springende kat som en del af logo var ikke i strid med PUMA's varemærkeret

Den Europæiske Unions Ret (»Retten«) har af to omgange afsagt dom i sagen mellem PUMA SE (»PUMA«) og EUIPO. Begge sager handlede om, hvorvidt CMS Costruzione Macchine Speciali SpA's (»CMS«) ansøgning den 21. december 2012, om varemærkeregistriering af et logo, krænkede PUMA's allerede registrerede varemærkerettigheder. Derudover angik tvisten, om der var begået sagsbehandlingsfejl i forbindelse med vurderingen af PUMA's varemærkerettighed. EUIPO's Appellkammer havde tidligere truffet afgørelse til fordel for CMS, og PUMA søgte derfor Rettens annullation af denne afgørelse.

Den første afgørelse (T-711/20) blev afsagt den 5. oktober 2022, og blev vurderet efter forordning 207/2009 (EF) af 26. februar 2009 om EF-varemærker (»den gamle varemærkeforordning«), da varemærkeansøgningen blev indgivet i 2012, hvilket er før Europa-Parlamentets og Rådets forordning (EU) 2017/1001 af 14. juni 2017 om EU-varemærker (»varemærkeforordningen«) ikrafttrædelse.

Her fandt Retten, at bogstaverne »CMS« i det ansøgte varemærke udgjorde den dominante del af logoet, og den springende kat var således af sekundær betydning. Retten tog individuelt stilling til PUMA's tre varemærker og fandt for alle tre tilfælde, at der forelå ingen eller ringe grad af visuel, fonetisk og konceptuel sammenlignelighed mellem varemærkerne. CMS' logo krænkede

således ikke PUMA's registrerede varemærke.

Retten annullerede dog EUIPO's Appellkammers afgørelse for så vidt angik to ud af PUMA's tre varemærker, idet Retten vurderede, at EUIPO's Appellkammer fejlagtigt ikke havde inddraget alle relevante oplysninger i forbindelse med vurderingen af disse to varemærker.

Retten skulle derfor på ny tage stilling til disse to varemærker i sagen T-4/22, der blev afgjort den 21. december 2022.

Retten fandt, at der ikke var fejl i EUIPO's Appellkammers behandling, hvad angår inddragelsen af det ældre varemærkes stærke renommé i bedømmelsen af, om der forelå forvekslingsrisiko mellem varemærkerne. Det kunne endvidere ikke anses for en fejl, at EUIPO's Appellkammer havde lagt vægt på uligheden af de varer, som sagens parter sælger.

Samlet fastslog Retten, at EUIPO's Appellkammer med rette havde fundet, at der ikke vil kunne skabes en sammenhæng mellem de omtvistede varemærker. PUMA's varemærke blev således ikke krænkede ved, at EUIPO tillod registrering af CMS' varemærke.

Læs dommen af 5. oktober 2022 her: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=266804&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1158277>

Læs dommen af 21. december 2022 her: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=268760&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=91694>

Indehaveren af varemærker på lægemidler kan modsætte sig parallelimportørers ompakning

EU-Domstolen afsagde den 17. november 2022 dom i sag C-224/20 mellem en række lægemiddelproducenter og varemærkeindehavere for lægemidler som sagsøger og en række sagsøgte, der alle driver virksom-



Illustrationsfoto: Colourbox.com

hed med parallelimport af lægemidlerne til Danmark.

Dommen var foranlediget af en præjudiciel forelæggelse fra Sø- og Handelsretten og vedrørte syv tvister angående sagsøgte parallelimport og ompakning af lægemidler. Lægemidlerne var bragt på markedet i andre medlemsstater og søgtes nu solgt i Danmark.

Sagen vedrørte to typer af ompakning. For det første, ompakkede sagsøgte de importerede lægemidler i ny ydre emballage, hvorpå sagsøgte placerede sagsøgernes respektive varemærker. For det andet, ompakkede sagsøgte i ny ydre emballage,

hvorpå sagsøgernes varemærker ikke genanbringes, men hvor de i stedet placerede et nyt produktnavn, inden lægemidlet blev markedsført i Danmark.

De præjudicielle spørgsmål for EU-Domstolen angik, artikel 15, stk. 2, i Europa-Parlamentets og Rådets forordning (EU) 2017/1001 af 14. juni 2017 om EU-varemærker («varemærkeforordningen»), der vedrører muligheden for under særlige forhold at forbyde brugen af et EU-varemærke, som denne selv har markedsført. Spørgsmålet i sagen var, om varemærkeforordningens artikel 15, stk. 2, skal fortolkes såle-

des, at producenter af lægemidler kan modsætte sig parallelimportørers forskellige ompakninger af produkterne.

EU-Domstolen fandt, at varemærkeindehaveren under visse omstændigheder har ret til at modsætte sig, at en parallelimportør markedsfører et ompakket lægemiddel i en ny, ydre emballage. Det gælder, når udskiftningen efterlader tydelige spor af, at emballagen har været brudt, hvis dette skaber en stærk modstand hos en betydelig del af forbrugerne. Domstolen fandt endvidere, at direktiv 2001/83 af 6. november 2001 om humanmedicinske lægemidler hindrer, at en medlemsstat bestemmer, hvorvidt parallelimporterede lægemidler principielt skal ompakkes i en ny ydre emballage.

Læs hele dommen her: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=268023&page-Index=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=91694>

Louis Vuittons ternede mønster havde ikke særpræg og havde ikke opnået ibrugtagning på hele området for EU

Den 19. oktober 2022 afsagde Den Europæiske Unions Ret (»Retten«) dom i sag T-275/21, mellem Louis Vuitton Malletier (»Louis Vuitton«) og EUIPO. Retten skulle tage stilling til, hvorvidt en begæring om ugyldighed af Louis Vuittons varemærke skulle opretholdes. Det centrale spørgsmål i sagen var, om varemærket efter registreringen havde fået fornødent særpræg for de varer eller tjenesteydelser, for hvilke det var registreret, jf. Europa-Parlamentets og Rådets forordning (EU) 2017/1001 af 14. juni 2017 om EU-varemærker (»varemærkeforordningen«) artikel 7, stk. 3 og 59, stk. 2. Retten besluttede, at Louis Vuitton ikke havde løftet bevisbyrden for, at varemærket havde opnået særpræg ved brug.

Indehaveren af et varemærke, der ikke har et selvstændigt særpræg, skal påvise særpræg ved brug

af varemærket. Derudover skal det opnåede særpræg påvises at være opnået på hele EU-området og ikke kun på en væsentlig del eller størstedelen af området.

Det omtvistede varemærke havde ikke et selvstændigt særpræg, idet det bestod af et ternet mønster. Derfor var det nødvendigt for at opnå varemærkeretlig beskyttelse, at der kunne statuere ibrugtagningen på hele området for EU.

Retten tog i sin vurdering udgangspunkt i en række lande, hvor Louis Vuitton ikke havde etableret fysiske butikker: Bulgarien, Estland, Letland, Litauen, Slovakiet og Slovenien.

Louis Vuitton argumenterede for, at der var opnået særpræg ved brug i de ovenstående lande, eftersom varemærket er et velkendt brand inden for luksussegmentet. Louis Vuitton fremlagde i den forbindelse en række beviser, herunder oplysninger om online salg, markedsføringsstrategier og ekspertudtalelser, der skulle påvise ibrugtagningen i de fornævnte lande.

Retten stadfæstede, for så vidt angår alle de respektive lande på nær Estland, EUIPO's Appellkammer afgørelse om, at der ikke forelå ibrugtagning af varemærket, idet bevisbyrden for ibrugtagning ikke var løftet. For så vidt angår Estland, kom Retten efter en samlet vurdering frem til, at EUIPO's Appellkammer havde foretaget en fejlbedømmelse i forhold til ugyldighed af varemærket i Estland.

Retten lagde særligt vægt på, at det ikke var bevist, at forbrugere fra de pågældende medlemsstater havde været udsat for det anfægtede varemærke i tilstrækkelig grad til at anse varemærket for taget i brug.

Det omtvistede varemærke havde således ikke opnået fornødent særpræg ved brug i alle EU's medlemsstater, hvorfor Louis Vuittons indsigelse mod begæringen om ugyldighed blev afvist.

Læs hele dommen her: <https://curia.europa.eu/juris/document/docu->

[ment.jsf?sessionid=0F-06772B16809A01AC4140968BFC-2FAC?text=&docid=267375&page-Index=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=10947](https://curia.europa.eu/juris/sessionid=0F-06772B16809A01AC4140968BFC-2FAC?text=&docid=267375&page-Index=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=10947)

Ældre varemærke kunne ikke tillægges betydning, da overgangsperioden for Storbritanniens udtræden af EU var udløbet

Den 12. oktober 2022 afsagde Den Europæiske Unions Ret (»Retten«) dom i sag T-222/21, mellem Shopify Inc. (»Shopify«) og EUIPO. Sagen vedrørte, hvorvidt Shoppi Ltd.'s (»Shoppik«) ansøgning om registrering af et figurvaremærke for et logo med skriften »Shoppik« krænkede Shopifys registrerede varemærke »Shopify«.

Retten fandt for det første, at varemærket »Shopify« ikke havde fornødent særpræg, eftersom ordet »shop« udelukkende er af beskrivende karakter, ligesom endelsen »ify« er af ringe betydning.

Det blev herefter undersøgt, om varemærket ved indarbejdelse og ibrugtagning i Storbritannien havde opnået særpræg. Storbritannien udtrådte af EU i henhold til TEU artikel 50 den 1. februar 2020 med en overgangsperiode indtil den 31. december 2020. Retten fandt, at vurderingen af ibrugtagning af varemærket i det geografiske område skal kunne påberåbes på det tidspunkt, hvor EUIPO træffer afgørelse om begæringen om ugyldighed. EUIPO's Appellkammer traf afgørelse i sagen den 18. februar 2021 og dermed efter udløbet af overgangsperioden. Følgelig var EUIPO's Appellkammer ikke forpligtet til at tage hensyn til brugen af et andet ældre varemærke i Storbritannien.

Endelig kom Retten frem til, at der ikke var risiko for forveksling mellem de to varemærker, da der både var en ringe grad af visuel sammenlignelighed samt alene en gennemsnitlig grad af fonetisk og konceptuel sammenlignelighed.

Læs hele dommen her: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=267069&page-Index=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1158277>

Sorte og hvide linjer kunne ikke varemærkerregistreres på grund af manglende særpræg

Den Europæiske Unions Ret (»Retten«) afsagde den 5. oktober 2022 dom i sag T-502/21, mellem Philip Morris Products SA (»Philip Morris«) og EUIPO.

Twisten angik en anmodning om varemærkerregistrering af en illustration bestående af sorte og hvide linjer, der skabte en kontrastvirkning. Varemærkerregistreringen vedrørte varer i Nice kvalifikationsklasse 34 om tobaksvarer.

Philip Morris nedlagde påstand om annullation af EUIPO's afgørelse i sag R 78/2021-5 truffet den 26. maj 2021, hvor sagens varemærke blev nægtet registrering. Baggrunden herfor var, at varemærket ikke havde særpræg, som omhandlet i artikel 7, stk. 1, litra b, i Europa-Parlamentets og Rådets forordning (EU) 2017/1001 af 14. juni 2017 om EU-varemærker (»varemærkeforordningen«).

Philip Morris bestred EUIPO's argumenter og gjorde i sagen gældende, at varemærket på grund af sin originalitet og genkendelighed havde særpræg. EUIPO gjorde omvendt gældende, at varemærket, henset til sin enkelhed, ikke præsenterede aspekter eller kommunikerede et budskab, som ville blive lært udenad af den relevante kundekreds. EUIPO lagde endvidere vægt på, at de sorte linjer ikke egnede sig til at fremhæve et kommercielt budskab, men at disse nærmere ville blive opfattet som dekoration.

Retten stadfæstede følgelig EUIPO's afgørelse om at afvise varemærkerregistreringen.

Læs hele dommen her: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=266813&page-Index=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1158277>

[Index=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1139759](https://www.domstol.dk/media/njcf-b4qv/bs-24168-2022-olr.pdf)

Fremtidige, uidentificerede krænkelse kan ikke danne grundlag for midlertidigt forbud

Østre Landsret afsagde den 9. november 2022 kendelse i sag BS-24168/2022-OLR, hvori retten afviste at nedlægge et midlertidigt forbud, navnlig under henvisning til, at forbuddet var formuleret så bredt, at det ikke var muligt at identificere en konkret og aktuel krænkelse, som der blev søgt beskyttelse mod.

Skechers U.S.A, INC. II (»Skechers«) nedlagde påstand om midlertidige forbud over for en række teleselskaber efter lovbekendtgørelse nr. 1655 af 25. december 2022 (»den danske retsplejelov«) § 413. Teleselskaberne viste og gav adgang til en række internetdomæner, som Skechers mente krænkede deres varemærkeret. Det indbefattede efter påstanden ethvert fremtidigt domæne, som Skechers underrettede teleselskaberne om, og som anvendte dennes varemærkeret på en måde som angivet i sagens bilag.

Østre Landsret fastslog, i tråd med Sø- og Handelsretten, at denne adgang til at nedlægge forbud over for en uidentificerbar, fremtidig tredjemands brug af varemærkeret, ikke opfyldte kravet om, at modpartens adfærd skulle nødvendiggøre forbuddet, idet en sådan adfærd ikke kunne konstateres på tidspunktet for afgørelsen. Hertil fremhævede retten, under henvisning til sag C-337/95, at det ikke var givet, at den angivne adfærd fra tredjemænd altid ville være uretmæssig, idet denne dom indrømmer en ret for forhandlere til en vis loyal brug af et varemærke.

Læs landsrettens kendelse her: <https://www.domstol.dk/media/njcf-b4qv/bs-24168-2022-olr.pdf>

Læs landsrettens pressemeddelelse her: <https://www.domstol.dk/oestrelandsret/>

[aktuelt/2022/11/ikke-forbud-mod-fremtidige-og-identificerede-krænkelser/](https://www.domstol.dk/media/njcf-b4qv/bs-24168-2022-olr.pdf)

Anvendelse af konkurrents varemærker i Google AdWords var i strid med varemærkeloven og markedsføringsloven

Sø- og Handelsretten afsagde den 2. november 2022 dom i sagerne BS-37234/2022-SHR og BS-2608/2022-SHR mellem JABS Group A/S og Sparvinduer A/S (»JABS/Sparvinduer«) over for Klarvinduer ApS og Klarvinduer OÜ (fælles »Klarvinduer«).

Sagerne handlede om, hvorvidt Klarvinduers anvendelse af varemærker tilhørende JABS/Sparvinduer som søgeord på Google Ads krænkede de pågældende varemærkerrettigheder, herunder indehaverens varemærkeretlige eneret efter lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) § 4, stk. 1. Yderligere gjorde JABS/Sparvinduer gældende, at Klarvinduer havde overtrådt lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 3, stk. 1, om god markedsføringsskik og § 22 om forretningskendetegn.

JABS/Sparvinduers påstod, at Klarvinduer havde brugt førstnævntes registrerede varemærker som Google AdWords i forbindelse med egen markedsføring af tilsvarende produkter. Ved brug af Google AdWords betalte Klarvinduer for at få sine annoncer vist i forbindelse med en Google-søgning på de pågældende varemærker.

Sø- og Handelsretten fandt det indledningsvist ikke godtgjort, at Klarvinduer ApS havde været involveret i den omstridte brug af Google AdWords, hvorfor denne blev frifundet.

For så vidt angår Klarvinduer OÜ's brug af Google AdWords, indledte Sø- og Handelsretten med henvisning til EU-Domstolens dom i de forenede sager C-236/08 og C-238/08 at fastslå, at det ikke i sig

selv er retsstridigt at anvende en anden erhvervsdrivendes varemærke som Google AdWord. Retten fandt følgelig, at der ikke var tilstrækkeligt grundlag for at nedlægge et generelt forbud herfor.

Spørgsmålet for Sø- og Handelsretten var herefter, om anvendelsen af Sparvinduer ApS' varemærke havde gjort det vanskeligt for gennemsnitsforbrugeren at gøre sig bekendt med, hvilken virksomhed annoncerne hidrørte fra. Ud fra en konkret vurdering fandt Sø- og Handelsretten, at det ved visse af Klarvinduer OÜ's annoncer ikke var muligt for en gennemsnitlig internetbruger at gøre sig bekendt med, om annoncerne produkter hidrørte fra JABS/Sparvinduer eller Klarvinduer OÜ. Sø- og Handelsretten fandt derfor, at Klarvinduer OÜ havde overtrådt den danske varemærkelovs § 4 samt den danske markedsføringslovs § 3 og § 22.

Endelig udtalte Sø- og Handelsretten, at det som udgangspunkt ikke er i strid med hverken god markedsføringsskik eller varemærkeretten, at en erhvervsdrivende afholder sig fra at registrere sine konkurrenters varemærker som negative søgeord. Et negativt søgeord indebærer, at en søgning ved bestemte ord eller sætninger forhindrer visning af den erhvervsdrivendes annoncer.

Læs hele dommen her: [https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-37234-2021-SHR_m.fl._\(sambehandling\).pdf](https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-37234-2021-SHR_m.fl._(sambehandling).pdf)

Forbrugerombudsmanden indskærper reglerne om markedsføring med bæredygtighedsudsagn over for fem virksomheder

Den danske Forbrugerombudsmand har den 16. december 2022 udstedt pressemeddelelse om, at hun har indskærpet reglerne om

markedsføring ved benyttelse af bæredygtighedsudsagn over for fem virksomheder. Indskærpelsen sker i medfør af lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 5 og § 13 om vildledende markedsføring.

Indskærpelsen sker på baggrund af virksomhedernes markedsføring af en række forskelligartede produkter, herunder bl.a. lamper, tekstil, legetøj og drikkeflasker i rustfrit stål. Virksomhederne havde på forskellig vis, ved betegnelser som indebar varianter af ordet »bæredygtigt«, markedsført deres produkter som særligt bæredygtige.

Det viste sig imidlertid, at udsagnene enten ikke kunne dokumenteres eller ikke var tilstrækkeligt underbyggede for at kunne markedsføres som bæredygtige. Forbrugerombudsmanden udtalte i den forbindelse, at virksomheder skal kunne markedsføre konkrete miljømæssige fordele ved deres produkter, men at anvendelsen af mere generelle udsagn uden dokumentation herfor, udgør vildledende markedsføring.

Yderligere udtalte Forbrugerombudsmanden, at hun generelt fraråder virksomheder at markedsføre deres produkter som bæredygtige, da et sådant udsagn forudsætter, at produktionen af produktet ikke har forringet miljøet eller tæret på klodens ressourcer til skade for de kommende generationer. Dette kriterium er ifølge Forbrugerombudsmanden sjældent opfyldt i praksis.

Endelig henviste Forbrugerombudsmanden til sin kvikguide til virksomheder om miljømarkedsføring af 2021, der vejleder om reglerne for anvendelse af miljømæssige udsagn i virksomheders markedsføring.

Læs pressemeddelelsen her: <https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2022/virksomheder-kald>

te-produkter-baeredygtige-uden-at-kunne-dokumentere-det/

Læs kvikguiden af 2021 her: <https://www.forbrugerombudsmanden.dk/media/56731/kvikguide-om-miljoe-markedsfoering.pdf>

Influent skal betale bøde på 40.000 kr. for skjult reklame

Den danske Forbrugerombudsmand udstedte den 5. oktober 2022 pressemeddelelse om, at Retten i Lyngby har idømt en influent en bøde på 40.000 kr. for at overtræde forbuddet mod skjult reklame i lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 6, stk. 4.

Bøden blev pålagt som følge af influentens mangelfulde markering på det sociale medie Instagram af, at der var tale om reklame for virksomheder og produkter. Virksomhederne var alene »tagget« på de pågældende opslag, hvilket ifølge Retten i Lyngby udgjorde promovering af de pågældende virksomheder.

Influenten havde opnået en økonomisk gevinst, idet hun bl.a. havde fået en tandbehandling, en cykel, en skitur, adgang til Disneyland, et hotelophold og børnesko. Forbrugerombudsmanden udtalte, at det skal fremgå meget klart, såfremt der er tale om reklame og influent har modtaget nogen form for vederlag, inden de viser et produkt på de sociale medier. Det gælder også i tilfælde, hvor influent modtager gratis produkter.

Læs pressemeddelelsen her: <https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2022/influent-skal-betale-bode-pa-40-000-kroner-for-skejult-reklame/>

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



Bird & Bird

Nathalie Sjölander, Associate,
& Max Stenberg, Trainee

Intermistiskt förbud mot att marknadsföra en dräkt benämnd Lussekatt, PMÖ 14536-22

Målet vid Patent- och marknadsöverdomstolen (PMÖD) från den 19 december 2022 gällde giltigheten av ett intermistiskt förbud som meddelats av Patent- och marknadsdomstolen (PMD). Beslutet från PMD innebar ett förbud att marknadsföra en dräkt som efterliknade det traditionella bakverket lussekatt. Käranden gjorde gällande att dräkten utgjorde ett intrång i deras registrerade gemenskapsformgivning, som även det efterliknade bakverket. Svaranden menade att gemenskapsformgivningen var ogiltig, att det inte förelåg sannolika skäl för intrång och att ett intermistiskt förbud inte är proportionerligt. PMD ansåg att sannolika skäl förelåg på sådant sätt att dräkten utgjorde ett intrång och meddelade därför det intermistiska förbudet.

Svaranden överklagade målet till PMÖD. Domstolen konstaterade inledningsvis att skyddsomfånget omfattar varje formgivning som inte ger en kunnig användare ett annat helhetsintryck. Domstolen fastställde att gemenskapsformgivningen i det aktuella fallet får anses ha låg särprägel, då den "(...) i princip utformats för att helt efterlikna det traditionella bakverk som kallas bl.a. lussekatt eller julgal". Skyddsomfånget ansågs därför vara snävt. Därefter konstaterade domstolen att dräkternas skillnader, däribland deras "(...) grundläggande form och skärning, samt olika detaljer i utformningen", ger en kunnig användare ett annat helhetsintryck. Därmed kunde det inte anses finnas sannolika skäl för intrång



Illustrationsfoto: Colourbox.com

i den registrerade gemenskapsformgivningen. PMÖD upphävde därav det intermistiska beslutet.

Se avgörandet i sin helhet:

<https://www.domstol.se/globalassets/filer/domstol/patentochmarknadsoverdomstolen/avgoranden/2022/pmo-14536-22.pdf>

Genkärsmål utifrån EU:s varumärkesförordning, PMÖ 7917-22

Patent- och marknadsöverdomstolen (PMÖD) meddelade den 5 december 2022 sitt avgörande avseende en processuellfråga utifrån Europaparlamentets och Rådets förordning 2017/1001 av den 14 juni 2017 om EU-varumärken (EU:s varumärkesförordning). Ett svenskt företag gjorde vid Patent- och marknadsdomstolen (PMD) gällande att två tyska företag hade gjort intrång i ett antal av det svenska företagets nationella varumärken samt EU-varumärken. De tyska företagen väckte då en ogiltighetstalan gentemot det svenska företagets

EU-varumärken. Det svenska företaget valde då att återkalla sin talan i den del som avsåg EU-varumärkena och yrkade att de tyska företagens talan skulle avvisas, vilket PMD avslag. Beslutet överklagades och frågan i PMÖD var huruvida de tyska företagens talan skulle avvisas.

PMÖD fastställde inledningsvis genom hänvisning till C-256/21 att väckt talan om ogiltighet vid ett intrångsmål ska anses vara ett genkärsmål i enlighet med artikel 124 och 128 i EU:s varumärkesförordning. Enligt EU-domstolens avgörande ska genkärsmål ses som en utvidgning av föremålet för tvisten som är separat och obundet från huvudyrkandet. Trots kopplingen till huvudsaken ska genkärålet därmed ses som en självständig talan. Nationella domstolar fortsätter därför vara behöriga att pröva genkärålet även när huvudkärålet återkallas.

I det aktuella fallet fastslog PMÖD att de tyska företagens talan skulle anses vara ett genkärsmål i enlighet med EU:s varumärkesför-

ordning. Domstolen konstaterade att PMD fortsätter vara behörig att pröva giltigheten av EU-varumärkena, oavsett de processuella dispositioner som det svenska företaget gjort. PMÖD avslog därför det svenska företags överklagande.

Se avgörandet i dess helhet här:

<https://www.domstol.se/patent--och-marknadsoverdomstolen/patent--och-marknadsoverdomstolens-angoranden/2022/121628/>

Angivelse av intervall i patentkravet samt intrång genom ekvivalens, PMT 5311-19

Målet avser en talan om patentintrång som avgjordes av Patent- och marknadsöverdomstolen (PMÖD) den 20 december 2022. Ett italienskt företag framförde i målet att ett svenskt företag begått patentintrång genom att producera provtagningspinnar som var identiska med det italienska företags provtagningspinnar. Den centrala frågan i målet var hur patentkravet angående s.k. fibervärden ska tolkas.

Patentkravet anger att fibervärdet ska vara mellan 1,7 och 3,3 i skalan Dtex. Det var tvistigt huruvida dessa värden avsåg ett nominellt värde eller de faktiska värdena i den producerade produkten. Det italienska företaget presenterade bevis-

ning i form av ett expertutlåtande där det angavs att värdena hänförs till standardvärden som fibrerna tillverkas med. Vid produktionen av fibrerna finns även vedertagna avvikelsetoleranser om ca 10%. Det lades även fram bevisning i form av material från fibertillverkare som visade standardvärden för åtminstone vissa fibrer.

Utifrån en samlad bedömning fann PMÖD att det saknades stöd i själva patentkravet för att fibervärdet skulle utgöra nominella standardvärden. I stället framhöll domstolen att patentkravet hänförs till faktiska värden.

I frågan om vilka fibervärden det svenska företags provtagningspinnar innehöll så presenterade båda parterna varsin utredning. Fibrernas medelvärde utifrån parternas respektive utredningar skiljde sig markant från varandra. Eftersom bevisbördan i detta hänseende ålåg det italienska företaget, samt att det inte fanns något som gav stöd för att någon av utredningarna var mer tillförlitlig och rättvisande än den andra, menade PMÖD att det inte gick att dra några säkra slutsatser om värdet på de testade fibrerna i det svenska företags produkter. Det italienska företaget ansågs därför inte ha visat att värdet på fibrer-

na låg inom det i patentkravet angivna intervallet. Därav ansåg PMÖD att ingen av de påstådda intrångsprodukterna uppfyllde det i patentkravet angivna särdraget.

Det italienska företaget hade i andra hand gjort gällande intrång genom ekvivalens. I den frågan uttalade PMÖD att uppfinningen avser en lösning som ligger nära på prioriteringsdagen känd teknik, vilken måste anses vara av enkelt slag. Dessutom hade det i patentkravet införda särdraget som hänförs till fibervärden förts in som en avgränsning i förhållande till känd teknik. Utrymmet för skydd genom ekvivalensstolkning angav PMÖD därför vara mycket begränsat. Domstolen kom därefter till slutsatsen att intrång inte heller förelåg på grund av ekvivalens. Till följd av dessa slutsatser saknades skäl för domstolen att ta ställning till andra delar av patentkravet. Det italienska företags talan ogillades.

Se avgörandet i dess helhet här:

<https://www.domstol.se/patent--och-marknadsoverdomstolen/patent--och-marknadsoverdomstolens-angoranden/2022/119694/>

Nathalie Sjölander, Associate, & Max Stenberg, Trainee i Advokatfirman Bird&Bird



simonsen vogtviig

Hedda Baumann Heier og Camilla Hagelien

Forslag til ny lov om beskyttelse av norsk forsvarsteknologi og sikkerhetsgraderte patenter.

Forsvarsdepartementet har fremlagt forslag til ny lov om beskyttelse av norsk forsvarsteknologi og sikkerhetsgraderte patenter. Forslaget er sendt på høring med høringsfrist 13. april 2023. Den foreslåtte loven skal erstatte gjeldende lov av 26. juni 1953 om oppfinnelser av betydning for rikets forsvar, og vil ha en bredere nedslagsfelt. Den skal kunne omfatte alle varer, tjenester og teknologi som brukes til forsvarsmål – uavhengig av hva som allerede er tilgjengelig på markedet og teknologiens utviklingsnivå. Hensikten er å redusere sårbarheter og tilrettelegge for nasjonale kontroll med sentrale innsatsfaktorer for å ivareta Forsvarets operative evne.

Loven vil komme til anvendelse på teknologi som departementet etter vedtak mener har vesentlig betydning for Forsvarets operative evne, og som derfor er beskyttelsesverdig. Hvorvidt teknologien anses for å ha vesentlig betydning, beror på en konkret helhetsvurdering, hvor det blant annet kan ses hen til hvilke konsekvenser tap av teknologien vil ha for operativ evne, om den er tilpasset norske forhold, om den er allment tilgjengelig på markedet og hvilken betydning teknologien har for beskyttelse av sensitiv informasjon.

Et vedtak om at en teknologi er beskyttelsesverdig innebærer blant annet at det kreves tillatelse fra departementet før teknologien kan deles. Videre vil departementet kunne pålegge eller forby bruk, utvikling eller produksjon av teknologien



Illustrasjonsfoto: Colourbox.com

dersom dette er nødvendig for å ivareta Forsvarets operative evne. Departementet vil også kunne ekspropriere og sikre seg rett til å utnytte en beskyttelsesverdig forsvarsteknologi dersom krav om tillatelse eller pålegg om forbud ikke gir tilstrekkelig kontroll.

Departementet legger opp til at et vedtak om ekspropriasjon eller rett til utnyttelse vil kunne gi rett til erstatning, mens rett til erstatning for øvrige vedtak vil avhenge av en konkret helhetsvurdering der utgangspunktet vil være at det ikke er en rett til erstatning.

Reglene om hemmelige patenter foreslås i all hovedsak videreført fra gjeldende lov.

Få tilgang til høringens dokumenter her: <https://www.regjeringen.no/no/no/dokumenter/boring-ny-lov-ombeskyttelse-av-norske-forsvarsteknologi-og-sikkerhetsgraderte-patenter/id2959220/>

Avgjørelse fra Høyesterett i Kystgjerde-saken (HR-2022-2222-A)

Høyesterett avsa den 16. november 2022 dom i saken mellom Norgesgjerde AS og Vindex AS (samlet «rettighetshaverne») og Kystgjerdet AS («Kystgjerdet»). Saken gjaldt utmåling av vederlag og/eller erstatning for varemerkekrenkelse.

Utgangspunktet for tvisten var at Kystgjerdet markedsførte sine PVC-gjerder gjennom annonsetjenester og kjøpte søkeord som sikret at Kystgjerdet ble prioritert i trefflisten. Kystgjerdet hadde kjøpt VINDEKX og NORGESGJERDE som søkeord i annonsene, som er varemerker tilhørende rettighetshaverne. Dette

innebar at når forbrukere søkte etter PVC-gjerder fra Vindex eller Norgesgjerde, ville Kystgjerdet komme øverst. Dette er ikke nødvendigvis ulovlig jf. HR-2021-2479 avsnitt 66, men i denne saken hadde lagmannsretten rettskraftig avgjort at varemerkene var brukt på en slik måte at det utgjorde en krenkelse. Saken for Høyesterett var begrenset til hvilken kompensasjon rettighetshaverne hadde krav på for krenkelsen.

Rettighetshaverne hadde krevd erstatning etter varemerkeloven § 58 første ledd bokstav b. Høyesterett mente at det ikke var grunnlag for å utmåle erstatning for fortjenestetap eller omdømmetap. Det var heller ikke adgang til å kreve vinningsvederlag etter § 58 første ledd bokstav c. Den gjenstående utmålingshjemmelen var da retten til å kreve rimelig lisensavgift etter § 58 første ledd bokstav a.

Etter en gjennomgang av ulike utmålingsmetoder, forkastet Høyesterett lagmannsrettens beregningsmodell, da det ikke fantes økono-

miske faktorer som ga et rimelig utgangspunkt for utregningen. Som konsekvens uttalte førstvoterende at «lisensavgiftene må utmåles som engangsbeløp etter et skjønn. Jeg har, slik saken ligger an, ikke grunnlag for å oppstille generelle prinsipper for hvordan en rimelig lisensavgift skal beregnes ved ulovlig bruk av andres varemerke i annonsetekster, når det skjer ved kjøp av konkurrenters varemerke som søkeord».

Høyesterett anså 400 000 kroner som et rimelig lisensavgiftsbeløp og siden Kystgjerde hadde handlet grovt uaktsom ble det tilkjent dobbellisensavgift som da utgjorde 800 000 kroner for hvert serskap.

For ordens skyld gjøres det oppmerksom på at Advokatfirmaet Simonsen Vogt Wiig representerte Kystgjerdet AS i saken.

Les avgjørelsen i sin helhet i Lovdatas database.

Skrevet av senioradvokat Hedda Baumann Heier og advokat Camilla Hagelien i Advokatfirmaet Simonsen Vogt Wiig AS.



Maren Tveten Aalbu

Ny lov om levering av digitale ytelser til forbrukere har trådt i kraft

Den 1. januar 2023 trådte den nye digitalytelsesloven i kraft. Loven gjennomfører EUs digitalytelsesdirektiv 2019/770 i norsk rett, men inneholder også flere særnorske regler. Loven gir forbrukere en rekke nye ufravikelig rettigheter ved kjøp av digitale ytelser. Levering av denne typen tjenester har nemlig tidligere ikke vært særskilt lovregulert i norsk rett. Leverandørene har derfor stått relativt fritt til å utforme ensidige og komplekse vilkår for levering. Dette blir det en slutt på nå.

1. Lovens anvendelsesområde

Digitalytelsesloven gjelder for levering av «digitale ytelser» mot «vederlag» i «forbrukerforhold», jf. lovens § 1.

Med digitale ytelser menes både «digitalt innhold» og «digitale tjenester». Loven omfatter derfor et bredt spekter av ytelser, alt fra strømmetjenester for film, serier og musikk, til sosiale medier. Loven gjelder også for meldingstjenester, dataspill, e-bøker og skylagringstjenester, og da uavhengig av hvilket medium som brukes til overføring eller tilgjengeliggjøring av den digitale ytelsen.

Vilkåret om at det må foreligge et «forbrukerforhold» har det samme innholdet som etter forbrukerkjøpsloven. Loven kommer derfor bare til anvendelse der en nærings-

drivende leverer en ytelse til en forbruker, altså en person som ikke hovedsakelig handler som ledd i næringsvirksomhet.

Vederlagsbegrepet omfatter naturligvis betaling i form av penger, og da både fysisk og digital valuta. Et interessant trekk ved den nye loven er at vilkåret også vil være oppfylt der forbrukeren oppgir sine personopplysninger, med mindre leverandøren kun behandler personopplysningene for å levere ytelsen eller overholde lovpålagte plikter. Flere tjenester som tradisjonelt sett er ansett for å være gratis, som for eksempel Facebook, Instagram og Twitter, vil derfor være omfattet av loven.

Det er verdt å merke seg at digitalytelsesloven ikke kommer til anvendelse ved salg av fysiske ting.

Dette reguleres av forbrukerkjøpsloven. Digitale ytelser leveres imidlertid ofte sammen med en ting, som for eksempel et dataspill som leveres på en CD. Spørsmålet blir da hvilken lov som kommer til anvendelse. Utgangspunktet er at digitalytelsesloven gjelder der den fysiske tingen utelukkende brukes som bærer av den digitale ytelsen, som i eksempelet med dataspillet. Dersom den digitale ytelsen er nødvendig for at den fysiske tingen skal fungere, er det forbrukerkjøpsloven som kommer til anvendelse. Dette vil for eksempel være tilfellet for smarttelefoner (ting) som leveres sammen med forhåndsinnstilte apper (ytelse).

2. De viktigste bestemmelsene

Digitalytelsesloven gir forbrukere en rekke nye ufravikelige rettigheter ved kjøp av digitale ytelser. Flere av disse vil mange kjenne igjen fra forbrukerkjøpsloven. Loven inneholder imidlertid også andre typer regler som er tilpasset digitale ytelser. I det følgende gis det en innføring i de reglene som vil kunne ha størst praktisk betydning for både forbrukerne og leverandørene.

2.1 Krav til ytelsen

Loven stiller for det første nærmere krav til selve ytelsen. Nærmere bestemt skal den digitale ytelsen sam-

svare med det som er avtalt, både når det gjelder art, mengde og kvalitet. Den digitale ytelsen skal også passe for de formål som tilsvarende ytelser vanligvis brukes til og som forbrukeren har grunn til å forvente.

Ytelsen skal videre leveres uten unødig opphold og i den nyeste versjonen som er tilgjengelig på avtale-tidspunktet. Leverandøren skal også sørge for at forbrukeren får beskjed om og får levert oppdateringer, som for eksempel sikkerhetsoppdateringer.

2.2 Mangler og reklamasjoner

Hvis den digitale ytelsen ikke svarer med nevnte krav, foreligger det en mangel ved ytelsen. Dette er i tråd med forbrukerkjøpsloven. Digitalytelsesloven inneholder imidlertid også en bestemmelse om at det er leverandøren som har bevisbyrden for at ytelsen ikke er mangelfull. En mangel som oppstår innen ett år etter levering antas nemlig å ha eksistert på leveringstidspunktet, med mindre leverandøren kan bevise noe annet.

Digitalytelsesloven åpner videre opp for at forbrukeren kan kreve erstatning for ikke-økonomisk tap ved kontraktsbrudd som har påført forbrukeren en konkret og ikke ubetydelig ulempe. Dette kommer altså i tillegg til de alminnelige misligholdsbeføyelsene som vi kjenner igjen fra forbrukerkjøpsloven. Som eksempel kan nevnes tap av familiebilder som følge av en feil ved iCloud.

Forbrukeren kan, på samme måte som etter forbrukerkjøpslo-

ven, tape sin rett til å gjøre gjeldende krav ved passivitet. Etter digitalytelsesloven vil imidlertid forbrukeren først miste sin rett til å reklamere hvis han har ventet så lenge at det vil virke «illojal» overfor leverandøren å gjøre kravet gjeldende. Denne fristen kan trolig ikke være kortere enn to måneder.

2.3 Endringer

Digitalytelsesloven begrenser også leverandørens adgang til å gjøre endringer.

Leverandøren kan nemlig bare endre ytelsen når endringen har grunnlag i avtalen, den kan foretas uten kostnad for forbrukeren og forbrukeren informeres om endringen på en klar og tydelig måte.

Dersom en endring påvirker den digitale ytelsen negativt på en «ikke uvesentlig måte», kan forbrukeren heve avtalen, med mindre leverandøren gjør det mulig for forbrukeren å beholde sin ytelse uendret og uten mangler. En forbruker som godtar en valgfri oppdatering i AppStore kan altså ikke heve avtalen selv om det senere skulle vise seg at ytelsens funksjonalitet har blitt redusert.

Prisene kan bare økes i den grad dette har grunnlag i standardvilkårene. Forbrukeren skal videre varsles om prisstigninger innen rimelig tid, og kan som hovedregel si opp tjenesten kostnadsfritt ved prisøkninger over konsumprisindeksen.

2.4 Bindingstid

Loven inneholder også en regel om at bindingstid bare kan avtales hvis

forbrukeren gis en økonomisk fordel som står i forhold til bindingstidens lengde, typisk en redusert pris.

Videre er det som hovedregel ikke tillatt med en bindingstid på mer enn seks måneder. Det kan avtales lengre bindingstid i særlige tilfeller, men aldri mer enn tolv måneder.

2.5 Varsel om løpende levering

Ved løpende levering av digitale ytelser plikter leverandøren å minst én gang hver sjettede måned sende forbrukeren et varsel om at avtalen løper, og at forbrukeren kan si opp avtalen. Unnlater leverandøren å sende et slikt varsel, kan forbrukeren kostnadsfritt si opp avtalen og få refundert det beløpet som er betalt for tjenesten i perioden etter at varselet senest skulle vært sendt.

2.6 Oppsigelse ved manglende betaling

Digitalytelsesloven inneholder også en regel som skal beskytte forbrukerne fra å betale for tjenester som de ikke lenger bruker.

Dersom det er avtalt periodevis betaling for løpende levering av digitale ytelser, og forbrukeren ikke har betalt for tjenesten i en periode på seks måneder etter forfall, anses nemlig avtalen som oppsagt fra forbrukerens side. Er det avtalt bindingstid, vil oppsigelsen først få virkning etter utløp av denne.

Maren Tveten er fast advokat i avdeling HITEK i Advokatfirmaet Selmer, Oslo.



Gorrissen Federspiel

Tue Goldschmieding

DORA-forordningen styrker cyber- og informationssikkerheden inden for den finansielle sektor

Den 16. januar 2023 trådte Europa-Parlamentets og Rådets Forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i kraft, på engelsk kendt som Digital Operational Resilience Act (»DORA«).

DORA-forordningen er rettet mod den finansielle sektor og har til formål at styrke finansielle virksomheders modstandsdygtighed over for forestående cyber- og informationssikkerhedshændelser. Forordningen er samtidig en del af en større lovpakke, der sigter mod at forbedre og harmonisere kravene til it-sikkerhed i EU.

DORA-forordningen fastsætter specifikke og detaljerede krav til sikkerheden i net- og informationssystemer, der skal sætte de finansielle virksomheder i stand til at modstå og reagere på cyber- og informationssikkerhedshændelser, således at de kan forsætte med at levere deres finansielle ydelser og minimere forstyrrelser for kunder og samfundet. Forordningens krav finder anvendelse på en bred vifte af finansielle virksomheder, herunder betalings-tjenesteudbydere, kreditinstitutter, pengeinstitutter, pensionselskaber og forsikringselskaber.

Forordningens øgede krav til cybersikkerhed indebærer samtidig ændringer i den måde, hvorpå de finansielle virksomheder håndterer deres cyber- og informationssikkerhed. Fremover skal de finansielle virksomheder bl.a. have et cybersikkerhedsprogram, der omfatter poli-

tikker, procedurer og risikostyringsaktiviteter.

DORA-forordningen vil finde anvendelse for de finansielle virksomheder fra den 17. januar 2025. Det forventes, at der i implementeringsperioden vil blive foretaget ændringer og tilpasninger i de nuværende danske regler.

Læs forordningen her: <https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A32022R2554>

DSA-forordningen skærper kravene til digitale formidlingstjenester

Den 16. november 2022 trådte Europa-Parlamentets og Rådets Forordning (EU) 2022/2065 af 19. oktober 2022 om et indre marked for digitale tjenester i kraft. Forordningen, der går under navnet Digital Services Act (»DSA«), regulerer digitale formidlingstjenester i deres rolle som bindeled mellem brugere, der udveksler information, varer eller tjenesteydelser. Formidlingstjenester omfatter bl.a. sociale medier, digitale markedspladser og søgemaskiner.

DSA-forordningen udgør en del af en større lovpakke, der har til formål at modernisere reguleringen af de digitale markeder i EU. DSA-forordningen indfører derfor en række omfattende ændringer af Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 (»e-handelsdirektivet«), som blev vedtaget for mere end 20 år siden. Disse ændringer er udtryk for et øget ansvar for formidlingstjenesterne samt en større kontrol af disse, hvilket skal være med til at bi-

drage til et mere sikkert, gennemsigtigt og ansvarligt onlinemiljø.

DSA-forordningens omfattende regelsæt indeholder blandt andet i) nye regler for formidlingstjenesters ansvar for nedtagning af ulovligt indhold, ii) regler for reklamer på formidlingstjenesterne, herunder skærper af kravene for indhold tilgængeligt for mindreårige, iii) en forpligtelse for formidlingstjenester til at sikre brugerne adgang til at anmelde ulovligt indhold på formidlingstjenesterne og iv) forbud mod såkaldte 'dark patterns', der er en påvirkningsteknik, som har til hensigt at vildlede brugerne til at træffe en beslutning, som de ellers ikke ville have truffet.

Sanktionerne for overtrædelse af DSA-forordningen er ikke ubetydelige, idet formidlingstjenesterne kan sanktioneres med op til 6 % af deres samlede årlige indtægt eller omsætning.

Læs forordningen her: <https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32022R2065&from=EN#d1e1527-1-1>

NIS2-direktivet sikrer et højere cybersikkerhedsniveau

Den 16. januar 2023 trådte Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (»NIS2«) i kraft. NIS2-direktivet er en videreudvikling af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for



Illustrationsfoto: Colourbox.com

net- og informationssystemer i hele Unionen (»NIS«), hvis formål var at styrke det generelle cybersikkerhedsniveau i EU.

Formålet med det nye NIS2-direktiv, der erstatter NIS-direktivet, er at yderligere styrke og ensarte cyber- og informationssikkerheden i EU som følge af en stigende cybertrussel. NIS2-direktivet indeholder derfor flere og mere omfattende krav, ligesom anvendelsesområdet udvides til at omfatte flere sektorer og aktører, som anses for værende kritiske for samfundet og økonomien.

Mere konkret er anvendelsesområdet for NIS2-direktivet udvidet til at gælde virksomheder, organisatio-

ner og myndigheder, der kategoriseres som »væsentlige enheder« eller »vigtige enheder«. Disse begreber er nærmere defineret i direktivet og indeholder rum til fortolkning. Derudover udvides omfanget af sektorer således, at reglerne blandt andet også gælder for sektorer som fødevarerproduktion, affaldshåndtering og hele forsyningskæden. Den samlede liste over omfattede sektorer kan findes i NIS2-direktivets bilag 1 og 2.

Af de væsentligste krav i NIS2-direktivet kan nævnes risikostyring, sikkerhedsforanstaltninger, etablering af nødprocedurer, ledelsesmæssig forankring og processer for rapportering til tilsynsmyndighe-

derne. Desuden introduceres der strengere sanktioner, som blandt andet skal være effektive og have afskrækkende virkning.

NIS2-direktivet har implementeringsfrist i Danmark den 17. oktober 2024, hvorefter de nationale bestemmelser og love skal anvendes og håndhæves fra den 18. oktober 2024.

Læs hele direktivet her: <https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32022L2555&from=EN-d1e4509-80-1>

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



Christina Wikström og
Anton Karlsson

Sekretessgenombrott vid teknisk bearbetning och lagring

Regeringen överlämnade den 26 januari 2023 remiss *Sekretessgenombrott vid teknisk bearbetning eller lagring av uppgifter* till Lagrådet, avseende förslag till en ny sekretessbrytande bestämmelse i offentlighets- och sekretesslagen (2009:400) (OSL), som möjliggör för myndigheter att lämna uppgifter som omfattas av sekretess till en enskild eller till en annan myndighet som har i uppdrag att tekniskt bearbeta eller tekniskt lagra uppgifterna för den uppgiftslämnande myndighetens räkning. Förslaget till en ny sekretessbrytande bestämmelse bygger på resultatet av betänkandet *Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering*¹, även kallad it-driftsutredningen, som tillsattes för att kartlägga och analysera statliga myndigheters rättsliga förutsättningar för utkontraktering av it-drift till privata tjänsteleverantörer och samordnad it-drift mellan myndigheter.

It-driftsutredningen utmynnade bland annat i ett förslag om att införa en sekretessbrytande bestämmelse med sikte på utkontraktering av it-drift, och det är en reviderad version av detta förslag som är föremål för den remiss som regeringen överlämnat till Lagrådet. Det råder en viss osäkerhet avseende de rättsliga förutsättningarna för statliga myndigheter att

utkontraktera it-drift, och då särskilt med hänsyn till när en uppgift som omfattas av utkontraktering ska anses röjd enligt OSL.² För att en utkontraktering, genom vilka uppgifter vanligen utlämnas, ska vara förenlig med OSL föreslås därför att en sekretessbrytande bestämmelse införs i OSL.

Förslaget i lagrådsremissen innebär att sekretess inte hindrar att en uppgift lämnas till en enskild eller till en annan myndighet som för den utlämnande myndighetens räkning har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra³ uppgiften, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut. I motiven till förslaget förtydligörs att en privat tjänsteleverantör som inte omfattas av offentlighets- och sekretesslagen, inte kan tillämpa den sekretessbrytande bestämmelsen när denne avser att exempelvis överföra uppgifter till en underleverantör.

Lagrådet lämnade den 14 februari 2023 yttrande avseende förslaget, genom vilket följande modifierade formulering föreslås:

- 2 Dir. 2019:64, *Säker och kostnadseffektiv it-drift för den offentliga förvaltningen*, s. 5.
- 3 En analys av advokat Christina Wikström och Partners Advokatbyrå, av begreppet ”teknisk bearbetning eller teknisk lagring” publicerades i Lov&Data 2021 nr. 4 s. 4–8.

”Sekretess hindrar inte att en myndighet lämnar en uppgift till en enskild eller till en annan myndighet om det sker med anledning av uppdrag att för myndighetens räkning tekniskt bearbeta eller tekniskt lagra uppgiften. En uppgift får dock lämnas endast om det inte är olämpligt.”

Förslaget väntas leda till en minskad osäkerhet för myndigheter i samband med utkontraktering eller samordning av it-drift. Regeringen föreslår också att tystnadsplikten enligt lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter ska ha företräde framför rätten att meddela och offentliggöra uppgifter (meddelarfriheten)⁴. En proposition är avsedd att avlämnas till riksdagen för slutbehandling den 11 april 2023 med ett planerat ikraftträdande den 1 juli 2023.⁵

- 4 Meddelarfriheten följer av 1 kap. 1 § andra stycket och 7 § första stycket tryckfrihetsförordningen (1949:105) samt 1 kap. 1 § första stycket och 10 § första stycket yttrandefrihetsgrundlagen (1991:1469).
- 5 Statsrådsberedningens propositionsförteckning våren 2023, <https://www.regeringen.se/48ecec/contentassets/0e418b396c044cf39acb6daae9f33f10/propositionsfor-teckning-varen-2023.pdf>.

1 SOU 2021:1.

Tolkning av it-avtal omfattande licens och utveckling

Hovrätten för Västra Sverige lämnade den 20 januari 2023 dom i mål T 6331–21, avseende tolkning av it-avtal omfattande licens och utveckling. Genom ett licensavtal åtog sig MYBW Office Management AB (Office Management) att till Art Clinic AB (Art Clinic) tillhandahålla ett journalsystem. Journalsystemet kom även att kundpasseras genom ett utvecklingsarbete. Sedan Art Clinic hävt avtalet med hänvisning till att journalsystemet var i dröjsmål och behäftat med fel, uppkom tvist om vilken leverans avtalet omfattade och när leverans skulle ske. Art Clinic menade att avtalet omfattade utveckling enligt viss kravspecifikation till viss leveransdag, medan Office Management menade att avtalet omfattade licens med grundkonfiguration, och att utvecklingsarbete enligt viss kravspecifikation och viss tidplan föll utanför avtalet.

Hovrätten konstaterade inledningsvis att någon gemensam partsavsikt med avtalet inte gick att fastställa, varför en samlad helhetsbedömning med hänsyn till samtliga omständigheter, däribland avtalets ordalydelse, i stället skulle bli avgörande. Även om det i licensavtalet saknades föreskrifter om att journalsystemet skulle utvecklas enligt viss kravspecifikation, ansåg hovrätten att flertalet omständigheter talade för att parternas avtal omfattade utveckling av journalsystemet, bland annat avtalets ändamål och att Office Management inte krävt betalt efter att grundkonfigurationen levererats. Utredningen visade däremot att Art Clinic tillhandahållit flertalet kravspecifikationer, som också löpande utvecklats. Med utgångspunkt från detta drog hovrätten slutsatsen att avtalet innehöll att journalsystemet skulle utvecklas, men däremot inte att så skulle ske i enlighet med en bestämd kravspecifikation. Av licensavtalet framgick vidare att leveranstiden är enligt överenskommelse. På samma sätt som gäller kravspecifikationen följer av utredningen att denna har

förändrats över tid, varför hovrätten även i denna del drog slutsatsen att avtalet inte heller kunde anses innehålla att journalsystemet skulle vara levererat vid tidpunkt som Art Clinic angivit som leveransdag.

Rättsfallet åskådliggör den komplexitet som omgärdar systemleveransavtal omfattande grundlicens, konfiguration och kundunik utveckling, särskilt när kraven löpande fastställs i ett agilt utvecklingsprojekt. För att kunden under sådana omständigheter ska kunna göra sin rätt till resultat, enligt överenskommen kravspecifikation på avtalad leveransdag, gällande, krävs ett tydligt avtal där leverantörens åtagande framgår av det ursprungliga avtalet eller av löpande tillägg till avtalet.

En svensk statlig e-legitimation

Myndigheten för digital förvaltning (Digg) slutredovisade den 30 januari 2023 uppdraget⁶ att föreslå hur en statlig e-legitimation kan utformas. I slutrapporten, *En säker och tillgänglig statlig e-legitimation*, understryker Digg att Sverige behöver en statlig e-legitimation. Sverige är idag ett av ett fåtal länder i EU där det allmänna fortfarande inte råder över den samhällskritiska infrastruktur som e-legitimation utgör. Vidare är användningen av e-legitimationen i Sverige bred, och det särskilt genom e-legitimationen BankID. Avbrott och störningar i BankID kan få stora negativa konsekvenser för flera delar av det svenska samhället, vilket talar för att Sverige behöver en statlig e-legitimation.

Att staten ska utfärda en e-legitimation föreslogs redan 2019 av 2017 års ID-kortsutredning⁷. Utredningen konstaterade dock att det inte var möjligt för utredningen att uppskatta kostnaderna för bland annat utveckling och förvaltning av e-legitimationen. Vidare har det visat sig tidskrävande att ta

fram ett kombinerat id-kort och e-legitimation, i enlighet med utredningens förslag. Under 2021 föreslog EU-kommissionen en revidering av eIDAS-förordningen, vilket bland annat skulle innebära ett krav på att Sverige inrättar en statlig e-legitimation inom viss tid.⁸ I kombination med ett förändrat säkerhetsläge har behov av viss skyndsamhet med framtagandet av en statlig e-legitimation ansetts föreligga. Regeringen tillsatte av denna anledning den 22 december 2022, vid sidan av Diggs uppdrag, en särskild utredare⁹ med uppgift att bland annat lämna förslag på hur en statlig e-legitimation kan utformas och tillhandahållas. Diggs slutrapport kommer att utgöra ett beredningsunderlag till utredningen, och kompletterar de analyser som tidigare gjorts genom exempelvis ID-kortsutredningen.

Digg föreslår att den statliga e-legitimationen ska ges ut i formen av ett kontaktlöst aktivt kort, som ska användas tillsammans med en personlig kod och en klientapplikation, exempelvis en mobilapplikation. E-legitimationen är avsedd att utgöra ett komplement till befintliga lösningar på marknaden. Utvecklingstiden, från det att nödvändiga beslut fattats av regering och riksdag, bedömer Digg vara 24 månader. Nästa steg i utvecklingen av en svensk statlig e-legitimation är att regeringsuppdraget delredovisas den 16 oktober 2023.

Christina Wikström, advokat och partner, och Anton Karlsson, biträdande jurist, verksamma vid Wikström & Partners Advokatbyrå i Stockholm och specialiserade på IT, IP och dataskydd.

8 COM(2021) 281, *Förslag till Europaparlamentets och rådets förordning om ändring av förordning (EU) nr 90/2014 vad gäller inrättandet av en ram för europeisk digital identitet.*

9 Dir. 2022:142, *Säker och tillgänglig digital identitet.*

6 Regeringsbeslut I2022/01335, Uppdrag att föreslå hur en statlig e-legitimation kan utformas.

7 SOU 2019:14, *Ett säkert statligt ID-kort – med en e-legitimation.*

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

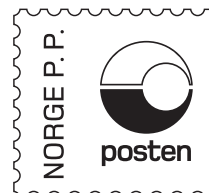
BESTILL I DAG

Er du Lovdatakunde kan du bestille
direkte gjennom Lovdata Pro.

<https://pro.lovdata.no>



LOVDATA
PRO



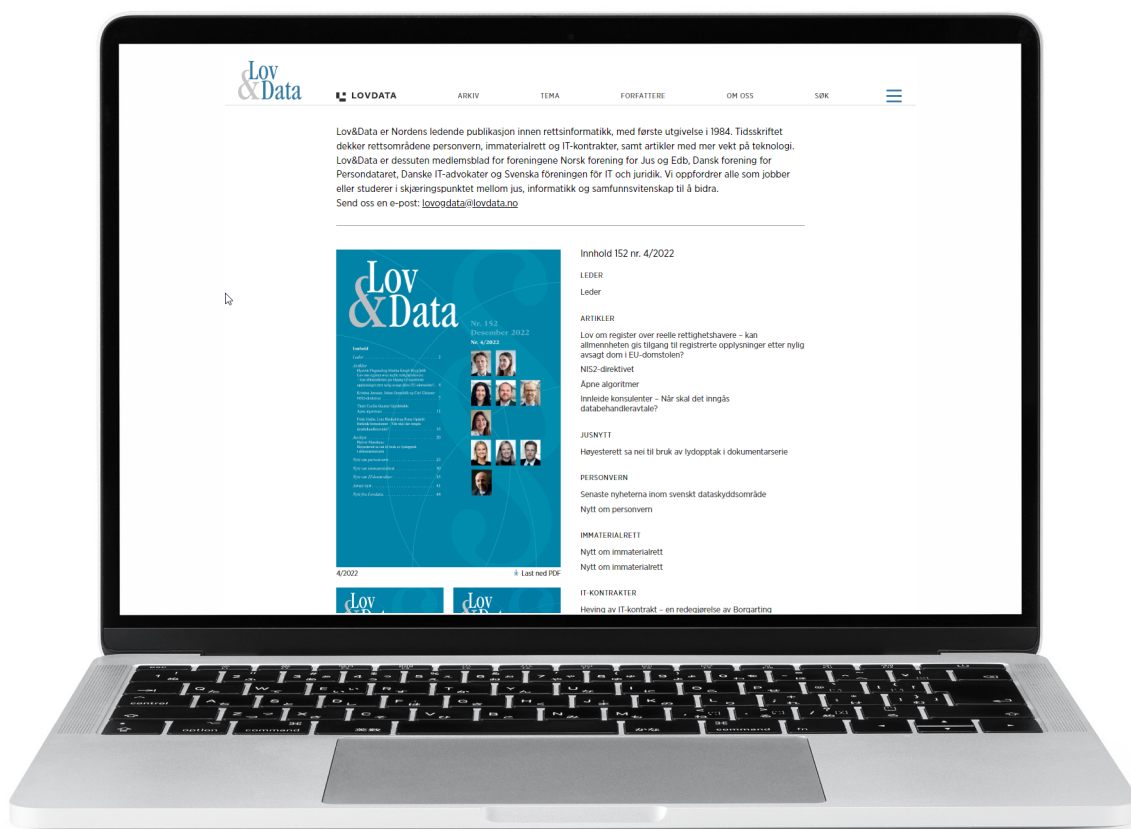
Returadresse:
Lovdata
Pb. 6688 St. Olavs plass
NO-0129 Oslo
Norge

Nytt fra



Tidsskriftet Lov&Data i elektronisk utgave

Etter 39 år blir Lov&Data endelig lansert i elektronisk utgave! Det betyr at du vil finne tidsskriftet åpent tilgjengelig og i sin helhet på lod.lovdata.no



Nettsiden er tilgjengelig på norsk, svensk og dansk – med integrasjon mot Lovdata Pro.

Vi ønsker deg god lesing!