Lov & Data

Juni 2024
Nr. 158 2/2024

Innhold

Lov&Data er et nordisk 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
Alias: www.lovogdata.no
www.lawanddata.no

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

Lov&Data er medlemsblad for foreningene Norsk forening for Jus og EDB, Dansk forening for Persondataret, Danske IT-advokater, Svenska föreningen för IT och juridik (SIJU) og Finnish IT Law Association.

Fra 2024 er Lov&Data kun tilgjengelig på nett, lod.lovdata.no.

Trykkeri: Payout: TRYKT I NORGE NO - 1470 Miljøfyrtårn®

Leder

Kjære kolleger og lesere,

Etter ti år som redaktør for Lov&Data, er det på tide å overlate roret til Sarah Habberstad. I disse årene har bladet gjennomgått mange endringer, både med hensyn til digitalt format og også med hensyn til innhold. Det har hele tiden vært et fantastisk godt samarbeid med Lovdata (Kari Gyllander, Trine Shil Kristiansen og Odd Storm-Paulsen), noe som har bidratt til å gjøre arbeidet gledesfylt. Tilsvarende har det vært et veldig godt samarbeid med redaktørene for de andre nordiske landene. Arbeidet som redaktør har vært både interessant og gøy.

Jeg er spesielt glad for å kunne overlate roret til nettopp Sarah Habberstad, fordi jeg vet hun deler det samme engasjementet for teknologi og jus som Lovdata og jeg selv. Sara bringer et nytt og friskt perspektiv, og jeg vet at hun allerede har gode planer for organisering av arbeidet og samarbeidet. Jeg gleder meg til å følge bladet videre, og til å være leser og bruker av bladet. Nå som jeg ikke lenger skal være redaktør, gleder jeg meg også til å bidra til bladet i form av artikler og annet innhold.

Den rivende utviklingen vi har hatt med AI er blant de veldig mange temaene som gjør at bladet fortsatt har stor relevans. Det blir spennende å se hvordan disse store og

Jarle Roar Sæbø

viktige temaene blir belyst for et bredt spekter av lesere i fremtiden.

Jeg benytter også anledningen til å ønske velkommen Viveca Still vår nye redaktør for Finland, et land som så langt ikke har vært dekket så godt i bladet. Det er svært gledelig at bladet fremover også vil bringe perspektiver og nyheter fra finske bidragsytere.

Avslutningsvis vil jeg takke alle våre bidragsytere som velvillig har tatt imot oppfordringer til å bidra med innhold. Det har alltid vært svært enkelt å oppfordre travle mennesker til å bruke til på å skrive artikler og annet innhold til Lov&Data, og dette er en god indikasjon på at bladet oppleves som en relevant og viktig arena for kunnskapsspredning.

Jarle Roar Sæbø

Illustrasjon: Colourbox.com

Lov, logging, lagring og lengde

Logging som sikkerhetstiltak etter GDPR

Av Hanne Gulbrandsen og Ole Martin Moe

Ifølge GDPR artikkel 32 er det påkrevd å ha tilstrekkelige tekniske og organisatoriske tiltak for å sikre et passende sikkerhetsnivå ved behandling av personopplysninger. Logging er en essensiell del av disse tiltakene. Et spørsmål vi ofte møter som advokater er hvilke logger man må ha som virksomhet og hvor lenge man kan eller plikter å lagre slike logger.

Logging i IT-sammenheng refererer til prosessen med å registrere og lagre detaljer om hendelser og aktiviteter i et system. Dette kan inkludere informasjon om hvem som har utført hvilke handlinger, når, og hvordan. Logging er kritisk for å sikre sporbarhet og overvåking av systemers integritet og konfidensialitet. I denne artikkelen vil vi bruke begrepet logging om det å registrere hendelser og aktiviteter som skjer i et datanettverk eller ved bruk en it-tjeneste eller et informasjonssystem med det formål å kunne finne tilbake til hvilken bruker som stod bak den enkelte aktivitet/hendelse. Dette formålet betegnes også ofte som sporing. Hendelser inkluderer alt fra pålogging og avlogging av brukere til endringer i systeminnstillinger og forsøk på uautorisert tilgang og benevnes ofte som aktivitets- og hendelseslogger.

Logging er viktig fordi det gir virksomheter mulighet til å:

- Spore og undersøke mistenkelige aktiviteter.
- Overvåke systemytelse og identifisere feil.
- Overholde lovpålagte krav til sikkerhet og databeskyttelse.
- Tilby dokumentasjon i tilfelle juridiske tvister eller etterforskninger.

Hanne Gulbrandsen

Ole Martin Moe

I denne artikkelen vil vi se nærmere på de rettslige rammene for logging og lagringstid etter GDPR.

Behandling av personopplysninger

Fordi formålet med slike logger (også) er å kunne følge med på hvem som har gjort hva og når, vil det å logge innebære behandling av personopplysninger med den følge at personvernprinsippene og personvernregelverket gjelder. Vi vil særlig se på hvordan prinsippet om lovlighet treffer logging ved å se nærmere på kravet til behandlingsgrunnlag og hvilke rammer prinsippet om lagringsbegrensning setter for oppbevaring av logger. Vi vil også se på noen konkrete forslag til lagringsfrister som finnes i lovgivning og i veiledning fra offentlige myndigheter.

Logger for andre formål enn sporing og tilgangsstyring kan også innebære behandling av personopplysninger slik at etterlevelse av personvernprinsippene er tilsvarende aktuelt. Vi vil imidlertid ikke berøre dette i denne artikkelen.

> Et spørsmål vi ofte møter som advokater er hvilke logger man må ha som virksomhet og hvor lenge man kan eller plikter å lagre slike logger.

Krav til logging

Noen sektorer har i dag særlovgivning som setter tydelige rammer for at logging skal skje og hvor lenge loggene skal lagres. Disse har dermed behandlingsgrunnlag i en rettslig forpliktelse etter GDPR artikkel 6 nr. 1 bokstav c. Andre

virksomheter er prisgitt de generelle reglene i GDPR.

Det er vanlig praksis å basere logging på artikkel 6 nr. 1 bokstav f (berettiget interesse), med en henvisning til forpliktelsen til å sikre personopplysninger etter artikkel 32 og fortalepunkt 49[1] der lovgiver uttaler at sikkerhetsovervåking kan utgjøre en berettiget interesse.

Logging er et grunnleggende informasjonssikkerhetstiltak som skal være iverksatt, se for eksempel Datatilsynets overtredelsesgebyr til Østre Toten kommune.[2] Det følger også av NSMs grunnprinsipper for IKT-sikkerhet[3] at sikkerhetsovervåking (logging) er et grunnleggende sikkerhetstiltak som skal være på plass. En vurdering av berettiget interesse med vekting av nødvendighet og den avsluttende balansetesten kan dermed fremstå som overflødig når resultatet uansett er at logging skal skje.

GDPR artikkel 32 krever at virksomheter innfører passende tekniske og organisatoriske tiltak, for eksempel pseudonymisering og kryptering, samt evnen til å sikre konfidensialitet, integritet og tilgjengelighet av systemer og tjenester. Det kreves også at virksomheter kan gjenopprette tilgjengeligheten av personopplysninger i tilfelle fysiske eller tekniske hendelser. Logging er ikke nevnt eksplisitt i artikkel 32, men er en grunnleggende forutsetning for å oppfylle kravene til personopplysningssikkerhet. Logging er dessuten nevnt som et grunnleggende sikkerhetstiltak i NSMs grunnprinsipper for informasjonssikkerhet, samt påkrevd etter en rekke særlover, herunder helseregisterloven, pasientjournalloven og hvitvaskingsloven.

Det er et bærende prinsipp i personvernretten at personopplysninger kun skal gjøres tilgjengelig for dem som har tjenstlig behov. Dette følger av grunnprinsippet om informasjonssikkerhet og kravet til konfidensialitet nedfelt i personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 som stiller krav om at den behandlingsansvarlige gjennomfører tekniske og organisatoriske tiltak for å oppnå et egnet sikkerhetsnivå ved behandlingen av personopplysninger. Hvilket sikkerhetsnivå og hvilke tiltak som må gjennomføres må vurderes ut fra risikoen ved behandlingen, jf. bestemmelsens andre ledd. Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

Tilgang til personopplysninger skal styres av den ansattes arbeidsoppgaver og hvorvidt tilgang til personopplysningene er nødvendig for å utføre disse arbeidsoppgavene. Med dette følger også et behov for å kunne verifisere hvorvidt det forelå et tjenstlig behov eller hvorvidt personopplysninger er aksessert eller forsøkt aksessert uten at det et slikt behov forelå. I og med at logger kan identifisere og bidra til å spore mistenkelig aktiviteter og gjør det mulig å fastslå hvem som har utført bestemte handlinger eller endringer, vil logging og sporing være nødvendig for å opprettholde et egnet sikkerhetsnivå og oppfylle artikkel 32.

Personopplysningsforskriften[4] som var gjeldende før vedtakelse av personvernforordningen ga den behandlingsansvarlige betydelig bedre veiledning hva gjaldt både krav til innholdet i internkontrollen og overordnete føringer på etterlevelse av krav til informasjonssikkerheten. Da personvernforordningen trådte i kraft, ble det nasjonale spillerommet for å gi detaljerte bestemmelser innskrenket. Det følger imidlertid av forarbeidene at det til tross for mindre detaljering av regelverket, likevel ble ansett som åpenbart at det måtte foreligge et system for internkontroll og informasjonssikkerhet med visse elementer på plass. Den nå opphevede forskriften påla[5] den behandlingsansvarlig å registrere (logge) både autorisert og forsøk på uautorisert bruk av informasjonssystemet, hvilket tyder på at lovgiver mener at logging er et nødvendig element for å etablere tilfredsstillende informasjonssikkerhet.

Argumenter for og mot artikkel 32 som supplerende rettsgrunnlag

Som nevnt i forrige punkt er logging et grunnleggende informasjonssikkerhetstiltak som skal være iverksatt, og en vurdering av berettiget interesse kan dermed fremstå som overflødig når resultatet uansett er at logging skal skje. Man kan

1 Behandling av personopplysninger i det omfang som er strengt nødvendig og forholdsmessig for å sikre nett- og informasjonssikkerheten, det vil si et netts eller informasjonssystems evne til, på et bestemt sikkerhetsnivå, å stå imot utilsiktede hendelser eller ulovlige eller skadelige handlinger som svekker tilgjengeligheten, autentisiteten, integriteten og konfidensialiteten til lagrede eller overførte personopplysninger, samt sikkerheten i beslektede tjenester som tilbys av eller er gjort tilgjengelige via nevnte nett og systemer, av offentlige myndigheter, enheter for IT-beredskap (CERT), enheter for IT-sikkerhetshendelser (CSIRT), leverandører av elektroniske kommunikasjonsnett og -tjenester og leverandører av sikkerhetsteknologier og -tjenester, utgjør en berettiget interesse for den berørte behandlingsansvarlige. Dette kan f.eks. omfatte å hindre ulovlig tilgang til elektroniske kommunikasjonsnett og spredning av skadelige koder og å stoppe «tjenestenektangrep» og skade på datasystemer og elektroniske kommunikasjonssystemer

2 Datatilsynets referanse 21/00480-14

3 NSMs grunnprinsipper for IKT-sikkerhet, pkt. 3.2.4.

4 FOR-2000-12-15-1265 (opphevet)

5 Personopplysningsforskriften § 2-8 og § 2-14.

derfor spørre seg om artikkel 32 i seg selv kan være behandlingsgrunnlag for logging som en rettslig forpliktelse etter artikkel 6 nr. 1 bokstav c.

På den ene siden kan man argumentere for at artikkel 32 er en skjønnsmessig bestemmelse som tilsier at informasjonssikkerhetsnivået skal endres i takt med risikoen ved behandlingen, og at det derfor er vanskelig å si at bestemmelsen i seg selv etablerer et behandlingsgrunnlag. Det kan derfor være riktigere å hjemle den behandlingen av personopplysninger som skjer ved logging og sporing i artikkel 6 nr. 1 bokstav f) – berettiget interesse, der oppfyllelse av artikkel 32 vil være et vektig argument inn i interesseavveiningen. Dette utgangspunktet finner vi støtte for i fortalens punkt 49, som nedfeller at behandling av personopplysninger for å sikre informasjonssikkerheten anses som en berettiget interesse. Dette hadde selvsagt vært enklere om lovgiver kunne beholdt reguleringen i den tidligere personopplysningsforskriften, men nå må den behandlingsansvarlige altså selv dokumentere vurderingen av den berettigete interessen i dette tilfellet. Med tanke på tidligere regulering, artikkel 32 og fortalens (49) burde dokumentasjonen kunne gjøres relativ enkel. Når loggingen er basert på artikkel 6 nr. 1 bokstav f kan den registrerte også protestere etter artikkel 21. Såfremt den behandlingsansvarlige har gjort en god vurdering av dataminimering og formålsbegrensning i loggingen er det imidlertid ikke gitt at protesten skal tas til følge. I lys av momentene vi har listet opp så langt i denne artikkelen har den behandlingsansvarlige gode argumenter for at logging oppfyller kravet til «tvingende berettigede grunner» i artikkel 21 og at logging derfor uansett skal skje.

Dersom artikkel 32 skal kunne brukes som et selvstendig behandlingsgrunnlag er det mest nærliggende å anse den som en rettslig forpliktelse etter artikkel 6 nr. 1 bokstav c.

Rammene for hva som kan utgjøre en rettslig forpliktelse etter bokstav c følger av artikkel 6 nr. 3. Bestemmelsen viderefører i stor grad den tilsvarende bestemmelsen i personverndirektivet artikkel 6 bokstav c og personopplysningsloven 2000 § 8 første ledd bokstav b. En forskjell er imidlertid at GDPR krever at den aktuelle rettslige forpliktelsen skal være hjemlet i unionsretten eller medlemsstatenes nasjonale rett som den behandlingsansvarlige er underlagt.

Illustrasjon: Colourbox.com

Ifølge nr. 3 må formålet med behandlingen følge av det supplerende rettsgrunnlaget, men det kreves ikke at behandlingen av personopplysninger er regulert eksplisitt. Det er her tilstrekkelig at behandling av personopplysninger er en forutsetning for å oppfylle formålene som er fastsatt i lov, forskrift eller vedtak.[6] Samtidig er det viktig å ha med seg at legalitetsprinsippet og rettspraksis knyttet til EMK artikkel 8 innebærer at jo mer inngripende en behandling av personopplysninger er, jo klarere supplerende rettsgrunnlag kreves.

Det følger av forordningen at formålet med behandlingen skal være fastsatt i det supplerende rettsgrunnlaget. Samtidig fremgår det at det nasjonale rettsgrunnlaget kan inneholde spesifikke regler for å legge til rette for etterlevelse av bestemmelsene i personvernforordningen.[7] Dette kan for eksempel være regler om hvilke opplysninger som kan behandles, hvem det kan behandles opplysninger om og hvor lenge opplysningene kan lagres.

Det finnes også eksempler på andre rettslige forpliktelser i GDPR som forutsetter behandling av personopplysninger: når den behandlingsansvarlige utleverer den registrertes personopplysninger etter innsynsretten i artikkel 15 og når man behandler en protest der den registrerte gjør gjeldende særlige forhold ved hens situasjon etter artikkel 21. GDPR er altså i seg selv ikke til hinder for en slik løsning, og inneholder tvert imot flere plikter for den behandlingsansvarlige som forutsetter behandling av personopplysninger.

Ordlyden i GDPR artikkel 32 nr. 1 ser slik ut:

> *Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,*
>
> *a. pseudonymisering og kryptering av personopplysninger,*
>
> *b. evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,*
>
> *c. evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,*
>
> *d. en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er*
>
> (Vår utheving)

Bestemmelsen er inntatt i norsk rett gjennom personopplysningsloven, fastsetter formålet «oppnå et sikkerhetsnivå som er egnet» og inneholder spesifikke regler for å sikre etterlevelse av bestemmelsene i forordningen (eksemplene på tiltak i bokstav a–f). Dette oppfyller kravene til supplerende rettsgrunnlag i GDPR artikkel 6 nr. 3.

Et relevant spørsmål er hvor inngripende logging artikkel 32 kan hjemle i seg selv. Ordlyden er generell og tar ikke innover seg spesielle hensyn som kan gjøre seg gjeldende i ulike sektorer og ved logging i arbeidsforhold. Vi mener imidlertid uansett at artikkel 32 kan brukes som supplerende rettsgrunnlag for det NSM beskriver som minimumstiltak i prinsippene for IKT-sikkerhet[8], da dette er tiltak som alltid skal være iverksatt. Disse minimumstiltakene er logging av:

a. data relatert til tilgangskontroll (vellykkede og mislykkede pålogginger) på enheter og tjenester og
b. administrasjons- og sikkerhetslogger fra enheter og tjenester i IKT-systemene. For klienter bør man i tillegg som minimum registrere
c. forsøk på kjøring av ukjent programvare (ref. 2.3.2) og
d. forsøk på å få forhøyede systemrettigheter («privilege escalation»).

Dersom loggingen vil være særlig inngripende ved at den for eksempel registrerer særlige kategorier av personopplysninger kan man diskutere hvor langt hjemmelen rekker. Vi mener på bakgrunn av dette at artikkel 32 ikke kan være prinsipielt utelukket som behandlingsgrunnlag for sikkerhetstiltak og at man som behandlingsansvarlig tvert imot kan vise til artikkel 32 som rettslig forpliktelse for «vanlig» sikkerhetslogging.

> Vi mener imidlertid uansett at artikkel 32 kan brukes som supplerende rettsgrunnlag for det NSM beskriver som minimumstiltak i prinsippene for IKT-sikkerhet, da dette er tiltak som alltid skal være iverksatt.

Krav til lagringstid

Enten loggingen er basert på artikkel 6 nr. 1 bokstav c, jf. artikkel 32 eller en vurdering av berettiget interesse etter bokstav f inneholder ikke GDPR konkrete tidsfrister for hvor lenge logger skal lagres, men artikkel 5 nr. 1 e) fastsetter prinsippet om lagringsbegrensning. Dette prinsippet innebærer at personopp-

6 Skullerud mfl., Personvernforordningen. Lovkommentar, Artikkel 6. Behandlingens lovlighet, Juridika (kopiert 27. mai 2024)

7 Ibid.

8 NSMs grunnprinsipper for IKT-sikkerhet, pkt. 3.2.4.

lysninger ikke skal lagres lenger enn nødvendig for formålene de ble samlet inn for.

Den behandlingsansvarlige må derfor vurdere formålet med loggene og bestemme en passende lagringstid. Dette innebærer å ta hensyn til:

- Formålet med loggingen.
- Sensitiviteten av opplysningene.
- Risikoen for den registrerte hvis loggene blir kompromittert.
- Relevante lovkrav og bransjestandarder.
- Tekniske og praktiske hensyn, inkludert lagringskapasitet og sletterutiner.

GDPRs generalitet gir fleksibilitet for den behandlingsansvarlige, men kan samtidig gjøre det arbeidskrevende og vanskelig å skulle lande en lagringstid for logger – både med og uten personopplysninger. Vi har derfor samlet noen kilder som kan si noe om dette, men vet samtidig av erfaring at det i store norske virksomheter er et vidt spenn i lagringstid: fra noen måneder til over ti år.

- **Nasjonal sikkerhetsmyndighet (NSM)** anbefaler at logger generelt bør lagres i minst 1 år for å kunne avdekke og håndtere avvik.
- **Normen for informasjonssikkerhet og personvern i helse- og omsorgssektoren** anbefaler at logger i helsesektoren lagres i minst 3 år for å ivareta krav til dokumentasjon og etterprøvbarhet.
- **Datatilsynet** gir veiledning om at logger som inneholder personopplysninger ikke bør lagres lenger enn nødvendig for formålet de ble samlet inn for, og anbefaler at sensitive opplysninger lagres kortere enn mindre sensitive opplysninger.
- **Politiregisterloven** krever at logger oppbevares i minst 1 år og maksimum 3 år
- **Verdipapirhandelloven** krever at logger som dokumenterer investeringstjenester oppbevares i minst 5 år.
- **Bokføringsloven** krever at regnskapsmateriale oppbevares i enten 3 år og 6 måneder eller 5 år, avhengig av type materiale.
- **Hvitvaskingsloven** krever at personopplysninger relatert til risikovurdering av hvitvasking og terrorfinansiering oppbevares i 5 år, med mulighet for forlengelse til 10 år.

Også her finner man god generell veiledning i den gamle personopplysningsforskriften som krevde at loggene minst skulle lagres i

3 måneder[9]. Det er viktig å ta med seg loggens formål i denne sammenheng; den skal muliggjøre sporing av uautoriserte oppslag mv. i personopplysninger. Lagringstiden bør da ikke være for restriktiv.

Avsluttende merknader

Logging er et grunnleggende sikkerhetstiltak som må være på plass for å sikre konfidensialitet, integritet og tilgjengelighet etter GDPR artikkel 32. Virksomheter må sørge for at de har effektive loggsystemer på plass som sikrer sporbarhet og beskyttelse av personopplysninger. Ved å følge prinsippet om dataminimering og overholde relevante lovkrav og bransjestandarder, kan virksomheter sikre at de logger og lagrer data på en måte som både ivaretar sikkerheten og respekterer personvernet til de registrerte.

For å sikre effektiv implementering av loggingspraksis bør virksomheter også regelmessig gjennomgå og oppdatere sine loggpolicyer, samt sørge for at ansatte er godt informert og trent i korrekt bruk av logging som et sikkerhetsverktøy. Dette inkluderer forståelse av relevant lovgivning, interne prosedyrer og beste praksis for å beskytte personopplysninger og sikre sporbarhet i informasjonssystemer.

Gode grunner taler for at man kan basere logging på artikkel 32 som en rettslig forpliktelse etter GDPR artikkel 6 nr. 1 bokstav c. Samtidig må man se hen til hva slags logging det er snakk om og hvor stort inngrep det utgjør i den registrertes rettigheter og friheter. Som behandlingsansvarlig har man uansett artikkel 6 nr. 1 bokstav f å falle tilbake på, jf. fortalepunkt 49.

Ole Martin Moe, manager og advokatfullmektig og Hanne Pernille Gulbrandsen, partner og advokat i Deloitte Advokatfirma AS.

9 Personopplysningsforskriften § 2-16

KI-forordningen: Klassisk produktregulering i møte med grunnleggende rettigheter

Av Lars Arnesen

Forordningen om kunstig intelligens (KI-forordningen) er endelig vedtatt, og vil tre i kraft i EU i løpet av sommeren 2024.[1] Det foreligger allerede en rekke grunnleggende innføringer om kunstig intelligens og KI-forordningen, gjennom et utall artikler, foredrag og podkaster. Denne artikkelen søker å gå litt mer ned i detaljene, særlig rundt delt ansvar mellom tilbyder (provider) og bruker (deployer), med søkelys på det delte ansvaret for å ivareta menneskelig tilsyn, og den delte plikten til å vurdere grunnleggende rettigheter før KI-systemer tas i bruk.

Artikkelen fokuserer kun på reglene som gjelder for KI-systemer med «høy risiko». Dette gjelder blant annet KI-systemer som brukes i en lang rekke regulerte produkter, fra heis og taubaner, til fly, biler, og medisinsk utstyr.[2] Det er i tillegg en rekke bruksformål som er regulert som «høy risiko», slik som KI-systemer som brukes for å avgjøre hvem som har rett til velferdsgoder og trygdeytelser, eller KI-systemer som brukes til å screene kandidater ved nyansettelser.[3]

Artikkelen identifiserer en kollisjon mellom to rettstradisjoner, men uten å gi et endelig svar på hvordan denne kollisjonen skal løses.

1 EU-parlamentet vedtok forordningen 13. mars, etterfulgt av EU-rådets godkjenning 14. mai 2024. Forordningen trer i kraft 20 dager etter at den er innført i *Official Journal of the European Union*.

2 KI-forordningen artikkel 6(1)(a).

3 KI-forordningen artikkel 6(1)(b).

Lars Arnesen

Delt ansvar mellom tilbyder og bruker

KI-forordningen er i utgangspunktet bygget opp på samme måte som andre produktreguleringer, slik som leker og medisinsk utstyr.[4] Dette innebærer, kort oppsummert, at tilbyderen må definere et bruksformål for KI-systemet. Tilbyderen må deretter definere en rekke funksjonelle og ikke-funksjonelle krav, som KI-systemet må oppfylle for å fungere trygt etter sitt tiltenkte formål. KI-systemet må til slutt gjennomgå en samsvarsvurdering (conformity assessment). En vellykket samsvarsvurdering gir rett til å merke KI-systemet med et CE-merke, som gir full tilgang til det europeiske markedet.

Det som så langt er beskrevet er klassisk produktreguleringsmetodikk, der forpliktelsene for å oppnå CE-merket ligger på tilbyderen av KI-systemet. Klassiske produktreguleringer er i utgangspunktet kun relevante for produsentene, enten det gjelder KI-systemer, leker eller medisinsk utstyr. Som bruker av en leke, enten du er barn eller voksen, skal du kunne stole på at leken er trygg å leke med uten å iverksette egne sikkerhetstiltak, såfremt leken er CE-merket. Heller ikke profesjonelle leketøysbrukere, slik som for eksempel barnehager, har særskilte forpliktelser etter produktregelverket for leker.[5] Det samme gjelder medisinsk utstyr. Som bruker av medisinsk utstyr, enten du er forbruker eller profesjonell bruker, har du ingen forpliktelser etter forordningen.[6]

KI-forordningen skiller seg fra klassiske produktreguleringer, ved å gi omfattende forpliktelser til profesjonelle brukere («deployers»). Begrepsbruken har variert i løpet av forhandlingene om forordningen, fra «user» i det opprinnelige forslaget fra EU-kommisjonen,[7] til «deployer» i den endelig vedtatte versjonen.[8] Begrepet «deployer» viser til enhver person eller virksomhet som bruker et KI-system, med unntak av bruk til rent personlige, ikke-

4 KI-forordningen er bygd opp i tråd med *New Legislative Framework (NLF)*, på lik linje med andre produktreguleringer i EU.

5 Direktiv 20009/48/EC (leketøydirektivet).

6 Men profesjonelle brukere i Norge har forpliktelser etter håndteringsforskriften, se også fotnote 20-21.

7 EU-kommisjonen 21. april 2021 (COM/2021/206 final).

8 Versjonen vedtatt av EU-rådet 14. mai 2024. Det er ventet at forordningen snarlig publiseres i *Official Journal of the European Union*.

profesjonelle aktiviteter.[9] Forordningen har ingen egen definisjon av «user.» Den endelige versjonen er ennå ikke oversatt til norsk, svensk eller dansk. Begrepet «profesjonell bruker» eller kun «bruker» er derfor brukt i denne artikkelen, som den foreløpig uoffisielle norske oversettelsen av «deployer.»[10]

Profesjonelle brukere av KI-systemer er ansvarlig for å sette seg inn i instruksjonene fra tilbyderen.[11] I tillegg gjelder blant annet krav til menneskelig tilsyn, dataforvaltning, varsling, overvåking, logging og vurdering av grunnleggende rettigheter.[12] Det nærmere innholdet i disse forpliktelsene varierer fra KI-system til KI-system, og er avhengig av bruksformål og instruksjonene gitt av tilbyderen.

Menneskelig tilsyn – et delt ansvar

Ansvaret for menneskelig tilsyn mellom tilbyder og bruker er delt. På den ene siden er tilbyderen ansvarlig for å designe og utvikle et system som legger til rette for menneskelig tilsyn. KI-systemet skal i henhold til artikkel 14(1) være «designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use.» Tiltakene som tilbyderen er ansvarlig for er i hovedsak todelt, og består av innebygde tiltak, samt tiltak som er «appropriate to be implemented by the deployer.» Innebygde tiltak gjelder så fremt de er «technically feasible.»[13]

På den andre siden er brukeren ansvarlig for å føre menneskelig tilsyn med KI-systemet, i tråd med tilbyderens instruksjoner.[14] I henhold til artikkel 26(2) skal brukeren ha «the necessary competence, training and authority, as well as the necessary support.» Kravet til menneskelig tilsyn innebærer at brukeren må ha nødvendig kompetanse til å kunne forstå hvordan KI-systemet fungerer, for å kunne oppdage feil, svakheter og uforutsette hendelser.[15] Brukeren skal også ha nødvendig kompetanse til å kunne å kunne intervenere og avbryte systemet, ved behov.[16]

Tilbyderen skal altså designe systemet med innebygd menneskelig tilsyn, så fremt det er «technically feasible,» og for øvrig har brukeren ansvar for å iverksette og implementere nødvendige tiltak, i tråd med tilbyderens instruksjoner. Tilbyderen kan utvikle et system som enten krever svært høy, eller svært lav grad av menneskelig tilsyn fra brukeren. Hva som er «technically feasible» vil kunne avhenge av hvilken type maskinlæringsmetode som er benyttet, og hva som er formålet med KI-systemet. I praksis kan det bli svært komplisert å fastlegge hvor tilbyderens ansvar for menneskelig tilsyn slutter, og hvor brukerens ansvar begynner. Tilsvarende kan brukeren i varierende grad ha ansvar for dataforvaltning, varsling, overvåking og logging, avhengig av hvordan KI-systemet er designet, og hvilke instruksjoner som tilbyderen har gitt til brukeren.[17] Noen KI-systemer kan være svært brukervennlige, og kreve mindre kompetanse på brukersiden, mens andre systemer kan være mer komplekse. Både tilbyder og bruker kan bøtelegges, og holdes ansvarlig, for brudd på KI-forordningen.[18] Dette tilsier at brukeren bør gjennomgå den tekniske dokumentasjonen grundig, for å kartlegge hvilke forpliktelser brukeren har i det enkelte tilfelle.

> I praksis kan det bli svært komplisert å fastlegge hvor tilbyderens ansvar for menneskelig tilsyn slutter, og hvor brukerens ansvar begynner.

Til sammenligning, i klassisk produktregulering, slik som for eksempel forordningen om medisinsk utstyr, ligger ansvaret på produsenten og aktører i produsentleddet, slik som importører, distributører og autoriserte representanter.[19] Brukeren har selvsagt også et juridisk ansvar for forsvarlig bruk av medisinsk utstyr, i tråd med produsentens instruksjoner, men dette ansvaret er ikke direkte regulert av forordningen. Brukerens ansvar for medisinsk utstyr er regulert av nasjonal lovgivning, og i Norge er dette løst gjennom håndteringsforskriften.[20] Håndteringsforskriften er svært enkel, og angir i hovedtrekk kun at brukeren har ansvar for å følge produsentens instruksjoner, deriblant ansvar for nødvendig opplæring.[21]

Når skal rettighetsbrudd regnes som lovlig og akseptabelt?

Under KI-forordningen holder det ikke å kun følge tilbyders instruk-

9 KI-forordningen artikkl 3(4).
10 KI-forordningen definerer kun «deployer», og har ingen egen definisjon av «user». Ikke-profesjonelle brukere er ikke omfattet av forordningen, og er derfor ikke definert. I denne artikkelen bruker jeg derfor begrepet «bruker» som en betegnelse på profesjonnelle brukere («deployers»).
11 KI-forordningen Artikkel 26(1).
12 Artikkel 26 og 27.
13 Artikkel 14(3).
14 Artikkel 26(2).
15 Artikkel 14(4)(a).
16 Artikkel 14(4)(e).
17 KI-forordningen artikkel 26.
18 KI-forordningen artikkel 99(4).
19 Forordningen om medisinsk utstyr (forordning nr. 2017/745), artikkel 10-14.
20 Forskrift om håndtering av medisinsk utstyr (FOR-2013-11-29-1373).
21 Håndteringsforskriften §§ 8-12. I tillegg kommer selvsagt også den alminnelige helselovgivningen inn, med plikt til å gi forsvarlig helsehjelp.

Illustrasjon: Colourbox.com

sjoner. Brukeren har også et selvstendig ansvar for å foreta en egen vurdering av grunnleggende rettigheter.[22] Denne forpliktelsen gjelder for offentlig sektor og private tilbydere av offentlige tjenester, innenfor nærmere definert områder, deriblant bruk av biometri, tilgang til utdanning og evaluering av studenter/elever, rekruttering og evaluering av ansatte, tilgang til essensielle tjenester, samt kriminalitetsbekjempelse.[23] Oppsummert gjelder forpliktelsen for det offentlige, der private aktører i hovedsak er unntatt.

Grunnleggende rettigheter viser til EUs Charter om grunnleggende rettigheter, som til dels samsvarer med Den europeiske menneskerettskonvensjon (EMK), men ikke på alle områder. Charteret har for eksempel en særskilt rett til personvern, og ikke kun privatliv, samt et mer omfattende diskrimineringsvern enn EMK.[24] Det er også en rekke rettigheter i Charteret som ikke finnes i EMK. Charteret er del av EU-retten, men ikke EØS-retten.[25] Charteret er dermed ikke inntatt i norsk rett, men får likevel indirekte virkning gjennom KI-forordningen (og annet regelverk som viser til Charteret).

Både brukeren og tilbyderen skal gjøre en vurdering av grunnleggende rettigheter. KI-forordningen fortalepunkt nr. 48 nevner at grunnleggende rettigheter blant annet omfatter retten til menneskeverd, privatliv, familieliv, personvern, ytringsfrihet, forsamlingsfrihet, diskrimineringsvern, rett til utdanning, forbrukervern, arbeiderrettigheter, rettigheter for personer med nedsatt funksjonsevne, barns rettigheter, likestilling, miljøvern, immaterielle rettigheter, og rett til en effektiv rettstat. Dette er alle forhold som tilbyderen og brukeren mulig må vurdere før KI-systemet tas i bruk.

Kravet til å vurdere grunnleggende rettigheter reiser to vesentlige spørsmål. Det første spørsmålet er hva som skjer ved avvik mellom tilbyders og brukers vurdering. Det andre spørsmålet er hva som skal regnes som en «akseptabel» risiko for rettighetsbrudd.

Avvik mellom tilbyder og bruker

Tilbyderen skal ta grunnleggende rettigheter i betraktning ved design og utvikling av KI-systemet, og tilbyderen er forpliktet til å redusere risikoen for rettighetsbrudd.[26] Risikoreduserende tiltak kan være både produktorienterte og brukerorienterte. Et brukerorientert tiltak kan for eksempel være å forplikte brukeren til å føre menneskelig tilsyn, i tråd med tilbyderens instruksjoner. Risikoen skal reduseres eller elimineres på en slik måte at risikoen er «judged to be acceptable.»[27] Gitt at man benytter et CE-merket KI-system, og følger tilbyders instruksjoner, regnes altså risikoen for rettighetsbrudd å være «akseptabel».

Til tross for at tilbyderen allerede har gjort en vurdering, og redusert risikoen for rettighetsbrudd til et akseptabelt nivå, skal brukeren, innenfor enkelte sektorer nevnt i KI-forordningen artikkel 27, foreta en egen vurdering av grunnleggende rettigheter. Det ligger i forpliktelsens natur at brukeren vil kunne identifisere forhold som tilbyderen ikke har fanget opp. Spørsmålet som da reiser seg, er hva som gjelder ved eventuelt avvik mellom brukers og tilbyders risikovurdering av rettighetsbrudd.

Svaret, i henhold til KI-forordningen, er trolig at tilbyders risi-

22 KI-forordningen artikkel 27.

23 Kravet gjelder også for private aktører som ønsker å gjennomføre kredittvurderinger, samt for evaluering av vilkårene for livs- og helseforsikring.

24 Chartret artikkel 8 (personvern) og artikkel 21 (diskrimineringsvern).

25 Traktaten om den Europeiske Union (Lisboa-traktaten) artikkel 6.

26 Artikkel 9(2) a.

27 Artikkel 9(5).

kovurdering skal legges til grunn.[28] Brukeren er kun ansvarlig for å foreta en vurdering av grunnleggende rettigheter, men har ingen selvstendig plikt til å gjennomføre risikoreduserende tiltak på samme måte som tilbyderen. Så fremt KI-systemet er CE-merket, og brukeren følger tilbyders instruksjoner, er bruken lovlig. Men i tillegg til å følge tilbyders instruksjoner skal brukeren gjennomføre en vurdering av grunnleggende rettigheter på følgende måte:

- Brukeren skal først gi en beskrivelse av hvordan KI-systemet vil bli brukt, inkludert frekvens og tidsperiode for bruken, samt fysiske personer som vil bli omfattet av bruken.[29]

- Deretter skal brukeren gjøre en risikovurdering av hvilke konsekvenser bruken av KI-systemet kan ha for de fysiske personene som er omfattet.[30]

- Brukeren skal beskrive tiltak for menneskelig tilsyn i tråd med tilbyderens instruksjoner.[31]

- Til slutt skal brukeren beskrive tiltak som vil bli iverksatt dersom uønskede hendelser skulle inntreffe, altså i tilfelle brudd på grunnleggende rettigheter.[32]

Ved brudd på grunnleggende rettigheter skal brukeren iverksette «measures», deriblant «arrangements for internal governance and complaint mechanisms.»[33] Berørte personer skal altså få mulighet til å klage ved brudd på grunnleggende rettigheter, slik som brudd på personvernet eller diskrimineringsvernet. Det sentrale poenget med brukers vurdering av grunnleggende rettigheter er altså å identifisere berørte parter, for deretter å iverksette beredskapstiltak, i tilfelle rettighetsbrudd mot de berørte partene skulle forekomme. Det forhold at rettighetsbrudd kan forekomme er derimot akseptabelt og lovlig etter KI-forordningen, såfremt risikoen for rettighetsbrudd fra er «judged to be acceptable.»[34]

Akseptable rettighetsbrudd?

KI-forordningen er bygget opp ut fra en klassisk risikobasert tilnærming, der målet er å finne fram til et akseptabelt risikonivå. Risikoen for ulykker og skade kan aldri elimineres helt, og tilbyders ansvar er følgelig begrenset til å prioritere egnede tiltak ut fra estimert risiko for uønskede hendelser.

Denne metodikken passer dårlig på grunnleggende rettigheter, som i utgangspunktet er absolutte. En viss grad av rettighetsbrudd kan ikke veies opp mot andre fordeler, eller nedprioriteres for å redusere risikoen for andre uønskede hendelser. Ut fra et rettighetsperspektiv er ingen brudd på grunnleggende rettigheter akseptabelt. Et inngrep i rettigheter er kun lovlig gitt at bestemte kriterier er oppfylt, deriblant at inngrepet har hjemmel i lov.[35] Litt ulovlig diskriminering er ikke greit, selv om det bringer med seg fordeler. KI-systemer skal være trygge å bruke, uten fare for å bli utsatt for diskriminering eller brudd på andre grunnleggende rettigheter. Til tross for dette bygger KI-forordningen bygger på en logikk der en viss grad av rettighetsbrudd er akseptabelt, ut fra en tradisjonell produktbasert risikotilnærming. Brukeren, på sin side, er ansvarlig for å gjøre klart beredskapstiltak, deriblant klageadgang, til personer som er berørt av rettighetsbrudd. Denne forpliktelsen gjelder likevel kun for en begrenset gruppe brukere, og private aktører er i hovedsak unntatt.

Vurderingen av grunnleggende rettigheter kan tilforlatelig se ut til å mye til felles med personvernkonsekvensvurderinger etter artikkel 35 i personvernforordningen. Forskjellen er imidlertid at personvernforordningen verner om grunnleggende rettigheter. I tillegg gjelder personvernforordningen for alle behandlingsansvarlige, uten unntak for private aktører. Personvernkonsekvensvurderingen er ment å avdekke brudd eller fare for brudd på grunnleggende rettigheter, slik at behandlingsansvarlig kan justere behandlingsaktivitetene på en måte som unngår rettighetsbrudd.[36] Vurderingen av grunnleggende rettigheter etter KI-forordningen, derimot, ser ut til å akseptere risikoen for en viss mengde rettighetsbrudd eller en viss type rettighetsbrudd (så lenge risikoen er akseptabel). Ut fra en klassisk risikobasert tilnærming er alvorlighetsgrad og sannsynlighet avgjørende. Det er likevel uklart hvordan et akseptabelt rettighetsbrudd skal måles, og hvilke faktorer som skal ha avgjørende betydning.

Kanskje gir dette uttrykk for en innrømmelse om at KI-systemer ikke kommer uten en risiko for brudd på grunnleggende rettigheter, og at vi må tillate en viss mengde rettighetsbrudd dersom vi samtidig ønsker å tillate bruk av KI-systemer med høy risiko. Akkurat hvor grensen mellom det akseptable og uakseptable går, gjenstår å avklare.

Av Lars Arnesen, stipendiat ved Senter for rettsinformatikk (SERI), Universitetet i Oslo. Arnesen har tidligere jobbet som advokat i advokatfirmaet SANDS (2016–2021). Fra 2021 til 2023 har han jobbet som internadvokat i det norske helseteknologiselskapet Dignio, primært med personvern og regulatoriske spørsmål knyttet til medisinsk utstyr. Han jobber nå på et forskningsprosjekt om kunstig intelligens i helsektoren.

28 Dette utelukker ikke at brukeren likevel kan bli holdt ansvarlig for rettighetsbrudd på andre grunnlag.
29 Artikkel 27(1) a–c.
30 Artikkel 27(1) d.
31 Artikkel 27(1)e.
32 Artikkel 27(1)f.
33 Artikkel 27(1)f.
34 Artikkel 9(5).
35 Charteret om grunnleggende rettigheter, artikkel 52–54.
36 Personvernforordningen artikkel 35 nr. 7.

EDPB:s ställningstagande avseende ”samtyck eller betala” – modellen[1]

Av Fredrik Gustafsson och Francisco Stråhle

Inledning

Europeiska dataskyddsstyrelsen (European data protection board, EDPB) antog den 17 april i år ett yttrande efter en begäran enligt artikel 64.2 i dataskyddsförordningen (GDPR) från flera europeiska dataskyddsmyndigheter.[2] I yttrandet behandlas legaliteten av ”stora onlineplattformars” användning av s.k. ”samtyck eller betala”-modellen. Det är en modell som uppkommit på senare tid i ett försök att uppfylla kraven på frivillighet vid behandling av personuppgifter med stöd av samtycke som rättlig grund. Modellen har bl.a. implementerats av Meta och varit föremål för betydande debatt bland europeiska dataskyddsmyndigheter.

Bakgrund

EDPB:s yttrande kan sägas ha sin grund i EU-domstolens dom den 4 juli 2023 i mål C-252/21 (Meta v. Bundeskartellamt) där Metas rättsliga grund för behandling av personuppgifter för att tillhandahålla sina användare personanpassad reklam prövades. Domstolens ställningstagande innebär kortfattat att Metas behandling som utgångspunkt inte kan ske med stöd av fullgörande av ett avtal eller ett berättigat intresse som rättslig grund. Gällande samtycke som rättslig grund konstaterade domstolen att användarna måste kunna vägra lämna samtycke till bestämda åtgärder för behandling av personuppgifter som inte är nödvändiga för fullgörandet av avtalet och det utan att de är skyldiga att fullständigt avstå från att använda den tjänst som erbjuds av operatören av det digitala sociala nätverket. Det innebär enligt domstolen att användarna ska erbjudas ett likvärdigt alternativ som inte åtföljs av sådan behandling. Ett sådant likvärdigt alternativ kan erbjudas även mot lämplig ersättning.

Mot denna bakgrund beslutade EDPB några månader senare, efter begäran av den norska tillsynsmyndigheten[3], att instruera Irlands tillsynsmyndighet att vidta slutliga åtgärder avseende Meta och att införa ett förbud mot behandlingen av personuppgifter för beteendebaserad reklam med stöd av avtals fullgörande och berättigat intresse som rättslig grund inom hela Europeiska ekonomiska samarbetsområdet (EES). Som svar på EDPB:s beslut meddelade Meta att bolaget i stället planerade att förlita sig på samtycke som rättslig grund för dess beteendebaserade marknadsföringsverksamhet avseende användare inom EES. Det skulle ske genom att, i likhet med EU-domstolens antydningar, utforma en prenumerationsmodell där användare som inte samtycker till att dela sina personuppgifter och ta emot riktade annonser kan välja att i stället betala en månadsavgift. Modellen har kommit att kallas för ”samtyck eller betala”-modellen och bygger på att

Fredrik Gustafsson

Francisco Stråhle

> Modellen har kommit att kallas för ”samtyck eller betala”-modellen och bygger på att de registrerade ställs inför valet att antingen samtycka till att deras personuppgifter behandlas för beteendestyrd marknadsföring eller att betala för att slippa.

1 Av Fredrik Gustafsson, Partner, och Francisco Stråhle, Associate, Törngren Magnell & Partners Advokatfirma.

2 Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms.

3 Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd.

Illustrasjon: Colourbox.com

de registrerade ställs inför valet att antingen samtycka till att deras personuppgifter behandlas för beteendestyrd marknadsföring eller att betala för att slippa.

EDPB:s ställningstagande

EDPB har nu antagit ett yttrande gällande under vilka förutsättningar som ”samtycke eller betala”-modeller relaterade till beteendestyrd reklam kan implementeras av stora onlineplattformar som Meta för att uppfylla kraven på giltigt samtycke enligt GDPR. Även om EDPB inte förespråkar något absolut förbud mot sådan behandling ifrågasätts modellen. EDPB menar att det i de flesta fall inte kommer att vara möjligt för stora onlineplattformar att uppfylla kraven på giltigt samtycke om de endast ger sina användare valet mellan att samtycka till behandlingen av personuppgifter för beteendemässiga reklamändamål eller att betala en avgift.

EDPB konstaterar att personuppgifter inte är att betrakta som en handelsvara och att det finns ett behov av att förhindra att den grundläggande rätten till dataskydd omvandlas till något som den registrerade måste betala för att åtnjuta. Därför anser EDPB att det inte bör vara standard för personuppgiftsansvariga att endast erbjuda ett betalt alternativ till tjänster som innebär behandling av personuppgifter för beteendebaserad marknadsföringsändamål.

Vid utvecklingen av andra alternativ menar EDPB att stora onlineplattformar bör överväga att ge enskilda personer ett ”likvärdigt alternativ” som inte medför en avgift. Enligt EDPB bör detta fria alternativ vara utan eller med begränsad beteendebaserad reklam, t.ex. med en form av reklam som innebär behandling av färre eller inga personuppgifter. Ett sådant ytterligare alternativ kan ha betydelse vid bedömningen av samtyckets giltighet och förenkla för den personuppgiftsansvarige att visa att giltigt samtycke har inhämtats.

Utgångspunkten vid behandling av personuppgifter med stöd av samtycke som rättslig grund är att den registrerade ska ha ett genuint fritt val och inte utsättas för någon påverkan vid sitt beslutsfattande. I detta ingår att den registrerade inte får drabbas av några betydande negativa följder eller nackdelar med anledning av att denne inte lämnar sitt samtycke. I sådant fall är samtycket ogiltigt.

Av EDPB:s yttrande framgår att om användarna inte erbjuds något avgiftsfritt alternativ kan avgiften komma att betraktas som en nackdel för användarna, vilket skulle göra samtycket ogiltigt. EDPB anser att eventuella avgifter inte får vara sådana att de effektivt hindrar registrerade från att göra ett fritt val. Det ska därför betraktas som en nackdel för den registrerade om införandet av avgifter för tillgång till någon av de större onlineplattformarna skulle leda till att användare utestängs. Det gäller särskilt i de fall det är en framträdande onlineplattform eller om den är avgörande för deltagande i det sociala livet eller tillgång till professionella nätverk.

Slutord

Vi ser att framtiden för ”samtycke eller betala”-modellers utbredning i stort är fortsatt oprövad. EU-domstolens dom i Meta v. Bundeskartellamt möjliggjorde användningen av ”samtycke eller betala”-modeller. EDPB är i sitt yttrande tydlig med att inte förespråka ett absolut förbud mot att införa avgifter. EDPB framhåller att det bör bedömas i

varje enskilt fall huruvida en avgift överhuvudtaget är lämplig och vilket belopp som i så fall är lämpligt. Det får också sägas gå i linje med EDPB:s tidigare riktlinjer om samtycke. Dessa anger att samtycke endast kan vara giltigt om den registrerade får möjlighet att välja fritt och om det inte finns risk för betydande negativa konsekvenser som till exempel ”*betydande* tilläggskostnader”.[4]

Det är mot denna bakgrund inte otänkbart att nästa steg för de större plattformarna är att anpassa modellen och sänka sina avgifter i hopp om att dessa ska godtas av EU och tillsynsmyndigheterna. Oaktat hur plattformarna väljer att gå vidare med detta kommer EDPB:s ställningstagande att medföra betydande konsekvenser för stora onlineplattformar. Sådana har ofta som affärsidé att samla in stora mängder personuppgifter om sina användare och att använda dessa för individanpassad annonsering. För att säkerställa kravet på frivillighet kan plattformarna tvingas att ändra sina affärsmodeller. Skulle onlineplattformarna ta till sig EDPB:s förslag om att inrätta ett tredje alternativ utan eller med begränsad beteendebaserad marknadsföring, skulle det sannolikt innebära betydande begränsningar i dessa bolags tjänsteerbjudanden gentemot annonsörer, med lägre intäkter som följd.

> Det återstår att se hur de större onlineplattformarna och EU:s tillsynsmyndigheter väljer att hantera frågan om ”samtycke eller betala”-modeller.

EDPB:s ställningstagande är inte bindande och avser endast större onlineplattformar. Ställningstagandet kan dock ha betydelse för alla aktörer som tillhandahåller dessa typer av plattformar. Dessutom fäster Integritetsskyddsmyndigheten ofta stor vikt vid EDPB:s riktlinjer i sina vägledningar och beslut. Fram till dess att EDPB utarbetat nya riktlinjer med ett bredare tillämpningsområde som inte bara avser större onlineplattformar[5], kan ställningstagandet tillsammans med EU-domstolens praxis och EDPB:s äldre riktlinjer därför ge vägledning även för mindre plattformar.

Det återstår att se hur de större onlineplattformarna och EU:s tillsynsmyndigheter väljer att hantera frågan om ”samtycke eller betala”-modeller. Dessutom har EU-kommissionen i skrivande stund inlett en utredning mot flera större onlineplattformar gällande Metas ”samtycke eller betala”-modell i förhållande till efterlevnaden av förordningen om digitala marknader (eller mest känd på engelska som ”Digital Markets Act”).[6] Tydligt är att den juridiska terrängen för onlineplattformarnas verksamhet är under förändring och att EDPB:s ställningstagande säkerligen kommer att ge upphov till ytterligare diskussioner om beteendeanpassad marknadsföring i förhållande till de registrerades rättigheter.

Fredrik Gustafsson (partner) och Francisco Ståhle (biträdande jurist) arbetar på Törngren Magnell & Partners Advokatfirma där de är verksamma i byråns Techgrupp.

4 Riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679.

5 Se EDPB:s pressmeddelande tillgänglig här: *https://www.edpb.europa.eu/news/news/2024/edpb-consent-or-pay-models-should-offer-real-choice_en*.

6 Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster).

Kan databehandler behandle metadata om norske elever til videreutvikling?

Av Lina Breivik og Ida Thorsrud

Flere databehandlere bruker metadata til å videreutvikle tjenestene de tilbyr. Den danske Chromebook-saken viser at dette er problematisk når det gjelder metadata om skoleelever.[1] Denne artikkelen gjør rede for hvilket handlingsrom norske skoleeiere har innenfor opplæringslovens rammer, og ansvarsforholdet til databehandler.

Lina Breivik

Ida Thorsrud

Datatilsynet uttrykker at den nye opplæringsloven som etter planen trer i kraft fra august 2024, er en «unik mulighet» til å klargjøre skoleeiers handlingsrom i utviklingen av verktøy som brukes i undervisningen.[2] Kunnskapsdepartementet sier likevel at de vil «ved behov komme tilbake til dette på eit seinare tidspunkt».[3] Vi mener at behovet allerede er her, og stiller oss bak Datatilsynets oppfordring.

Behovet aktualiseres av den danske Chromebook-saken, hvor 53 danske kommuner forbys å bruke Chromebook. Det danske Datatilsynet mener at deres folkeskolelov ikke åpner opp for at databehandler kan bruke metadata til videreutvikling av produkter og tjenester om danske elever, og etterlyser en klar politisk retning.[4] I denne artikkelen utforsker vi handlingsrommet og rettssituasjonen i Norge, og hvorfor vi mener handlingsrommet til skoleeier er større i Norge enn i Danmark. Vi bruker Google Workspace for Education (GWFE) som eksempel, med standardproduktene som er inkludert (kjernetjenestene).

> I denne artikkelen utforsker vi handlingsrommet og rettssituasjonen i Norge, og hvorfor vi mener handlingsrommet til skoleeier er større i Norge enn i Danmark.

Den aktive norske eleven

Norsk skole legger opp til at eleven aktivt skal være deltakende i sin egen læring. Dette er en viktig forutsetning når skoleeier skal sette rammene for opplæring.

Med aktiv siktes det til at elever gjennom egen erfaring, både alene og i samspill med andre, skal få forståelse for kritisk og vitenskapelig tenkning. Et av hovedformålene med opplæringen er nettopp at elevene «skal få utfalde skaparglede, engasjement og utforskartrong», slik at skolen skal «opne dører mot verda og fremtida» jf. opplæringsloven (oppl.) § 1-1. At opplæringen skal legge til rette for aktive elever, er derfor en av de viktigste forutsetningene skoleeier må ta hensyn til når de anskaffer nye tjenester.

Før anskaffelse av en ny tjeneste, må skoleeier ha et formål for å kunne behandle personopplysninger. I undervisningssammenheng er dette formålet som oftest «Tilpassa opplæring» etter oppl. § 1-3, og det er dette formålet vi utforsker nær-

1 *Chromebook-saken* (journalnr. 2023-431-0001)
2 *Datatilsynets AVT – sluttrapport*, og *Prop. 57 L (2022-2023)*, s. 472
3 *Prop. 57 L*, s. 474
4 *Chromebook-saken*

mere i denne artikkelen. Opplæringen må skje i samsvar med læreplanen (§ 2-3), og skoleeier kan behandle personopplysninger så lenge det er nødvendig (§ 15-10), jf. GDPR art. 6(1) e).

Opplæringsloven er forsiktig med å sette grenser for hvilke personopplysninger som faktisk er nødvendige å bruke når og til hva. Dagens lov gir derfor en vid skjønnsmessig adgang til skoleeier, og åpner opp for at det kan være store forskjeller fra skole til skole.

Det vide handlingsrommet kan ses i sammenheng med lærerens profesjonsskjønn og lokale forhold, men også at Norge er et særlig teknologipositivt land. Opplæringsloven skal være «mest mulig teknologinøytral, det vil si et regelverk som ikke er til hinder for at det lokalt tas i bruk gode teknologiske løsninger».[5] Er regelverket for snevert, kan det stenge for gode løsninger, men er det for vidt, kan vi risikere formålsutglidning. Vi skal se nærmere på hvilke personopplysninger vi vurderer er nødvendig for å oppnå formålet, men først vil vi definere hvilke personopplysninger vi setter søkelys på i denne artikkelen.

Opplæringsloven skiller ikke mellom ulike kategorier av personopplysninger. Vi deler likevel her inn personopplysninger i to: innholdsdata og metadata. Begge er personopplysninger etter GDPR, men må ikke forveksles med hverandre. Innholdsdata er personopplysninger som elever og lærere lager eller deler selv, det kan være tekst og bilde, eller lærerens vurderinger. Metadata er data om data, eller med andre ord informasjon som beskriver egenskaper om annen informasjon. Google bruker begrepet tjenestedata.[6] Det vil bl.a. omfatte data om hvordan verktøyet brukes, posisjon og innstillinger på enheten. Slik metadata er pseudonymisert, som vil si at elever og andre kan indirekte identifiseres. I denne artikkelen ser vi kun på bruken av metadata.

Illustrasjon: Colourbox.com

Behandling av metadata til tilpasset opplæring

Kan metadata om elever behandles under opplæringslovens formål om tilpasset opplæring?

Bestemmelsen om tilpasset opplæring videreføres i ny språkdrakt uten realitetsendring fra gammel til ny opplæringslov.[7] Derfor vil presiseringen og tolkningen av lovreglene være sammenfallende, og vi bruker i stor grad de ferskeste retningslinjene for tolkingsrommet.

Den nye bestemmelsen er flyttet til § 11-1, og sier at tilpasset opplæring innebærer «at elevane får eit tilfredsstillande utbytte av opplæringa uavhengig av føresetnader, og at alle skal få utnytta og utvikla evnene sine». Forarbeidene sier at opplæringen «innanfor eit fellesskap – skal leggjast til rette på ein slik måte at alle elevar skal få så godt utbytte av opplæringa som mogleg».[8] Etter vår forståelse er det en tydeliggjøring av at alle elever skal få mulighet til å delta aktivt i opplæringen. Dette blir altså en viktig forutsetning når skoleeier skal anskaffe nye tjenester.

Digitale ferdigheter er en av de fem grunnleggende ferdighetene som elever skal læres opp i etter læreplanen. Det skal være «en naturlig del av grunnlaget for læringsarbeid både i og på tvers av faglige emner», og «gir muligheter for nye og endrede læringsprosesser og arbeidsmetoder».[9] Dette betyr at eleven selv aktivt må bruke digitale tjenester i opplæringen, som igjen kan utvide hva som er nødvendig å behandle av personopplysninger. Vi ser nærmere på dette under de ytre rammene for formålet.

Aller først betyr det, slik vi ser det, at skoleeier strategisk må velge

5 *NOU 2019: 23*, 153

6 Se Googles *personvernerklæring for GWFE*

7 *Prop. 57 L*, s. 183

8 *Prop. 57 L*, s. 180

9 *Rammeverk for grunnleggende ferdigheter del. 2.1 (Digitale ferdigheter)*

ut verktøy som legger til rette for både samhandling og individuelt arbeid for elever, og som gir lærerne mulighet til å tilpasse opplæringen etter forholdene for best mulig utbytte. Da kan vi vanskeligere slå oss til ro med verktøy som er basert på data og behov fra andre læringskulturer og syn. For å illustrere dette kan vi se til løsningen YouTube, en tilleggstjeneste som ikke er inkludert i GWFE og som er et kommersielt videoverktøy Google er behandlingsansvarlig for. For å unngå at Google behandler personopplysninger om elever til kommersielle formål, har de laget en løsning hvor lærere kan dele video-lenker med elevene i Google Classroom. Denne løsningen gjør at elever ikke har mulighet til å aktivt delta i opplæringen selv, og dekker derfor ikke det pedagogiske behovet norske skoler har.

Derfor mener vi at skoleeier må ha en langvarig strategi som tar hensyn til om tjenestene er og kan fortsette å tilpasses det norske læringssynet og behovet.[10] For å få til dette er det nødvendig at strategien bygger på et godt datagrunnlag om norske elever. Her vil vi lene oss på samme argument som Kunnskapsdepartementet bruker for at staten skal kunne innhente elevdata til å lage nasjonale strategier: «Eit godt datagrunnlag, som også inkluderer individdata, er derfor nødvendig for å sikre eit godt kunnskapsgrunnlag for nasjonale styresmakter i styring av sektoren».[11]

Sagt på en annen måte: For å oppnå formålet om tilpasset opplæring må skoleeier anskaffe digitale tjenester som tillater en aktivt deltakende elev i tråd med norsk læringssyn. Det innebærer at skoleeier må ta strategiske valg både ved anskaffelse av tjenesten og ved senere bruk, bl.a. basert på et kunnskapsgrunnlag fra metadata. Neste spørsmål blir da: Hva er de ytre rammene for databehandlers behandling av metadata?

De ytre rammene for formålet

De aller fleste leverandører bruker metadata som produseres ved bruk av tjenesten de tilbyr, og vi skal komme nærmere inn på ansvarsforholdet. Først påpeker vi at skoleeier alltid har en plikt til å sørge for at viderebehandling av elevers metadata ikke skjer på en måte som er uforenlig med det opprinnelige formålet, jf. GDPR art. 6(4) og 5(1) b). Det er dermed behov for å vurdere det ytre handlingsrommet som ligger i opplæringslovens bestemmelse om tilpasset opplæring.

For viderebehandling av metadata ser vi på disse tre formålene:

1. levering, tilgjengelighet og sikkerhet for tjenesten
2. videreutvikling av den konkrete tjenesten
3. videreutvikling av andre og nye produkter fra leverandører

Levering, tilgjengelighet og sikkerhet for tjenesten

Når en tjeneste anskaffes, plikter skoleeier etter GDPR art. 28, å sørge for å bare inngå kontrakt med en leverandør som kan etterleve personvernforpliktelsene sine. Tjenesten som velges, må også tilby sikker og tilgjengelig bruk.[12] Rammen for kravene følger av ulike lovregler, men prinsippene er grunnleggende og skal ligge i bunn av alle behandlinger av personopplysninger, etter kravet om innebygget personvern og KIT (konfidensialitet, integritet og tilgjengelig).[13]

En sikker og tilgjengelig tjeneste vil f.eks. innebære å hindre at uvedkommende får tilgang til tjenesten, men også å skjerme elever fra skadelig innhold.[14] For å få til dette kan det være nødvendig å behandle metadata som IP-adresse og lokasjon.

Ofte er det naturlig og behov for at skoleeier delegerer en del av slike behandlinger til den som leverer tjenesten. Dette henger sammen med skoleeiers valgfrihet til å velge hvilket verktøy som er best egnet til å oppnå formålet om tilpasset undervisning.

Formålet levering, tilgjengelighet og sikkerhet for tjenesten, er derfor forenlig med formålet om tilpasset opplæring.

Videreutvikling av den konkrete tjenesten

Med den konkrete tjenesten sikter vi til det eller de verktøyene som skoleeier anskaffer og kjøper lisens til. En tjeneste kan inneholde flere produkter. GWFE sine kjernetjenester består bl.a. av produktene Classroom, Dokumenter og Kalender. Videreutvikling kan f.eks. være å forbedre stavekontrollen på norsk eller identifisere hvor det er behov for å gjøre endringer for å bedre brukeropplevelsen.

Når vi ser på det opprinnelige formålet om tilpasset opplæring, har skoleeier et visst handlingsrom til å bestemme hvordan opplæringen skal foregå. Vi har drøftet hvordan og hvorfor vi mener skoleeier må ha en langvarig strategi som tar høyde for å tilby tjenester som henger med og utvikler seg med tiden. Denne argumentasjonen anerkjennes også av det danske Datatilsynet i Chromebook-saken, selv om dansk lov ikke åpner opp for det nå. Siden handlingsrommet er større etter norsk lov mener vi at denne argumentasjonen kan tas til følge hos oss, og at oppl. § 1-3 kan tolkes utvidende. Viderebehandlingen må likevel vurderes opp mot flere hensyn i tråd med GDPR art. 6(4).

10 Kunnskapsdepartementet understreker også viktigheten av å ha en god strategi for tilpasset opplæring som gagner alle i *Prop. 57 L*, s. 603-604

11 *Prop. 57 L*, s. 57

12 Selvstendige krav til sikkerhet følger av bl.a. GDPR art. 32(1) b) og eForvaltningsforskriften § 15 (2)

13 GDPR art. 5(1) f) og 32(1) b)

14 Plikt til å skjerme elever fra skadelig innhold følger av flere bestemmelser, f.eks. bildeprogramloven § 1 og oppl. § 9 A-3

Personopplysninger i skolen samles tradisjonelt primært inn for å brukes her og nå i elevens opplæring. Behandlingen kan oppleves mindre forutsigbar for elever og foreldre når opplysningene brukes til videreutviklingsformål. Samtidig vil hensynet til fellesskapet være innenfor formålets rammer slik vi tolker det, og det er en tydelig sammenheng mellom tilpasset opplæring til den enkelte elev og tilpassede verktøy til elevfellesskapet. Åpenhet om hvorfor og hvordan behandlingen foregår vil være et viktig element som bidrar til at sammenhengen blir synlig og forutsigbar.

En nødvendig garanti vil også være at det ikke er den enkelte elevs bruksmønster som skal vurderes, men datasett av elevmassen. For GWFE sin del innebærer det at opplysningene pseudonmiseres og aggregeres. Profilering av elevene og deres individuelle bruk omfattes ikke. Personopplysninger skal ikke brukes mot dem senere i livet til f. eks. atferdsbasert markedsføring, som er en viktig forutsetning påpekt av Personvernkommisjonen og som vi stiller oss bak.[15] Risiko for at elever og lærere skal endre atferd fordi de følger seg overvåket (nedkjølingseffekt), er derfor mindre. F. eks. vil et mønster i et datasett kunne være med å lokalisere en feil i systemet som må rettes. En slik behandling vil i mindre grad fremstå upåregnelig.

Vi mener derfor at formålet videreutvikling av den konkrete tjenesten, er forenlig med formålet om tilpasset opplæring.

Videreutvikling av andre produkter

For videreutvikling av andre produkter fra leverandører som skoleeier ikke har anskaffet, er det vanskeligere å se at dette er i tråd med opprinnelig formål.

Elever kan vanskelig få utfolde «skaparglede, engasjement og utforskartrong» gjennom produkter som ikke brukes av skolen, jf. oppl. § 1-1. Selv om det vil kunne tenkes å være en fordel at det utvikles flere produkter som er tilpasset det norske samfunn og som skoleeier kan velge mellom, vil argumentet om at produktene kanskje kan brukes på sikt være svært grunt. Etter vår mening ville det være å tolke skoleeiers handlingsrom for å utvikle strategier for vidt.

Å bruke metadata om elever til å utvikle produkter som verken kommer eleven eller elevfellesskapet til gode, vil samtidig ha et kommersielt aspekt som vil stride med opplæringsloven. Behandlingen vil også være lite forutberegnelighet fordi leverandør gis vide rammer til å utvikle helt nye produkter.

Formål nr. 3, videreutvikling av andre produkter fra leverandør, er derfor ikke forenlig med formålet om tilpasset opplæring.

Ansvarsforholdet mellom skoleeier og leverandør

Utgangspunkter for norske kommuner og skoleeiere er at de er behandlingsansvarlig for personopplysninger for elever, lærere og andre ansatte. Behandlingsansvarlig er den som «alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes».[16] Skoleeier vil med andre ord være behandlingsansvarlig for alle personopplysninger som behandles i skolen. Dette inkluderer metadata, og det behandlingsansvaret er ikke noe som en skoleeier kan avtale seg bort fra.

Opplæringsloven setter rammer for behandlingsansvaret. Dette betyr at norske skoleeiere ikke kan behandle personopplysninger om elever, lærere og andre ansatte på en måte som ikke er kompatibel med formålene i opplæringsloven. Opplæringsloven setter med andre ord rammer for hvilke metadata skoleeier kan behandle, hvilke metadata skoleeier kan dele med leverandøren og til hvilke formål leverandøren kan viderebehandle opplysningene til.

Større teknologiselskaper opererer noen ganger som behandlingsansvarlig for flere av tjenestene sine. For Google gjelder det f.eks. tjenestene Youtube, Google Søk og Google Maps. I utgangspunktet kan ikke norske skoleeiere bruke tjenester der Google også er behandlingsansvarlig uten å ta en vurdering av om de formålene som Google viderebehandler personopplysningene til, er kompatible med de opprinnelige formålene i opplæringsloven.[17]

Selv for tjenester der Google i utgangspunktet er databehandler, er Google behandlingsansvarlig for metadata. Sagt på en annen måte behandler Google metadata til egne formål. Det gjelder f.eks. kjernetjenester i GWFE. [18]

Google tilbyr ulike avtaler eller «terms of service» for GWFE som åpner for forskjellige løsninger for hvem som er behandlingsansvarlig for hvilke personopplysninger. Om det er skoleeier eller Google som er behandlingsansvarlig for innholdsdata avhenger i all hovedsak av hvilke tjenester skoleeier velger å bruke (kjernetjenester eller tilleggstjenester). Når det gjelder hvem som er behandlingsansvarlig for metadata, kan skoleeier ut ifra Google sin avtalestruktur velge om de ønsker å være behandlingsansvarlig, eller om Google skal være behandlingsansvarlig alene.

Som tidligere nevnt, er skoleeier behandlingsansvarlig for alle personopplysninger som behandles i skolen. Opplæringsloven skiller ikke på innholdsdata eller metadata. Sko-

15 *NOU 2022: 11*, s. 11

16 GDPR art. 4(7)

17 GDPR art. 5(1) b)

18 Dette er tilfellet for kjernetjenestene i GWFE og Chrome nettleser med Data Processor Mode på en administrert Chromebook

leeier er behandlingsansvarlig for all data som er personopplysninger. Det betyr at norske skoleeiere må velge de avtalene hvor de beholder behandlingsansvaret også for metadata.[19]

Å beholde behandlingsansvaret også for metadata vil samtidig gjøre at norske skoleeiere beholder revisjonsretten. En databehandler som Google kan i utgangspunktet ikke bruke personopplysninger til egne formål,[20] med mindre de nye formålene er kompatible med behandlingsansvarliges egne formål.[21]

Videre skal behandlingsansvarlige bare inngå avtaler med databehandlere som stiller tilstrekkelige garantier for GDPR-etterlevelse.[22] Det betyr at det er viktig for norske skoleeiere å kunne verifisere at de formålene som Google viderebehandler metadata til, er kompatible med de formålene som fremgår av opplæringsloven.

Hva er neste?

Den danske Chromebook-saken, Datatilsynets etterlysning etter tydelige lovhjemler i opplæringsloven og denne artikkelen viser at utfordringen rundt leverandørers bruk av metadata om elever til egne formål er kompleks. Problemstillingen dreier seg om skoleeiere kan ta i bruk tjenester hvor leverandøren behandler metadata til egne formål og samtidig ivaretar sitt behandlingsansvar.

Vi mener at videreutvikling av konkrete produkter som kan tilpasses norske elever og norsk skolekultur, er innenfor det opprinnelige formålet som følger av opplæringslovens bestemmelse om tilpasset opplæring. Dette er en utvidet tolkning som vi også mener er innenfor opplæringslovens opprinnelige formål, som bl.a. sier at elevene «skal få utfalde skaparglede, engasjement og utforskartrong», slik at skolen skal «opne dører mot verda og fremtida».[23]

Vi har i denne artikkelen forsøkt å gi noen rammer både for leverandørens bruk av metadata om elever til egne formål, og for hva skoleeier må være oppmerksom på ved kjøp av digitale verktøy og tjenester som brukes i skolen.

> Problemstillingen dreier seg om skoleeiere kan ta i bruk tjenester hvor leverandøren behandler metadata til egne formål og samtidig ivaretar sitt behandlingsansvar.

At en skoleeier kan kjøpe tjenester av en leverandør som bruker metadata, må ikke bli en hvilepute. Tvert imot stiller presiseringen i denne artikkelen krav til både skoleeiere og levererandører. Skoleeier på sin side må sørge for at de ikke inngår avtaler med leverandører som behandler metadata til andre formål enn de som er kompatible med formålene i opplæringsloven. Denne presiseringen kan også bli et kriterie ved revisjon av leverandøren.[24] For leverandører som leverer tjenester til skolen, setter presiseringen føringer både for hvilke personopplysninger leverandøren kan samle inn, og hva opplysningene kan brukes til.

Lina Breivik. Jurist og prosjektmedarbeider i den nasjonale Google-DPIA (KS).

Ida Thorsrud. Jurist og prosjektleder for den nasjonale Google-DPIA (KS).

19 Per denne artikkelens dato må norske skoleeiere godta «the Optional Service Data Addendum» for også å være behandlingsansvarlig for metadata som behandles i kjernetjenestene til GWFE, og godta og aktivere Data Processor Mode for å være behandlingsansvarlig for metadata som behandles i Chrome nettleser og for «essential services» i Chrome OS på en administrert Chromebook.

20 GDPR art. 4 nr. 8 og art. 28(3) a)

21 GDPR art. 5(1) b)

22 GDPR art. 28(1)

23 Oppl. § 1-1

24 GDPR art. 28(3) h)

Har behandlingsgrunnlaget betydning for hvorvidt en registrert skal få gjennomslag for retten til å protestere?

Av Ingrid Hestnes og Ida Thorsrud

Er det en forskjell på vurderingen av om det foreligger «tvingende berettigede grunner» i GDPR artikkel 21 ut ifra om behandlingsgrunnlaget er GDPR artikkel 6(1) e) eller GDPR artikkel 6(1) f)? I denne artikkelen argumenterer vi for at det er en presumsjon for at det foreligger «tvingende berettigede grunner» når behandlingsgrunnlaget er GDPR artikkel 6(1) e).

Ingrid Hestnes

Ida Thorsrud

Innledning

Retten til å protestere er en av de vanskeligste rettighetene for behandlingsansvarlig å ta stilling til. Dette fordi det er en rettighet som den registrerte kan påberope seg og få gjennomslag for *selv om* behandlingen er lovlig. Resultatet av at den registrerte får gjennomslag for protesten vil i utgangspunktet være at den behandlingsansvarlige må slette den registrertes personopplysninger, altså stoppe behandlingen av personopplysningene til den registrerte som har protestert.

Sagt på en annen måte, den behandlingsansvarlig kan ha et gyldig behandlingsgrunnlag, ha iverksatt alle nødvendige risikoreduserende tiltak etter GDPR artikkel 32 og ivaretatt alle krav til personvern, og *likevel* må den behandlingsansvarlige slette den registrertes personopplysninger hvis protestesten har blitt tatt til følge. Det er derfor viktig å forstå når en protest skal tas til følge, og når den ikke kan lede frem.

Dette gjelder særlig for behandlingsansvarlige som er offentlige virksomheter og som bruker GDPR artikkel 6(1) e) som behandlingsgrunnlag. Disse behandlingsansvarlige kan stå i en posisjon hvor de er pålagt å utføre en oppgave i allmennhetens interesse i henhold til nasjonal rett,[1] men likevel vil måtte ta stilling til en protest.

I denne artikkelen forsøker vi å svare på spørsmålet om vurderingen det foreligger «tvingende berettigede grunner» blir forskjellig etter hvilket behandlingsgrunnlag behandlingen baserer seg på.

1 Også kalt «supplerende behandlingsgrunnlag»

Problemstillingen

Den registrerte har en rett til å protestere av grunner knyttet til vedkommendes særlige situasjon etter GDPR artikkel 21(1). At den registrerte er i en «særlig situasjon» er med andre ord en forutsetning for retten til å protestere.

> I denne artikkelen forsøker vi å svare på spørsmålet om vurderingen det foreligger «tvingende berettigede grunner» blir forskjellig etter hvilket behandlingsgrunnlag behandlingen baserer seg på.

Retten til å protestere forutsetter også at behandlingsgrunnlaget er GDPR artikkel 6(1) e) «en oppgave i allmennhetens interesse eller utøvelse av offentlig myndighet» eller

GDPR artikkel 6(1) f) «berettiget interesse». Hvis en behandlingsansvarlig skal avvise en protest, må den vise at det foreligger «tvingende berettigede grunner for behandlingen som går foran den registrertes interesser».[2]

Når behandlingsgrunnlaget er berettiget interesse,[3] er det forholdsvis enkelt å forstå hvordan vurderingen av om det foreligger «tvingende berettigede grunner» skal gjøres. Behandlingsgrunnlaget berettigede interesser er allerede en interesseavveining, og det vil foreligge «tvingende berettigede grunner» hvis interessen til den behandlingsansvarlige står spesielt sterkt sett opp mot den registrertes særlige situasjon.

Vurderingen av hva «tvingende berettigede grunner» er når behandlingsgrunnlaget er «en oppgave i allmennhetens interesse eller utøvelse av offentlig myndighet»,[4] er mer uklart.

GDPR artikkel 6(1) e) er det behandlingsgrunnlaget offentlige organer som hovedregel bruker for sine behandlinger av personopplysninger når de er pålagt oppgaver med hjemmel i lov. Det som skiller dette behandlingsgrunnlaget fra GDPR artikkel 6(1) c) «rettslig forpliktelse», er at det offentlige organet er gitt forholdsvis stor frihet i å bestemme hvordan oppgaven de er pålagt skal løses. Den behandlingsansvarlige kan med andre ord være i en situasjon hvor den ikke kan velge å *ikke* gjøre den oppgaven den er pålagt, men kan bestemme *hvordan* den skal løses. Den behandlingsansvarlige kan for eksempel bestemme hvilke midler eller verktøy den skal bruke for å løse den lovpålagte oppgaven.

Hvis en registrer har en særlig situasjon som tilsier at en behandling bør stoppe, vil den behandlingsansvarlige som hovedregel måtte stoppe behandlingen.[5] Det betyr at den behandlingsansvarlige vil kunne komme i en situasjon hvor den på en og samme tid både må løse den lovpålagte oppgaven, og samtidig ikke behandle personopplysningene til den registrerte som har protestert.

Den behandlingsansvarlige trenger imidlertid ikke å gi den registrerte gjennomslag for protesten dersom det foreligger «tvingende berettigede grunner»[6].

Problemstilling: Hvordan skal en behandlingsansvarlig vurdere om det foreligger «tvingende berettigede grunner» og om en protest dermed ikke skal tas til følge når behandlingsgrunnlaget er GDPR artikkel 6(1) e)?

Hensynet bak retten til å protestere

I henhold til GDPR artikkel 21(1), har den registrerte rett til å protestere mot behandling av personopplysninger om vedkommende som har grunnlag i GDPR artikkel 6(1) e) eller f) av grunner knyttet til vedkommendes særlige situasjon. Den behandlingsansvarlige skal ikke lenger behandle personopplysninger om den som har protestert, med mindre det foreligger «tvingende berettigede grunner» for å fortsette behandlingen av personopplysningene.

Den registrerte har bare rett til å protestere når personopplysninger blir behandlet med grunnlag i GDPR artikkel 6(1) e) eller f). Det vil si at den behandlingsansvarlige anser behandlingen av personopplysninger som nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,[7] eller av hensyn til den behandlingsansvarliges eller en tredjeparts berettigede interesser.[8]

Med andre ord er det gjennomført en interessevurdering i forkant av behandlingen, der den behandlingsansvarlige har kommet frem til at de interessene som begrunner behandlingen, det vil si allmennhetens interesse, offentlige interesser eller andre berettigede interesser, veier tyngre enn de ulempene som den registrerte generelt må antas å ha av behandlingen.

Interessevurderingen som gjøres for behandlinger med grunnlag i GDPR artikkel 6(1) e) og f) kan begrunne hvorfor den registrerte ikke har rett til å protestere mot behandlinger som har grunnlag i et av de øvrige behandlingsgrunnlagene i GDPR artikkel 6.

Dersom den registrerte har samtykket til behandling av personopplysninger etter GDPR artikkel 6(1) a), kan hen til enhver tid trekke tilbake samtykket. Behandlingen av personopplysninger skal da stoppe uten at den registrerte må begrunne dette i sin «særlige situasjon».

Dersom det er nødvendig å behandle personopplysninger for å oppfylle en avtale som den registrerte er part i etter GDPR artikkel 6(1) b), må det antas at det ikke er konflikt mellom den registrerte og den behandlingsansvarlige sine interesser i å gjennomføre avtalen.

Videre må det legges til grunn at lovgiver har gjort en interessevurdering av hensynene for og imot en behandling når behandlingsgrunnlaget er nødvendig for å oppfylle en rettslig plikt etter GDPR artikkel 6(1) c).

Det må også antas at den behandlingsansvarlige har «tvingende berettigede grunner» for å gjennomføre en behandling som er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser det er nødvendig etter GDPR artikkel 6(1) d). Det vil dermed ikke være hensiktsmessig med en rett til å protestere i disse tilfellene.

I tillegg til at GDPR artikkel 6(1) e) og f) krever at den behandlingsansvarlige har vurdert at det er in-

2 GDPR artikkel 21(1)
3 GDPR artikkel 6(1) f)
4 GDPR artikkel 6(1) e)
5 GDPR artikkel 21(1)
6 GDPR artikkel 21(1)
7 GDPR artikkel 6(1) e)
8 GDPR artikkel 6(1) f)

teresseovervekt for å gjennomføre behandlingen, kan også retten til å protestere begrunnes i behandlingsgrunnlagenes karakter. I motsetning til de andre behandlingsgrunnlagene, som gjerne gir grunnlag for å behandle personopplysninger om en bestemt registrert, gir GDPR artikkel 6(1) e) og f) typisk behandlingsgrunnlag for behandling av personopplysningene til en større gruppe av mennesker. Selv om allmennhetens interesser, offentlige interesser eller andre berettigede interesser gir lovlig grunnlag for å behandle personopplysninger, kan det være særlige forhold ved enkelte registrerte som veier tyngre enn interessene for behandlingen. Denne forståelsen støttes også av fortalen til GDPR punkt 69:

> *«Dersom personopplysningene kan behandles på lovlig vis fordi behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt, eller av hensyn til en behandlingsansvarligs eller en tredjeparts berettigede interesser, bør en registrert imidlertid ha rett til å protestere mot enhver behandling av personopplysninger som gjelder vedkommendes særlige situasjon. Det bør være opp til behandlingsansvarlige å påvise at vedkommendes tvingende berettigede interesse går foran den registrertes interesser eller grunnleggende rettigheter og friheter.»*

Interesseavveining i GDPR artikkel 21(1)

For å svare på hvorvidt det foreligger en «tvingende berettiget grunn»,[9] må den behandlingsansvarlige foreta en interesseavveining. Dette er en konkret skjønnsmessig vurdering hvor den behandlingsansvarliges interesser i å fortsette behandlingen veies opp mot den registrerte som har protestert sin særlige situasjon og interesse i at behandlingen skal opphøre.

Det er den behandlingsansvarlige som har bevisbyrden i denne interesseavveiningen. Det vil si at det er den behandlingsansvarlige som må godtgjøre at det faktisk foreligger en «tvingende berettiget grunn» slik at protesten kan avvises.[10]

For å kunne bruke berettiget interesse som behandlingsgrunnlag, må den behandlingsansvarlige allerede ha gjort en interesseavveining der resultatet av vurderingen ble at den behandlingsansvarliges interesser i å gjennomføre behandlingen veide tyngre enn personvernulempene for den registrerte.

Ordlyden «tvingende» i GDPR artikkel 21(1) «tvingende berettigede grunn», tilsier at det skal vesentlig mer til for at den behandlingsansvarlige skal kunne påberope seg dette unntaket, sammenlignet med interesseavveiningen for å fastslå at det foreligger en «berettiget interesse» i GDPR artikkel 6(1) f). For at noe skal være en berettiget interesse, holder det med noe mer enn en alminnelig interesseovervekt, mens det vil være strengere krav for at noe skal være en «tvingende berettigede grunn».[11]

Article 29 Working Partys «Guidelines on Automated Individual Decision-Making»[12] støtter denne forståelsen:

Illustrasjon: Colourbox.com

9 GDPR artikkel 21(1)

10 Dette forutsetter at den registrerte har gjort den behandlingsansvarlige oppmerksom på sin «særlige situasjon», og at protesten ikke skjer på bakgrunn av generelle motforestillinger mot behandlingen.

11 Denne forståelsen støttes også av Oxfords lovkommentar til artikkel 21 i GDPR, hvor Zanfir-Fortuna argumenterer for at «tvingende grunner» («compelling») betyr at de berettigede interessene må være «overwhelming» og overgå de registrertes interesser «in a strong, significant way»

12 Dette er en veileder som *EDPB har godkjent i sitt første møte 25. mai 2018*

«It is clear from the wording of Article 21 that the balancing test is different from that found in Article 6(1)(f). In other words, it is not sufficient for a controller to just demonstrate that their earlier legitimate interest analysis was correct. This balancing test requires the legitimate interest to be compelling, implying a higher threshold for overriding objections.»

Unntak fra retten til å protestere når behandlingen er vitenskapelige, historiske eller statistiske formål som skjer i allmennhetens interesse

Det er ingen ting i selve ordlyden i GDPR artikkel 21(1) som tilsier at det skal være en forskjellig standard for vurderingen av en protest skal tas til følge ut ifra om behandlingsgrunnlaget er GDPR artikkel 6(1) e) eller GDPR artikkel 6(1) f).

Imidlertid fremgår det av GDPR artikkel 21(6) at retten til å protestere på behandlinger hvor personopplysninger behandles for vitenskapelig eller historisk forskning, og statistiske formål faller bort når behandlingen er «nødvendig for å utføre en oppgave i allmennhetens interesse». GDPR inneholder med andre ord et unntak fra retten til å protestere for forskning og statistikk når dette gjøres i allmennhetens interesse.

Det taler for at en behandling som skjer i allmennhetens interesse etter GDPR artikkel 6(1) e), enklere også vil oppfylle kravet til «tvingende berettigede grunn» enn når behandlingsgrunnlaget er en alminnelig interesseavveining i GDPR artikkel 6(1) f).

En behandling som gagner samfunnet som helhet – hensynet til allmennhetens interesse

Hensynet til allmennhetens interesse ved en behandling av personopplysninger, er relevant for vurderingen av om det foreligger en «tvingende berettigede grunn». Dette fremgår blant annet av Article 29 Working Partys «Guidelines on Automated Individual Decision-Making». Veilederen slår fast at GDPR ikke inneholder en forklaring på hva som ligger i «tvingende berettigede grunner».

Imidlertid konstaterer veilederen at behandlinger av personopplysninger som kommer samfunnet til gode kan være et eksempel på at det foreligger «tvingende berettigede grunner»:

«It may be the case that, for example, the profiling is beneficial for society at large (or the wider community) and not just the business interests of the controller, such as profiling to predict the spread of contagious diseases.»[13]

En behandling som er hjemlet i behandlingsgrunnlaget i GDPR artikkel 6(1) e), er en behandling som er «nødvendig for å utføre en oppgave i allmennhetens interesse». Hvis en slik behandling kommer samfunnet som helhet til gode, vil det i seg selv tale for at det foreligger en «tvingende berettigede grunn».

Presumsjon for at lovgiver har hensyntatt personvern

Krav i utredningsinstruksen

Det er flere forskjeller på en behandling som har hjemmel i nasjonal lovgivning, og en som er bruker berettigede interesser som behandlingsgrunnlag. I en demokratisk rettsstat som Norge, er det for det første satt føringer i utredningsinstruksen med veiledninger[14] for utredningene som ligger til grunn for lovgivningsprosessen. Utredningsinstruksen 2-1 inneholder seks spørsmål som alltid skal vurderes i forbindelse med en utredning. Det fremgår av kapittel 2 til veiledningen til utredningsinstruksen[15] at personvern faller inn under spørsmål 3 om hvilke prinsipielle spørsmål som tiltakene reiser. Veilederen beskriver at «prinsippspørsmål kan for eksempel gjelde den enkeltes personvern og integritet».

I 2008 ble det utarbeidet et eget tillegg til veiledningen til utredningsinstruksen om hvordan utreder skulle vurdere personvernkonsekvenser som en del av lovgivnings- og utredningsprosessen. Det fremgår av denne veiledningen at hvor inngripende forskjellige tiltak og lovendringer vil være for personvernet særlig skal utredes.

Videre skal det tas hensyn til forholdsmessighet.[16] Det vil si at de personopplysninger som behandles skal stå i forhold til formålet med behandlingen, og må være egnet til å oppfylle det. Dersom formålet kan oppfylles på andre måter som ikke innebærer å behandle personopplysninger, vil kravet til forholdsmessighet ikke være nådd. Selv om dette tillegget til veiledningen er flere år gammelt, er det også et uttrykk for den forpliktelsen som lovgiver har for å vurdere personvernkonsekvenser i lovgivningsprosessen.

Både utredningsinstruksen, veilederen til utredningsinstruksen og veilederen om personvernkonsekvenser inneholder krav om at personvernspørsmål skal utredes i forbindelse med lovgivningsarbeidet der det er relevant. Særlig veilederen om personvernkonsekvenser understreker flere steder at personvernvurderingen skal ta hensyn til den enkeltes rett til personvern.[17] Det betyr at lovgiver skal ha vurdert relevante personvernspørsmål da lo-

13 Article 29 Working Partys Guidelines on Automated Individual Decision-Making s. 18

14 Utredningsinstruksen (FOR-2016-02-19-184) punkt 1-2

15 Veileder til utredningsinstruksen – instruks om utredning av statlige tiltak, Direktoratet for Økonomistyring (DFØ), 2018

16 *Vurdering av personvernkonsekvenser, Fornyings- og administrasjonsdepartementet, 2008* s. 15

17 *Vurdering av personvernkonsekvenser, Fornyings- og administrasjonsdepartementet, 2008* s. 6, 9, 10, 11 og 12

ven ble skrevet. Det taler for at det er enklere å anta at det foreligger «tvingende berettigede grunner» for en behandling som hjemlet i nasjonal lovgivning[18] sammenlignet med en hjemlet i «berettigede interesser».[19]

Demokratisk prosess

Når en behandling av personopplysninger har hjemmel i nasjonal lovgivning, har den videre vært gjenstand for en demokratisk prosess. I denne prosessen skal «berørte departementer involveres så tidlig som mulig i utredningsprosessen».[20]

Videre fremgår det av utredningsinstruksen at «ansvarlig departement skal forelegge alle forslag til tiltak med vesentlige virkninger for berørte departementer»[21].

Veiledningen til utredningsinstruksen kapittel 3 som gir veiledning om prosesskrav sier videre at «dersom tiltak som utredes vil medføre vesentlige virkninger for forholdet til personvern, skal saken forelegges Kommunal- og moderniseringsdepartementet».

Dette er tydelige krav som skal sikre at personvern særlig hensyntas i lovprosesser. Dette taler også for at personvernspørsmål er særlig hensyntatt i behandlinger som har hjemmel i lov.[22]

Lovgivningsprosesser er i tillegg gjenstand for offentlige høringer. Det fremgår av utredningsinstruksen at «utredninger, forslag til lov og forskrift til tiltak med vesentlige virkninger skal normalt legges ut på høring».[23]

Dette betyr at lovgiver vil få innspill fra det sivile samfunn, andre offentlige organer og private virksomheter om hvordan endringer i lovgivning vil påvirke dem på forskjellige måter. Det er grunn til å tro at personvernspørsmål vil være en del av slike høringer.

> Konklusjonene i denne artikkelen betyr imidlertid ikke at behandlingsansvarlig kan legge til grunn at det alltid foreligger «tvingende berettigede grunner» når en registrert protesterer på en behandling som har hjemmel i GDPR artikkel 6(1) e).

Konklusjon

I denne artikkelen har vi undersøkt hvordan det spesifikke behandlingsgrunnlaget påvirker vurderingen av den registrertes rett til å protestere i GDPR artikkel 21(1). Vi har argumenterer for at det er en presumsjon for at det foreligger «tvingende berettigede grunner» når behandlingsgrunnlaget er GDPR artikkel 6(1) e) som omhandler oppgaver i allmennhetens interesse eller utøvelse av offentlig myndighet.

Sagt på en annen måte er det en presumsjon for at det finnes «tvingende berettigede grunner» som kan rettferdiggjøre fortsatt behandling av personopplysninger når behandlingsgrunnlaget er GDPR artikkel 6(1) e).

Denne konklusjonen er støttet av den viktige rollen offentlige organer spiller i å oppfylle oppgaver pålagt av lov, hvor de må balansere nødvendigheten av å utføre disse oppgavene mot individets rett til personvern. Dette i motsetning til behandlinger basert på «berettiget interesse» i 6(1) f).

Konklusjonene i denne artikkelen betyr imidlertid ikke at behandlingsansvarlig kan legge til grunn at det alltid foreligger «tvingende berettigede grunner» når en registrert protesterer på en behandling som har hjemmel i GDPR artikkel 6(1) e). En viktig forutsetning er at det supplerende behandlingsgrunnlaget gjelder en behandling som faktisk skjer i «allmennhetens interesse».

Den behandlingsansvarlige må fortsatt også dokumentere at den har gjort en konkret skjønnsmessig vurdering hvor den enkelte registrertes spesielle forhold veies opp mot interessene den behandlingsansvarlige har til å fortsette behandlingen. Dette er spesielt viktig når «tvingende berettigede grunner» påberopes og protesten avvises.

Ingrid Hestnes. Jurist, Bergen kommune

Ida Thorsrud. Jurist og prosjektleder for den nasjonale Google-DPIA (KS)

18 GDPR 6(1) e)
19 GDPR 6(1) f)
20 Utredningsinstruksen kapittel 3, punkt 3-1(1)
21 Utredningsinstruksen kapittel 3, punkt 3-2(1)
22 GDPR artikkel 6(1) e)
23 Utredningsinstruksen kapittel 3, punkt 3-3(1)

Likhetsnormer som rettslig skranke for utviklingen av KI i helsehjelp

Av Julia Desiré Fuglestad Brodshaug

På tvers av rapporter beskrives kunstig intelligens (KI) som en teknologi med omfattende virkeområde, med et potensial det er vanskelig å se konsekvensene av. KI kan i dag brukes i helsehjelp på flere måter, herunder ved å gi beslutningsstøtte, forbedre diagnostikk og automatisere repetitive oppgaver. Teknologien kan brukes til planlegging og prioritering, slik at helsepersonell kan konsentrere seg om de pasientene som trenger det mest. Selv om en slik bruk og utvikling av KI innen helsesektoren har et enormt potensial, er den imidlertid ikke uten utfordringer. Spørsmålet i det følgende blir hvordan likhetsnormer kan brukes som en rettslig skranke for utviklingen av KI i helsehjelp.

Artikkelen vil i det følgende gjøre rede for fordommer i KI-systemer i helsehjelp, forsvarlighetskravet (herunder kravet til likebehandling av pasienter), samt motstridende argumenter knyttet til bruk av sensitive opplysninger i den videre utviklingen av KI i helsehjelp.

Fordommer i KI-systemer som ikke ser forskjell på rett og galt

Ved utviklingen av KI-systemer knyttet til behandling og diagnostikk, kan det oppstå skjevheter i befolkningens helsetilbud, og ulikheter når det kommer til hvem som får motta forsvarlig helsehjelp[1]. Grunnen til dette er at eksisterende bevisste og ubevisste fordommer kan

Julia Desiré Fuglestad Brodshaug

forsterkes ved bruk og utvikling av digitale systemer som ikke ser forskjell på rett og galt (algoritmisk forskjellsbehandling). Forsvarlighetskravet, herunder kravet til likebehandling av pasienter, vil imidlertid kunne utgjøre en skranke for en slik utvikling.

> Spørsmålet i det følgende blir hvordan likhetsnormer kan brukes som en rettslig skranke for utviklingen av KI i helsehjelp.

Forsvarlig utvikling av kunstig intelligens

Retten til liv og beskyttelse mot skader følger av Grunnloven § 93 og EMK artikkel 2. Disse prinsippene danner en ytre ramme som skal verne mennesker mot unødvendig smerte og lidelse. I forlengelse av denne rammen finner man forsvarlighetskravet, herunder kravet til likebehandling av pasienter. Denne sier noe om hva som til enhver tid kan forventes ved behandlingen av både mennesket og helseopplysningene deres[2].

Kravet om likebehandling av pasienter kommer videre til syne i en rekke lovbestemmelser. Det følger av pbrl. § 1-1 at formålet med loven er å bidra til å sikre befolkningen «lik tilgang på tjenester av god kvalitet». I spesialisthelsetjenesteloven (heretter «sphl.») følger det av § 1-1 at et av lovens formål er å bidra til et «likeverdig» tjenestetilbud. Videre er retten til helse regulert i blant annet FNs konvensjon om rettighetene til mennesker med nedsatt funksjonsevne (CRPD) artikkel 25, og innebærer en plikt til likebehandling. Forbudet mot diskriminering følger av Grunnloven § 98 og EMK artikkel 14.

Hva gjelder det nærmere innholdet i forsvarlighetskravet, følger det av helsepersonelloven (heretter «hpl.») § 4 at alt «helsepersonell» plikter å yte forsvarlig «helsehjelp». Med helsepersonell menes leger og andre som yter helsehjelp, jf. hpl. § 3 første ledd. Begrepet «helsehjelp» sikter til «handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende, rehabiliterende eller pleie- og omsorgsformål, og som er utført av helsepersonell». Etter sin ordlyd setter bestemmelsen noen viktige avgrensninger for hva som skal regnes som «helsehjelp». Det er snakk om to hovedvilkår, henholdsvis knyttet til innhold og personell. Det er klart at mange KI-systemer, slik de brukes innen helse i dag, faller inn under denne definisjonen.

1 Anne Kjersti Befring mfl., *Kunstig intelligens og big data i helsesektoren – rettslige perspektiver,* 1. utgave, Gyldendal 2020, s. 102.

2 Anne Kjersti Befring, *Helseretten*, 1. utg, Cappelen Damm akademisk 2022, s. 140.

Videre fremkommer det av hpl. § 4 at hva som er forsvarlig vil avhenge av hva som kan «forventes» etter en vurdering av «helsepersonellets kvalifikasjoner, arbeidets karakter og situasjonen for øvrig». Etter sin ordlyd tar bestemmelsen sikte på en skjønnsmessig vurdering.

Det er en rekke momenter og samfunnsforhold som vil kunne bidra til å skape en forventning til hvordan helsepersonell skal opptre[3]. Utviklingen innen medisinsk kunnskap, og fremveksten av nye digitale hjelpemidler, vil kunne føre til at det som var forsvarlig før er uforsvarlig i dag.

Det dynamiske innholdet i forsvarlighetskravet utdypes nærmere i Ot.prp. nr. 13 (1998–99) på side 216. Der fremheves det at begrepet «forsvarlighet» viser til en rettslig standard, hvor det er inntatt en distinksjon mellom helsepersonellets kvalifikasjoner og forholdene ellers. Med begrepet «kvalifikasjoner» siktes det til at ulike krav kan stilles ut ifra helsepersonellets faglige kompetanse. Dette innebærer at helsepersonell plikter å holde seg faglig oppdatert, og innrette seg etter krav til utstyr og legemidler basert på forskning. I sammenheng med fremveksten av kunstig intelligens, innebærer kravet til forsvarlighet dermed at helsepersonell plikter å holde seg oppdatert på utviklingen, og sette seg inn i bruken av kunstig intelligens. Forsvarlighetskravet innebærer at KI-systemer skal brukes på sin tiltenkte måte, på lik linje med at medisiner skal benyttes til det de er godkjent til.

Forvarlighetsplikten gjelder alle ledd i helsehjelpen[4]. Herunder alle hjelpemidler som tas i bruk i helsehjelp. Dette er relevant i forhold til KI-systemer innen helse, ettersom også en slik type teknologi på denne måten vil underlegges forsvarlighetskravet.

Datamønstre med fordommer

Overordnede rettslige prinsipper om forsvarlighet, herunder likebehandling av pasienter, har betydning for alle andre regelverk, herunder også for bruken av personopplysninger etter GDPR. For å kunne utvikle kunstig intelligens, samt å benytte maskinlæring, kreves det omfattende informasjon fra individer. Når slik informasjon hentes inn i stort omfang, øker risikoen for at det skjer en kategorisering av mennesker etter ulike egenskaper[5]. Grunnen til dette er at KI-systemer brukes på en slik måte at de finner mønstre i store mengder data. Disse mønstrene påvirkes av menneskelige fordommer, ettersom KI-systemer vil påvirkes av hvilke data som tas i bruk, og hvilke resultater som ønskes[6].

Eksempelvis kan bruk og utvikling av data-drevne algoritmer innen helsehjelp potensielt forevige og forsterke eksisterende etnisk diskriminering basert på hudfarge[7]. I en analyse gjort av Obermeyer et al. i USA, ble det avdekket at kunstig intelligens favoriserte hvite pasienter i vurderingen av hvilke pasienter som trengte potensielt fordelsaktive omsorgsprogrammer[8]. Dette til tross for at pasientene med ulik hudfarge hadde samme omfang av kroniske lidelser. Et slikt problem kan muligens knyttes til hvilke premisser («labels») og bilder man mater en algoritme med[9].

Et annet eksempel er hvordan utviklingen av KI-systemer innen helse potensielt kan forsterke en allerede eksisterende forskjell mellom helsehjelpen gitt til ulike kjønn. I tilfeller med lever-sykdommer rapporterer Vatsalya et al. om at kvinner oftere enn menn blir feildiagnostisert som friske av kunstig intelligens-systemer[10]. I praksis vil dette si at det er mange kvinner med lever-sykdom ikke får forsvarlig helsehjelp. Algoritmen som i stor utstrekning brukes for å oppdage og forutse lever-sykdom heter ILPD («The Indian Liver Patient Dataset»), og er klasssifisert som en av de mest effektive modellene på markedet[11]. Samtidig er dette en av modellene som i stor grad feildiagnostiserer kvinner. Dette problemet strekker seg til mange andre helseområder hvor kunnskapen om syk-

3 Hauglid, Mathias, «Karnov lovkommentar til helsepersonelloven.», Lovdata Pro, 2023, § 4 note 1. (lest 31.08.2023).

4 Anne Kjersti Befring mfl., *Kunstig intelligens og big data i helsesektoren – rettslige perspektiver,* 1. utgave, Gyldendal 2020, s. 405.

5 Anne Kjersti Befring mfl., *Kunstig intelligens og big data i helsesektoren – rettslige perspektiver,* 1. utgave, Gyldendal 2020, s. 103.

6 Heather Broomfield, Mona Naomi Lintvedt, «Snubler Norge inn i en algoritmisk velferdsdystopi?», *Tidsskrift for velferdsforskning,* 2022, s. 1–15, på s. 5. *https://doi-org.ezproxy.uio.no/10.18261/tfv.25.3.2.*

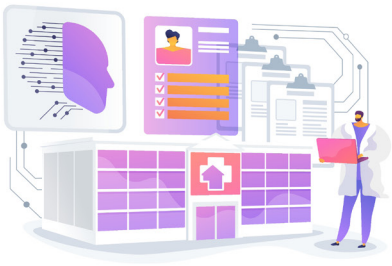
7 Jenna Wiens, W. Nicholson Price II, Michael W. Sjoding, «Diagnosing bias in data-driven algorithms for healthcare», *Naturemedicine*, 2020 s. 25–26. https://doi.org/10.1038/s41591-019-0726-6.

8 Jenna Wiens, W. Nicholson Price II, Michael W. Sjoding, «Diagnosing bias in data-driven algorithms for healthcare», *Naturemedicine*, 2020 s. 26. *https://doi.org/10.1038/s41591-019-0726-6*.

9 Jenna Wiens, W. Nicholson Price II, Michael W. Sjoding, «Diagnosing bias in data-driven algorithms for healthcare», *Naturemedicine*, 2020 s. 25–26. *https://doi.org/10.1038/s41591-019-0726-6*.

10 Isabel Straw og Honghan Wu, «Investigating for bias in healthcare algorithms: a sex-stratified analysis of supervised machine learning models in liver disease prediction», *BMJ Health & Care Informatics,* 2022 s. 1–8, på s. 1. doi: 10.1136/bmjhci-2021-100457.

11 Isabel Straw og Honghan Wu, «Investigating for bias in healthcare algorithms: a sex-stratified analysis of supervised machine learning models in liver disease prediction», *BMJ Health & Care Informatics,* 2022 s. 1–8, på s. 1. doi: 10.1136/bmjhci-2021-100457.


Illustrasjon: Colourbox.com

dom ikke tar utgangspunkt i de fysiologiske ulikhetene mellom kjønn[12]. I et likhetsperspektiv er dette svært problematisk, og kan føre til at pasienter med samme sykdom, får ulik helsehjelp.

Burde sensitive opplysninger brukes i utviklingen av KI-systemer i helsehjelp?

Et viktig poeng i sammenheng med likebehandling av pasienter, er at en algoritmisk forskjellsbehandling gjenspeiler en forskjellsbehandling som allerede finnes i helsevesenet. Et reflektert forhold til data og fordommer i utviklingen av kunstig intelligens, har dermed også potensialet til å fremme likebehandling av pasienter og hindre diskriminering[13]. Likhetsnormer som skranke for utviklingen av kunstig intelligens vil kunne føre til at helsetilbudet utvikles på en måte som gir den enkelte pasient et forsvarlig tilbud om helsehjelp, samt en forsvarlig behandling av sine personopplysninger[14].

> Et reflektert forhold til data og fordommer i utviklingen av kunstig intelligens, har […] potensialet til å fremme likebehandling av pasienter og hindre diskriminering.

Når dette er sagt, kan det oppstå en del motstridende argumenter i sammenheng med likhetsnormer som skranke for utviklingen av KI-systemer innen helse. En likhetsnorm kan på den ene siden tale for at sensitive opplysninger knyttet til etnisitet eller kjønn ikke burde brukes i utviklingen av KI-systemer. På den andre siden kan normen tale for at nettopp slike opplysninger burde brukes i utviklingen av KI-systemer, for å kunne sikre et forsvarlig helsetilbud med økt kunnskap om sykdomssituasjonen til marginaliserte grupper.

Videre kan prinsippet om likebehandling av pasienter føre til et økt fokus på fordelingsmekanismer og flere krav til hvordan helseopplysninger skal behandles i utviklingen av KI-systemer. På den andre siden kan dette imidlertid komme i strid med effektivitetshensyn, og potensielt gjøre det vanskeligere å ta i bruk helseopplysninger for å oppnå en effektiv utvikling.

Konklusjon

For å konkludere, er det ikke alltid like lett å forutse konsekvensene av utviklingen av KI-systemer innen helse, noe som kan gjøre det utfordrende å sikre effektiv og fortløpende likebehandling av pasienter. Denne artikkelen har vist hvordan likhetsnormer kan brukes som en skranke for utviklingen av KI i helsehjelp. Den har fremhevet sentrale mostridende argumenter rundt bruk av sensitive opplysninger i utviklingen av KI-systemer, og er ment som et utgangspunkt for rettslig diskusjon i tiden som kommer.

Julia Desiré Fuglestad Brodshaug jobber som jurist i Helfo.

12 Isabel Straw og Honghan Wu, «Investigating for bias in healthcare algorithms: a sex-stratified analysis of supervised machine learning models in liver disease prediction», *BMJ Health & Care Informatics,* 2022 s. 1–8, på s. 7. doi: 10.1136/bmjhci-2021-100457.

13 Jon Kleinberg, Himabindu Lakkaraju, Jure Leskovec, Jens Ludwig og Sendhil Mullainathan, «Human Decisions and Machine Predictions», *The Quarterly Journal of Economics*, 2018 s. 237–293, på s. 293. *https://doi.org/10.1093/qje/qjx032.*

14 Anne Kjersti Befring mfl., *Kunstig intelligens og big data i helsesektoren – rettslige perspektiver,* 1. utgave, Gyldendal 2020, s. 104.

Forholdet mellom GDPR artikkel 6 nr. 1 og 4: Datatilsynets tilnærming er hensiktsmessig

Av Carl Emil Bull-Berg

I *Lov&Data nr. 156 4/2023* stiller Ole Martin Moe og Hanne Pernille Gulbrandsen fra Deloitte spørsmål om Datatilsynet tar feil i sin vurdering av forholdet mellom GDPR artikkel 6 nr. 1 og nr. 4. Til tross for at jeg er enig i mye av det de skriver, ønsker jeg å understreke at det finnes flere gode grunner for Datatilsynets tolkning i vedtak 20/01626 og at tilsynets tilnærming virker mest hensiktsmessig – både for de registrerte og for de behandlingsansvarlige.

Krever behandling for nytt (forenlig) formål, et nytt behandlingsgrunnlag?

Enhver behandling av personopplysninger skal gjøres for spesifikke, uttrykkelige angitte og berettigede formål. Personopplysninger skal ikke behandles på en måte som er *uforenlig* med det opprinnelige formålet. Det er derfor sentralt å avklare når et formål er *forenlig* med et annet. En ikke uttømmende oversikt over momentene som skal hensyntas i vurderingen fremgår av

Carl Emil Bull-Berg

GDPR artikkel 6 nr. 4 bokstav a til e.

Et viktig spørsmål er om den nye behandlingen – nå utført for et nytt (forenelig) formål – krever et nytt behandlingsgrunnlag. Alternativt, om det er «fritt frem» så lenge den etterfølgende behandlingen er forenlig i henhold til GDPR artikkel 6 nr. 4 (og da under forutsetning av at behandlingen for det opprinnelige formålet hadde behandlingsgrunnlag). Sistnevnte oppfatning er trolig mest utbredt blant personvernjurister.

Datatilsynet la imidlertid i vedtak 20/01626 til grunn at det er både krav om forenlighet (etter GDPR artikkel 6 nr. 4) *og* et krav om nytt behandlingsgrunnlag etter GDPR artikkel 6 nr. 1.

> *«For behandling av personopplysninger for et annet formål enn det som personopplysningene ble samlet inn for, er det to kumulative krav i personvernforordningen. For det første kreves det, som ved all behandling av personopplysninger, at behandlingen har et rettslig grunnlag i artikkel 6 nr. 1 for å være lovlig. I tillegg kreves det at det nye formålet med behandlingen av personopplysninger er forenelig med formålet personopplysningene ble samlet inn for, jf. artikkel 6 nr. 4. Det er et unntak fra dette vilkåret dersom den nye behandlingen bygger på den registrertes samtykke eller har hjemmel i lov, men det er klart at dette unntaket ikke kommer til anvendelse i denne saken»*

I vedtaket konkluderte de med at NIFs (videre)bruk manglet behandlingsgrunnlag, og at det derfor ikke var nødvendig å ta stilling til om formålene var forenelig etter GDPR artikkel 6 nr. 4.

I artikkelen til Deloitte drøftes det om tilsynets konklusjon er riktig. Det er gode grunner til å reise denne diskusjonen. Som de henviser til, legger fortalepunkt 50 nemlig til grunn den motsatte konklusjon:

> *«Behandling av personopplysninger for andre formål enn de formål personopplysningene opprinnelig ble samlet inn for, bør bare være tillatt dersom behandlingen er forenlig med formålene som personopplysningene opprinnelig ble samlet inn for. I et slikt tilfelle kreves det ikke et annet rettslig grunnlag enn det som ligger til grunn for innsamlingen av personopplysninger».*

Juridisk teori legger også til grunn at det ikke er påkrevd med et nytt behandlingsgrunnlag.[1] EU-domstolen har blant annet henvist til fortalepunkt 50 i avgjørelse C-77/21, og de har ikke eksplisitt oppstilt et krav om nytt behandlingsgrunnlag, da i tillegg til at formålene må være forenelig.

Allikevel mener jeg at tilsynets konklusjon virker logisk og hensiktsmessig, både for de registrerte og for de behandlingsansvarlige.

For det første samsvarer tilsynets konklusjon best med GDPRs ordlyd. GDPR artikkel 6 nr. 1 slår fast at enhver behandling skal ha behandlingsgrunnlag. Til tross for at det er en åpenbar kobling mellom formål og hva som utgjør en behandling,[2] er viderebehandling for et nytt (men forenlig) formål en ny behandling av personopplysninger. Dette underbygges blant annet av ordlyden i artikkel 5 nr. 1 (som skiller mellom formåls- og lovlighetsprinsippet), definisjonen i GDPR artikkel 4 nr. 2 og C-77/21.[3]

Ordlyden i GDPR artikkel 6 nr. 1 trekker følgelig i retning av at det er påkrevd med et eget behandlingsgrunnlag for den nye behandlingen. Alternativet er å tolke ordlyden innskrenkende, da med hjemmel i fortalepunkt 50 mv.

For det andre fremstår konklusjonen mest hensiktsmessig fra både ståstedet til de registrerte og for de behandlingsansvarlige. Én av årsakene er at noen av de registrertes rettigheter er tilknyttet ulike behandlingsgrunnlag. Dersom det legges til grunn at det ikke er nødvendig med et nytt behandlingsgrunnlag, kan dette gi underlige utfall. Dette kan illustreres med et eksempel:

> Personopplysningene X samles inn for å levere en tjeneste (behandlingsgrunnlag: GDPR artikkel 6 nr. 1 bokstav b). Til tross for at det ikke var tiltenkt på tidspunktet for innsamlingen, ønsker den behandlingsansvarlige å viderebehandle personopplysningene X for å forbedre tjenesten. Det forutsettes i det videre at det nye formålet er forenlig med det opprinnelige formålet.
>
> Dersom den behandlingsansvarlige hadde hatt det nye formålet i tankene fra start, ville den behandlingsansvarlige benyttet GDPR artikkel 6 nr. 1 bokstav f som behandlingsgrunnlag. Imidlertid, dersom vi forutsetter at det ikke er påkrevd med et «nytt» behandlingsgrunnlag (og at det er tilstrekkelig med forenlighetsvurderingen), vil altså ikke den behandlingsansvarlige basere seg på GDPR artikkel 6 nr. 1 bokstav f.
>
> Den registrerte har derfor andre rettigheter enn hva vedkommende ville hatt dersom behandlingen var tiltenkt allerede fra start. Den registrerte vil da ikke kunne protestere mot behandlingen, jf. GDPR artikkel 21 (en mulighet vedkommende hadde hatt dersom behandlingen opprinnelig var opprinnelig tiltenkt, og derfor hadde sitt «eget» behandlingsgrunnlag).

Eksempelet illustrerer hvordan den registrerte kan ende opp med å bli plassert i en dårligere situasjon ved viderebehandling enn hva vedkommende ville vært dersom behandlingen var tiltenkt fra start.

Konklusjonen vil også kunne få underlige utslag for den behandlingsansvarlige. Vil dette medføre at den registrerte har rettigheter tilknyttet det opprinnelige behandlingsgrunnlaget, til tross for at det egentlig ikke passer på viderebehandlingen – for eksempel dataportabilitet? Dette var neppe intensjonen da fortalepunkt 50 ble skrevet.

Tilsynets tilnærming begrenser trolig ikke muligheten til å behandle personopplysninger

Noen jurister og virksomheter har nok reagert kritisk på Datatilsynets tolkning av GDPR artikkel 6 nr. 4, ettersom de opplever at tolkningen begrenser handlingsrommet til å behandle personopplysninger – og da at den medfører en høyere terskel for å behandle personopplysninger for nye forenelige formål. Reaksjonen fremstår umiddelbart som logisk, ettersom tilsynet tross alt stiller to vilkår istedenfor kun ett. En slik tolkning ser også advokatene fra Deloitte ut til å legge til grunn i sin artikkel.

Et slikt inntrykk bør nyanseres. Tilsynets tilnærming begrenser neppe virksomheters anledning til å behandle personopplysninger i praksis. Dersom den behandlingsansvarlige konkluderer med at viderebehandlingen av personopplysninger er forenelig med det opprinnelige formålet (da i henhold til GDPR artikkel 6 nr. 4), vil det trolig være en forholdsvis enkel sak å identifisere et behandlingsgrunnlag i GDPR artikkel 6 nr. 1. Vurderingen etter GDPR artikkel 6 nr. 4 er ikke begrenset til å kun angå «koblingen» og nærheten mellom det opprinnelige og det nye formålet, men består i stor grad av en interesseavveining.

Det er altså vanskelig å tenke seg en situasjon hvor en behandlingsansvarlig har grunnlag i GDPR artikkel 6 nr. 4, men sliter med å legitimere behandlingen etter GDPR artikkel 6 nr. 1. Terskelen for viderebehandling bør i sin natur anses til å ligge høyere enn en opprinnelig tiltenkt behandling.

Datatilsynets tilnærming virker altså hensiktsmessig og logisk, uavhengig av om den ender opp med å bli stående som gjeldende rett.

Carl Emil Bull-Berg, advokat.

---

1 Åste Marie Bergseng Skullerud mfl., Personvernforordningen. Ajourført lovkommentar til artikkel 6(4) GDPR, *Juridika*

2 Åste Marie Bergseng Skullerud mfl., Personvernforordningen. Ajourført lovkommentar til GDPR artikkel 4 Juridika og Ot.prp.nr.92 (1998-1999) side 102.

3 Se blant annet avsnitt 32.

Av Dag Wiese Schartum og Olav Torvund

Foto av Torvund: Kjetil Ree, 2009.

Jon Bing [1]

Ti år har gått siden professor, dr. juris og sciencefiction-forfatteren Jon Bing gikk bort.[2] I nesten 50 år hjalp han oss å forstå møtet mellom teknologien og rettslivet. Ti år er lang tid. Men det er mange av oss som samarbeidet med og kjente Jon som fortsatt forstår og verdsetter den kraften Jon Bings gjerning fremdeles representerer. I løpet av de ti årene som har gått, har mange nye forskere og fagfolk innen det rettsinformatiske feltet kommet til. Mange er mest opptatt av nåtid og fremtid og oppdager ikke at det er overraskende lenge siden mange av de problemstillingene vi i dag jobber med ble formulert. Enhver som interesserer seg for et «moderne» problemområde som f.eks. *automatiseringsvennlig lovgivning* har mye å lære av å lese Jons artikkel om emnet i Tidsskrift for rettsvitenskap fra 1977.[3]

I forkant av den teknologiske utviklingen

For Jon hang fremtiden nøye sammen med nåtiden: *"Fremtiden er ikke noe som ligger der ute og venter på å bli oppdaget. Fremtiden er noe vi skaper gjennom de valg og de handlinger vi foretar"*, pleide Jon å si. Noe av det beundringsverdige ved Jon Bing var hans store evne til å identifisere og framskrive trekk ved den teknologiske og samfunnsmessige utviklingen. Slik hjalp han samtiden å forstå mulige juridiske og andre implikasjoner av teknologier som var under utvikling. Når innsiktene hans ofte viste seg å sette fingeren på vesentlige forhold, var det ikke bare fordi han forstod teknologien; han hadde også dyp forståelse for det samfunnet denne teknologien skulle fungere i, og for de menneskene som skulle bruke den.

Jon Bing (1944–2014)
Foto: Rolf M. Aagaard / Aftenposten / NTB

Internasjonalisten

Jon Bing var stadig på reise og nøt stor respekt i det internasjonale rettsinformatiske miljøet. Tidligere dommer ved Australias høyesterett, Michael Kirby, som var sentral ved utarbeidelsen av de første internasjonale normene om personvern, skrev bl.a. i anledning Jons bortgang: *"I honour Jon Bing as one of the founders of global law and policy on information technology. I was very proud to know him as a colleague and friend."* Jon Bing ville ut i verden for å få impulser fra sine mange kollegaer og venner i mange land, og for å dele og diskutere egne analyser med de fremste internasjonale ekspertene. Dessuten var han en begeistret og begeistrende gjest i de landene han besøkte med stor interesse for hvert lands rettssystem, for kulturen, historien, maten og vinen …

> Når innsiktene hans ofte viste seg å sette fingeren på vesentlige forhold, var det ikke bare fordi han forstod teknologien; han hadde også dyp forståelse for det samfunnet denne teknologien skulle fungere i, og for de menneskene som skulle bruke den.

Bings rettsinformatiske rom

Jons faglige nysgjerrighet resulterte i et meget bredt faglig forfatterskap. Han har bl.a. skrevet innen opphavsrett, personvernrett, strafferett, forvaltningsrett, kontraktsrett, rettskildelære og om rettslige informasjonssystemer. Det vil si; han trakk disse fagene inn i sine rettsinformatiske rom og analyserte problemstillinger som han så komme. I dag er det knapt noe rettsområde uten problemstillinger som er knyttet til

1 Denne teksten er en videre bearbeidelse av omtalen av Jon Bing i *jonbing.net*.

2 Jon Bing døde 14. januar 2014, 69 år gammel.

3 Se Jon Bing, Automatiseringsvennlig lovgivning, i Tidsskrift for rettsvitenskap 1977, s. 174–185.

informasjons- og kommunikasjonsteknologi (IKT). Ikke sjelden var det Jon som åpnet broen mellom tradisjonelle rettsspørsmål og rettsspørsmål knyttet til IKT.

Institusjonsbyggeren

Jon Bing jobbet ikke alene. Når Jon lyktes så godt, er det bl.a. fordi han sammen med professor Knut S. Selmer ledet oppbyggingen av Avdeling for edb-spørsmål, som i dag er Senter for rettsinformatikk (SERI) ved Det juridiske fakultetet i Oslo. Etableringen av avdelingen var resultat av et seminar som ble holdt 16. mars 1970 der en diskuterte et notat Jon hadde skrevet om forholdet mellom «jus og edb». Etterhvert kunne han samarbeide med opp mot 20 medarbeidere ved SERI med lignende faglige ambisjoner som han selv; med fokus på juridisk bredde og teknologisk innovasjon.

Jon Bing var sentral ved etableringen av Lovdata i 1981. Jons rapport fra 1976 trakk perspektivene for et datamaskinbasert system for produksjon og vedlikehold av Lovsamlingen.[4] Sammen med Trygve Harvold planla Jon hvordan Norges lover skulle overføres til datamaskinbasert sats.

Faglig fellesskap og bygging av et rettsinformatisk miljø i Norge var et viktig element i den faglige delen av Jon Bings virke. Jon var entreprenøren som skaffet finansiering, arbeidsmulighet og faglig fellesskap for en rekke unge håpefulle studenter og forskere. Blant resultatene var etableringen av Norsk foreningen for jus og edb (NFJE). Ord som fellesskap, vennskap og tillit er nøkkel for å forstå Jons suksess med å bygge opp de rettsinformatiske miljøene i Norge.

Travel trivsel

Jon Bing arbeidet mye og trivdes med det. Jons faglitteræreproduksjon teller omtrent like mange verk i tillegg – alt fra romaner og noveller til skuespill, tegneserier og libretto. Viktige deler av skjønnlitteraturen ble skrevet sammen med Jons nære venn Tor Åge Bringsværd.[5] Bibliografiene vitner om meget store arbeidskapasitet. Det kan kanskje synes som om det har vært unødvendig for ham å prioritere, men dette må åpenbart være feil. Hva han i så fall har valgt bort er uansett vanskelig å skjønne: Fagartikler, fagbøker, foredrag, deltakelse på konferanser og møter over hele kloden, verv, skjønnlitteræreutgivelser og medieopptredener var blant aktivitetene han delte sin tid på. Han må jo ha sagt nei stadig vekk – men det bærer ikke Jon Bings CV og bibliografier preg av.

> Ord som fellesskap, vennskap og tillit er nøkkel for å forstå Jons suksess med å bygge opp de rettsinformatiske miljøene i Norge.

En verdsatt person

Mange verdsatte Jon Bings innsikt, teft, faglige dyktig og formidlingsevne. Han var blant annet æresdoktor ved Stockholms universitet (1997) og ved Københavns universitet (1998), og visiting professor ved King's College i London (1997 – 2000). Som medlem av Legal Advisory Board i Directorate General Information Society, gav han råd til Europakommisjonen. Han var dessuten medlem i ICANNs råd for globale toppnivå-domener (GNSO Council) i en tid da Internett var nytt. Her hjemme var Jon medlem av Det norske Videnskabsakademi. Jon ledet Personvernnemnda i de første åtte årene, fra 2000. Nemnda var klageorgan i saker etter Personverndirektivet og annen personvernlovgivning. Jon ledet Norsk kulturråd i åtte år. Han ble også gitt heder og ære ved i 1999 å bli utnevnt til Ridder av 1. klasse av St. Olavs Orden. I 2001 mottok han Brage hederspris for prestasjoner innen skjønnlitteratur, faglitteratur og relaterte aktiviteter.

Jon Bing i dag

Hvorfor har så mange valgt å engasjere Jon Bing, lese hans arbeider og lytte når han snakker? Svaret ligger trolig i Jons meget store faglige dyktighet og bredde, kombinert med en uvanlig evne til formidling. Dagens forskere kan lære mye av Jon om hvordan de kan skrive faglige tekster som identifiserer nye problemstillinger og vekker interesse og nysgjerrighet om fortsettelsen. Den som vil bli nærmere kjent med denne oppsiktsvekkende mannen og hans forfatterskap, finner fulle bibliografier på Jonbing.net.

Selv om mange av Jon Bings akademiske arbeider i dag mest har historisk interesse, hører forfatterskapet til det «grunnfjellet» som gjør det mulig for oss i dag å diskutere forholdet mellom jus og teknologi. I boken om 1000 år med norsk rettshistorie skriver rettshistorikeren, professor Jørn Øyrehagen Sunde: «Langsamt har [Jon Bings] visjonar vorte realitetar. No har tida kome til å setja denne utviklinga inn i ein historisk samanheng, og for å kopla den til rettsstaten, for på den måten å seia noko om kvar vegen vidare bør gå.»[6]

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

Olav Torvund, professor ved Det juridiske fakultet, Universitetet i Oslo

4 Iver Tangen Stensrud, *Retten i det digitale Norge. Senter for rettsinformatikk 1970 – 2020*, Fagbokforlaget 2020, s. 73.

5 Fullstendige bibliografier finnes på *JonBing.net*.

6 Jørn Øyrehagen Sunde, *1000 år med norsk rettshistorie - ei annleis noregshistorie om rett, kommunikasjonsteknologi, historisk endring og rettstat*, Dreyer 2023, s 19.

Halvor Manshaus

Halvor Manshaus er leder IP/Media-gruppen i Advokatfirmaet Schjødt AS, Oslo og fast spaltist i Lov&Data.

Kryptering: EMD lukker bakdøren

Den europeiske menneskerettsdomstolen (EMD) behandler tvister knyttet til Den europeiske menneskerettskonvensjonen (EMK). Det er et krav i Europarådet at stater som blir tatt opp som medlem, samtidig ratifiserer EMK. Da Russland trådte inn i Europarådet 28. februar 1996, ble landet dermed underlagt myndigheten til EMD etter ratifiseringen i mai 1998.

Dette utløste en periode med en rekke utfordringer for både domstolen og Russland. EMD ble raskt nedlesset med klagesaker fra russiske borgere. Ved utgangen av 2019 sto Russland for 15.050 av totalt 59.800 saker som lå til behandling. Dette ene landet av i alt 47 medlemsstater i 2019 sto altså for en fjerdedel av klagesakene. Russland har blitt felt i en rekke saker. Et kritisk tilfelle oppsto i 2011 i den såkalte Markin-saken. EMD landet på motsatt konklusjon av Russlands egen konstitusjonsdomstol og felte Russland. Russland svarte med å vedta en ny lov i 2015, samme dag som EMD i en annen sak dømte Russland for inngrep grunnet et system som overvåket kommunikasjon med mobiltelefon. Den nye loven ga den russiske konstitusjonen trinnhøyde over avgjørelser fra EMD, i strid med konvensjonsforpliktelsene. Dette har altså ikke vært et enkelt samarbeid.

Det har også vært problemer i kjølvannet av Russlands krigshandlinger i Europa. Da Russland annekterte Krim i 2014, svarte Europarådet med å frata Russland stemmeretten i rådets parlamentarikerforsamling. Denne prosessen ble senere omtalt som «Ruxit» av Europarådets daværende leder Thorbjørn Jagland. Etter en avstemning i 2018 ble stemmeretten gitt tilbake til Russland. Dette varte imidlertid ikke lenge, ettersom Russlands representasjonsrett i Europarådet ble suspendert allerede dagen etter invasjonen av Ukraina 24. februar 2022. Russland beholdt imidlertid medlemskapet og en sittende russisk dommer i EMD. Da krigen i Ukraina eskalerte i starten av mars 2022, ble Russland suspendert fra Europarådet. Den 15. mars samme år kom Europarådets parlamentarikerforsamling med en rådgivende uttalelse som konkluderte med følgende oppfordring til Russland:

> *«The Assembly, therefore, is of the opinion that the Committee of Ministers should request the Russian Federation to immediately withdraw from the Council of Europe. If the Russian Federation does not comply with the request, the Assembly suggests that the Committee of Ministers determine the immediate possible date from which the Russian Federation would cease to be a member of the Council of Europe»*

Russland innledet samme dag den formelle prosessen for å trekke seg ut av Europarådet. Europarådet svarte med å ekskludere Russland.[1] Regelverket innebar at Russland først etter utløpet av en seksmåneders periode trådte ut av EMK, den 16. september 2022.

På dette tidspunktet lå det fortsatt flere saker til behandling mot Russland, og det ble derfor nødvendig å ta stilling til hvordan disse sakene skulle håndteres. En pressemelding fra EMD fra 3. februar 2023[2] gjør rede for rettens håndtering av situasjonen. Det forelå på dette tidspunktet 16.730 klager mot Russland til behandling, og det var nylig blitt behandlet to saker mot Russland i storkammer som ga anvisning på håndteringen. Kort oppsummert har EMD lagt til grunn at handlinger eller unnlatelser som fant sted før Russlands uttreden fra EMD 16. september 2022, skal behandles for domstolen.

Dette er bakgrunnen for dommen fra EMD i saken Podchasov vs. Russland (application 33696/19)[3] som ble avsagt 13. februar 2024. Avgjørelsen ble dermed ble rettskraftig 13. mai 2024. Saken dreide seg om et russisk påbud ret-

1 https://rm.coe.int/0900001680a5da51

2 https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-7559628-10388013&filename=Future%20processing%20of%20applications%20against%20Russia.pdf

3 *https://hudoc.echr.coe.int/?i=001-230854*

tet mot «Internet Communication Organisers» (ICO). EMD gjengir definsjonen av ICO slik:

> *«An ICO is defined as a person or an entity that ensures the functioning of information systems and/or programmes for electronic devices, with the aim of receiving, transmitting, delivering and/or processing electronic communications on the Internet (section 10.1(1) of the Information Act)»*

Påbudet innebærer at alle kommunikasjonsdata skal lagres i ett år, og innholdet i kommunikasjonen skal lagres i seks måneder. Videre skal nødvendig informasjon og verktøy for å dekryptere kryptert innhold gjøres tilgjengelig for politimyndighetene. Regelverket omfatter alle opptak, tekst, bilder, video, lyd og andre former for elektronisk kommunikasjon som sendes, mottas, formidles eller behandles av brukere på internett. I tillegg til dette skal den aktuelle ICO identifisere brukerne av tjenesten med mobilnummer.

En forskrift med angivelsen 743, datert 31. juli 2014 og senere oppdatert 18. januar 2018, utvider påbudet. Disse endringene innebærer at den avgivende ICO i tillegg må gi myndighetene fjerntilgang til sine informasjonssystemer, slik at myndighetene kan motta den nødvendige informasjonen under påbudet. Etterfølgende tillegg til regelverket presiserer at myndighetene skal ha et grensesnitt for å søke opp og innhente informasjon fra den enkelte ICO, og at denne tilgangen skal være tilgjengelig døgnet rundt. Summen av det opprinnelige påbudet og etterfølgende oppdateringer er et meget omfattende system for å få tilgang til kommunikasjon over en rekke ulike kommunikasjonsplattformer på Internett.

Klageren i saken for EMD var en bruker av tjenesten Telegram. Dette er en chattetjeneste som kan sammenlignes med Messenger og Whatsapp, og som brukes mye i deler av Europa, Afrika og Asia. Per i dag opplyser tjenesten å ha over 900 millioner aktive brukere målt over en måned. Når man først tar i bruk Telegram, gjøres det ingen kryptering. Dette må brukeren selv aktivere. På nettsiden til Telegram beskrives denne funksjonen som en «secret chat»:

> *«All messages in secret chats use end-to-end encryption. This means only you and the recipient can read those messages – nobody else can decipher them, including us here at Telegram.»*

Russiske myndigheter sendte 12. juli 2017 en forespørsel til Telegram om teknisk informasjon som var nødvendig for å dekryptere kommunikasjon relatert til seks mobilnumre og brukerkontoer på Telegram. Informasjon om blant annet IP-adresse, TCP/UDP-port og dekrypteringsdata skulle sendes per e-post direkte til Russlands Federal Security Service (FSB).

Telegram nektet å utlevere informasjonen. Det ble vist til at de aktuelle brukerne hadde aktivert «secret chat», som altså innebar at meldingene ble kryptert fortløpende. Det ville være teknisk umulig å utlevere informasjon for å dekryptere kun disse brukernes meldinger. Slik tilrettelegging ville i praksis utgjøre en bakdør som ville gitt tilgang til kryptert informasjon for alt kryptert trafikk på Telegram. I den etterfølgende internrettslige prosessen tapte Telegram i samtlige instanser. Telegram ble bøtelagt, og domstolen besluttet at Telegram skulle blokkeres i Russland. Det er verdt å merke seg at denne avgjørelsen har vært rettskraftig etter at den ble avsagt 13. april 2018 og deretter opprettholdt av ankeinstansen. Til tross for dette har Telegram etter det jeg har kunnet bringe på det rene, aldri blitt blokkert eller stengt i praksis.

Podchasov og 34 andre personer klaget den siste avgjørelsen inn for en russisk domstol. Det ble vist til at et pålegg om pliktavlevering av verktøy for dekryptering ville innebære et inngrep i deres rett til privatliv og privat kommunikasjon. Videre ble det vist til at regelverket ikke hadde mekanismer for å beskytte mot slik bruk, og at FSB sto fritt til å overvåke all kommunikasjon når det først hadde fått denne «bakdøren». Da klagen ikke førte frem, anket Podchasov saken oppover i systemet helt til den russiske føderale høyesteretten avviste til slutt avviste saken.

Spørsmålet for EMD var om et påbud som beskrevet ovenfor gikk for langt i forhold til klagers rett til privatliv og fri kommunikasjon under EMK artikkel 8. EMD innleder sin analyse med å vise til flere internasjonale organer som har vurdert myndighetenes behov for innsyn opp mot enkeltindividets og samfunnets behov for fortrolig kommunikasjon. Det er ikke overraskende å lese at for eksempel FNs høykommissær for menneskerettigheter viser til at det er nødvendig med kryptering spesielt der ytringsfriheten er under sterkt press:

> *«In environments of prevalent censorship, encryption enables individuals to maintain a space for holding, expressing and exchanging opinions with others. In specific instances, journalists and human rights defenders cannot do their work without the protection of robust encryption, shielding their sources and sheltering them from the powerful actors under investigation.»*

EMD siterer også en resolusjon fra Europarådet fra 2015, som omtaler nettopp bruk av bakdører og andre virkemidler for å sette til side kryptering. I denne rapporten vises det til at slike virkemidler kan tenkes utnyttet av terrorister og kriminelle:

> *«The Assembly is deeply worried about threats to Internet security by the practices of certain intelligence agencies, disclosed in the Snowden files, of seeking out systematically, using and even*

creating 'back doors' and other weaknesses in security standards and implementation that could easily be exploited by terrorists and cyberterrorists or other criminals.»

Den samme resolusjonen stiller seg også skeptisk til nettopp overvåkningstiltak som er blitt implementert i Russland:

«High-technology surveillance tools are already in use in a number of authoritarian regimes and are used to track down opponents and to suppress freedom of information and expression. In this regard, the Assembly is deeply concerned about recent legislative changes in the Russian Federation which offer opportunities for enhanced mass surveillance through social networks and Internet services.»

Det som virkelig er verdt å ta med seg fra rapportene som EMD viser til, er en felles uttalelse fra Europol (EUs egen politimyndighet) og European Agency for Cybersecurity (ENISA) i en rapport av 20. mai 2016:

«Intercepting an encrypted communication or breaking into a digital service might be considered as proportional with respect to an individual suspect, but breaking the cryptographic mechanisms might cause collateral damage. The focus should be on getting access to the communication or information; not on breaking the protection mechanism»

Denne tilnærmingen vitner om en modning hos politimyndighetene, som har tatt inn over seg de negative konsekvensene ved en slik overvåkning som EMD behandlet i denne saken. Denne rapporten fremhever at for at den krypterte informasjonen skal kunne brukes, må den på et eller annet tidspunkt dekrypteres. Dette åpner igjen for at tradisjonelle etterforskningsmetoder fortsatt vil kunne benyttes, sammen med moderne teknologi og kompetanse som politiet bør ha tilgang til.

Vi ser da også en klar utvikling i retning av at politimyndigheter samarbeider på tvers av landegrenser og har utviklet metoder som delvis baserer seg på tradisjonell etterforskning i kombinasjon med utstrakt bruk av moderne teknologi. Der for eksempel etterforskning i utlandet avdekker kriminelle handlinger, vil det kunne avdekkes bevis som også kan felle personer bosatt i Norge. Høyesterett har langt på vei akseptert at kryptert datatrafikk avlest og innhentet av utenlandske myndigheter kan brukes som bevis i Norge. I saken *HR 2022-1314-A* (EnroChat-saken) oppstilte Høyesterett i avsnitt 26 tre generelle vilkår for at slik bevisførsel skal tillates i Norge.

– Bevisene må være innhentet i tråd med regelverket der det dette skjer
– Tiltalte må ha en rett til innsyn i materialet
– Innhenting skal ikke ha skjedd på en måte som innebærer at bevisførselen ville stride mot grunnleggende norske verdier

Bakgrunnen for saken var at Fransk og nederlandsk politi fikk tilgang til en dataserver som var plassert i Roubaix i Frankrike. Med bistand fra blant Europol ble det utviklet en teknisk løsning for å dekryptere kommunikasjonen på den aktuelle plattformen EncroChat. Systemet var basert på dedikerte mobiltelefoner som kun fungerte opp mot andre tilsvarende enheter med EncroChat installert. Telefonene ble levert med internasjonalt sim-kort, og inneholdt i tillegg til automatisk kryptering også funksjoner som panikksletting, fjernsletting og automatisk sletting av meldinger etter et gitt tidsintervall. Alle disse funksjonene la spesielt godt til rette for kriminell aktivitet.

Politiet i Frankrike installerte en falsk oppdatering på serveren i Roubaix, som ble spredt i nettverket og gjorde det mulig å forbigå krypteringen av meldingene. På grunn av sikkerhetsgradering av etterforskningsmetoden er det ikke klart om politiet hentet ned informasjon fra serveren eller direkte fra meldingsstrømmen i nettverket. I den etterfølgende straffesaken i Norge som gikk på omgang med en «meget betydelige mengde» narkotika ble det gjort gjeldende at bevisene var ulovlig innhentet. Her kom både tingrett, lagmannsrett og Høyesterett frem til det samme resultatet. Alle tre instanser la til grunn at bevisene var blitt lovlig innhentet i Frankrike og kunne brukes i Norge.

Som eksempel på at innhenting av bevis skjer i strid med grunnleggende norske verdier viser Høyesterett til at bevisene innhentes i et land der straffeprosessen bygger på et annet verdisyn enn det vi finner i Norge. Det vises også til tilfelle der innhenting fremstår som et forsøk på å unngå begrensninger som ellers ville følge av de prosessuelle reglene i norsk straffeprosess. Norske myndigheter kan altså be andre lands myndigheter om å innhente bevis, men ikke med sikte på å unngå sentrale skranker i vår internrett.

Høyesterett oppsummerer problemstillingen i saken presist i avsnitt 39:

«Kryptering er i seg sjølv korkje straffbart eller uynskt. Tvert om er moglegheita for kryptering og konfidensiell kommunikasjon ein viktig føresetnad for informasjons- og ytringsfridomen, jf. mellom anna EU-rådets resolusjon om kryptering 24. november 2020 (13084/1/20). Resolusjonen understrekar at det i statanes plikt til å respektere og sikre ytringsfridomen og retten til privatliv også ligg eit ansvar for å verne kryptert kommunikasjon. Samstundes peikar resolusjonen på at kryptert kommunikasjon er godt eigna til å verne kriminelle nettverk mot overvaking. Som det blir framheva i EU-resolusjonen, må difor omsynet til ytringsfridomen og retten til privatliv balanserast mot styresmaktenes kamp mot alvorleg kriminalitet. På den eine sida står personvernomsyn generelt

sterkt som verdi i Noreg. Masseovervaking av borgarane for å avdekke kriminalitet vil lett vera i strid med norske verdiar. På hi sida står omsynet til oppklaring av alvorleg kriminalitet.»

Som vi skal se nedenfor harmonerer dette utgangspunktet godt med avgjørelsen fra EMD som vi ser nærmere på i denne artikkelen. Balanseringen av samfunnets interesse og behov for krypterte tjenester opp mot behovet for å kunne innhente bevis i viktige saker står sentralt i begge sakene.

Tilbake til rapporten fra Europol og Enisa som EMD altså siterer i sin avgjørelse. Denne rapporten går konkret inn på pålegg om pliktavlevering av «bakdører» for å kunne overvåke også kryptert kommunikasjon. Her påpekes igjen de negative konsekvensene i et større samfunnsmessig perspektiv:

«While no practical encryption mechanism is perfect in its design and implementation, decryption appears to be less and less feasible for law enforcement purposes. This has led to proposals to introduce mandatory backdoors or key escrow to weaken encryption. While this would give investigators lawful access in the event of serious crimes or terrorist threats, it would also increase the attack surface for malicious abuse, which, consequently, would have much wider implications for society. Moreover, criminals can easily circumvent such weakened mechanisms and make use of the existing knowledge on cryptography to develop (or buy) their own solutions without backdoors or key escrow. [...]

Solutions that intentionally weaken technical protection mechanisms to support law enforcement will intrinsically weaken the protection against criminals as well, which makes an easy solution impossible.»

Betraktningene som fremmes her, er på linje med det vi kjenner fra EMD og norsk Høyesterett i saker om ytringsfrihet der domstolene har lagt vekt på den såkalte *chilling effect*. Sitatet fra rapporten fra Europol og ENISA ovenfor viser til at overvåkning kan fremstå proporsjonalt «with respect to an individual suspect», men at dette i et videre perspektiv kan «cause collateral damage». Dette er det samme som Høyesterett er inne på i Runesten-saken, RT-2010-1381, omtalt av undertegnede i LoD-2011-105-15, når førstvoterende skriver:

«I det lange løp er det en risiko for at en mer utstrakt bruk av vitneplikt vil kunne medføre at viktige kilder blir borte. Etter mitt syn tilsier derfor vesentlige samfunnsinteresser at media i størst mulig utstrekning bør kunne bevare anonymitet om sine kilder.»

EMD konstaterer i avgjørelsens avsnitt 50 at bare det å kreve lagring av data som knytter seg til en enkeltpersons privatliv, utgjør et inngrep etter EMK artikkel 8. Dette gjelder uavhengig av en eventuell etterfølgende bruk av denne informasjonen. I vurderingen av hvilken grad av privatliv som foreligger, viser EMD til at det i praksis er lagt vekt på konteksten for tilblivelse og innhenting av informasjonen, informasjonens art, måten informasjonen prosesseres og brukes på, samt resultatet av slik behandling. I dette tilfellet, hvor all klagerens kommunikasjon og tilhørende kommunikasjonsdata skulle lagres, er dette tilstrekkelig til å konstatere inngrep – uavhengig av om informasjonen ble aksessert av myndighetene eller ikke.

Ettersom klagen også tok opp myndighetenes krav på tilgang til og innsyn i den lagrede kommunikasjonen, måtte EMD ta stilling til dette separate spørsmålet. Det forelå ingen bevis for at myndighetene rent faktisk hadde fått tilgang til klagerens informasjon. Spørsmålet var likevel om bare eksistensen av det bakenforliggende påbudet om tilgang var tilstrekkelig til at det forelå inngrep. Dette spørsmålet har EMD tatt stilling til i saken Roman Zakharov vs. Russland (application 47143/06).[4] I denne avgjørelsen ble det slått fast at de russiske reglene om overvåkning ikke var proporsjonale. Det er der vist til at slik overvåkning gjøres i skjul, har et vidt omfang og rammer samtlige brukere av de aktuelle tjenestene. Samtidig mangler effektive virkemidler for kontroll og rettslig prøving. Til sammen innebærer dette at bare eksistensen av slike regler i seg selv gjør inngrep i privatlivet til det enkelte individ.

Det siste spørsmålet i saken gjaldt plikten til å avlevere verktøy og informasjon for dekryptering. EMD viser i avsnitt 57 til at en slik pliktavlevering ville ramme samtlige brukere av ICO-tjenesten. Det virker ut fra EMDs drøftelse på dette punktet som om anførselen ikke er fremført av klageren direkte for EMD, men at den utledes fra innleggene fra den nasjonale behandlingen i Russland. Det fremheves at Russland ikke har påvist at denne anførselen skulle være feil eller misvisende. Dermed legger EMD til grunn at pålegget vil påvirke samtlige brukere av krypterte tjenester på Telegram ved at krypteringen ikke lenger beskytter innholdet.

EMD oppsummerer deretter kravet til proporsjonalitet når det gjelder lagring og innsyn i data. Utgangspunktet er at slike regler må være nøye balansert opp mot behovet for personvern og privatliv. Disse betraktningene er generelle og oppsummerer altså EMDs syn på rettstilstanden når det gjelder denne typen overvåkning. I avsnitt 62 og 63 kommer dette klart til uttrykk:

«The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern technologies in the criminal-justice sys-

4 *https://hudoc.echr.coe.int/fre?i=002-10793*

tem were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such technologies against important private-life interests. […]

The core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and insist on limited periods of storage.»

I vurderingen av denne konkrete saken viser EMD deretter til at det russiske pålegget er meget omfattende og utgjør et ekstremt vidtrekkende og alvorlig inngrep i artikkel 8. Når det gjelder spørsmålet om proporsjonalitet og balanse i regelverket, hadde Russland vist til at en domstol skulle ha godkjent myndighetenes krav om innsyn i kommunikasjonen for de seks brukerne av Telegram. Det fremgår av saksfremstillingen i avgjørelsens avsnitt 7 at det skulle foreligge seks rettsavgjørelser om innsyn i brukerdata knyttet til de seks brukerkontoene på Telegram. Klageren har imidlertid vist til (gjengitt i avsnitt 39) at disse rettsavgjørelsene aldri ble gjort tilgjengelige for Telegram, for de etterfølgende internrettslige domstolene som behandlet klagesakene, eller for offentligheten.

EMD legger således i avsnitt 72 vekt på at FSB aldri fremla den rettslige prøvingen og godkjenningen av innsynsbegjæringen. I tillegg understreker EMD at de etterfølgende utvidelsene av det underliggende regelverket gir FSB direkte tilgang til de lagrede dataene. I dette ligger at FSB i praksis har full tilgang via fjernpålogging til alle kommunikasjonsdata og alt innhold hos den enkelte ICO. Det ligger i dette at domstolsprøving av den enkelte begjæring fra FSB uansett har liten betydning for den reelle muligheten for overvåkning. EMD understreker i den etterfølgende vurderingen at et slikt system er spesielt sårbart for misbruk fra myndighetenes side.

Halvor Manshaus / Midjourney AI-bilde.

Et sentralt trekk ved pålegget og dets konsekvenser var hvordan det i praksis ville ramme samtlige brukere av Telegrams krypterte meldingstjeneste. EMD trekker frem nettopp dette i avsnitt 70, der det fremheves hvordan pålegget i realiteten sto fristilt fra proporsjonalitet knyttet til eventuell mistanke om kriminelle handlinger:

«It affects all users of Internet communications, even in the absence of a reasonable suspicion of involvement in criminal activities or activities endangering national security, or of any other reasons to believe that retention of data may contribute to fighting serious crime or protecting national security.»

Når det gjaldt pålegget om å gi myndighetene de nødvendige midler for å dekryptere innhold, legger EMD vekt på at en slik tilnærming fremstår som uproporsjonal når den rammer samtlige brukere av tjenesten. Domstolen slår i avsnitt 76 fast at retten til privat og sikker kommunikasjon er en fundamental rettighet i et digital samfunn:

«…the Court observes that international bodies have argued that encryption provides strong technical safeguards against unlawful access to the content of communications and has therefore been widely used as a means of protecting the right to respect for private life and for the privacy of correspondence online. In the digital age, technical solutions for securing and protecting the privacy of electronic communications, including measures for encryption, contribute to ensuring the enjoyment of other fundamental rights, such as freedom of expression.»

Denne tilnærmingen til kryptering som en grunnleggende del av kommunikasjon og privatliv under artikkel 8 har stor praktisk betydning for myndighetenes adgang til å utføre massekontroll og overvåkning av kommunikasjonstjenester på internett. Når det gjelder myndighetenes adgang til å svekke beskyttelsen

som kryptering av innhold innebærer, for eksempel ved å kreve bakdører inn til innhold på generelt grunnlag, er EMD avvisende:

> *«Weakening encryption by creating backdoors would apparently make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications. Backdoors may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications.»*

EMD viser her til de ulike rapportene og uttalelsene som er gjengitt tidligere i avgjørelsen, og som trekker i retning av at slike tiltak ikke bare vil utfordre retten til ytringsfrihet og privatliv, men også kan ha uoversiktlige konsekvenser. Det påpekes at kriminelle potensielt kan utnytte slike svakheter og bakdører. Dette ville redusere sikkerheten for alle brukere av disse tjenestene. EMD peker deretter tilbake til de samme rapportene, der det er uttalt at myndighetene må utforske alternative tilnærminger for innsyn, i form av lovgivning og ved selv å følge den tekniske utviklingen. I avsnitt 80 konstaterer EMD ikke uventet at inngrepet er uforholdsmessig og ikke kan anses å være nødvendig i et demokratisk samfunn.

EMD fastslår deretter enstemmig at domstolen hadde jurisdiksjon til å behandle klagen for forholdene i saken som inntrådte før 16. september 2022, og at det forelå en krenkelse av privatlivet og retten til fri korrespondanse under artikkel 8.

Mulighetene for at en slik omfattende rett til overvåkning kan misbrukes, er åpenbare. Russland har i tillegg innført en rekke regler som kriminaliserer aktiviteter som vi ellers oppfatter som grunnleggende menneskerettigheter. Eksempelvis er det innført strenge regler rettet mot homofile og begrensninger av retten til å organisere seg og til å demonstrere. Slike forhold vil dermed innebære økt risiko for overvåkning fra myndighetene, ettersom dette kan karakteriseres som kriminell adferd.

Det kan ved første øyekast virke som om denne avgjørelsen har begrenset betydning. Russland vil neppe endre sine regler eller rutiner som følge av dommen. Da Russland trådte ut av og ble ekskludert fra Europarådet, besluttet ministerkomiteen at Russland fortsatt ville være bundet av etterfølgende rettsavgjørelser fra EMK.[5] I praksis håndteres fellende dommer fra EMD overfor den enkelte medlemsstat ved at det avholdes egne møter der dette diskuteres. Ministerkomiteen la i sin uttalelse til grunn i punkt 7 at Russland fortsatt var forpliktet til å delta i disse møtene og å implementere EMDs avgjørelser nasjonalt:

> *«The Committee of Ministers will continue to supervise the execution of the judgments and friendly settlements concerned and the Russian Federation is required to implement them.»*

Dette mener nok ministerkomiteen er i tråd med artikkel 70 i Wienkonvensjonen om traktatretten, som omhandler uttreden fra en traktat. Her heter det at slik uttreden fristiller parten (her Russland) fra plikter under avtalen, men at dette «does not affect any right, obligation or legal situation of the parties created through the execution of the treaty prior to its termination».

Russland på sin side har kuttet all kommunikasjon med EMD og ministerkomiteen siden mars 2022. Russland har heller ikke gitt noen informasjon eller oppdatering om hvorvidt avgjørelser fra EMD overhode følges opp. Dette er ikke overraskende, all den tid Russland heller ikke var den flinkeste i klassen til å følge opp avgjørelser fra EMD i årene de var medlem av Europarådet. I enkelte saker har Russland bare kort uttalt at avgjørelser er umulige å følge opp, mens i en rekke andre tilfeller har det aldri blitt gitt noen oppdatering på oppfølgning eller implementasjon.

Avgjørelsen inneholder likevel en rekke vurderinger og uttalelser som får betydning utover denne ene saken. Selv om vi nærmest kan legge til grunn at Russland vil ignorere utfallet i EMD, legger uttalelsene her føringer for de øvrige medlemsstatene. Dette er den første avgjørelsen som omhandler svekkelse av såkalt *end-to-end encryption* (E2EE), som har fått stor utbredelse i ulike chat- og delingstjenester på internett. Innhold krypteres på den ene siden før det overføres til mottakeren, som dekrypterer og gjør innholdet fullt tilgjengelig på sin side.

Det er også verdt å merke seg at avgjørelsen legger stor vekt på rapporter og uttalelser fra tunge organer innen menneskerettigheter og politietterforskning. Det er inntatt lange og fullstendige sitater fra disse rapportene. Denne teknikken er åpenbart ment å styrke EMDs argumenter og konklusjoner. Språket i avgjørelsen er også klart og tydelig. EMD uttrykker ikke her mye tvil om hvorvidt det foreligger et inngrep eller ikke, og om hvorvidt dette er «nødvendig i et demokratisk samfunn». EMD avslutter sin vurdering i avsnitt 80 med å påpeke at myndighetenes tilgang til elektronisk kommunikasjon uten noen reelle sikkerhetstiltak «*impairs the very essence of the right to respect for private life*». På denne måten fremhever EMD at det ikke er mye rom å manøvrere på her.

Dermed har EMD plantet et flagg når det gjelder medlemsstatenes adgang til overvåkning via bakdører inn i kryptert innhold som formidles via kommunikasjonstjenester på internett. Dette vil få betydning i diskusjonen om lovregulering, tiltak og etterforskningsskritt rettet mot kryptert innhold. Samtidig slår ikke EMD fast at all lagring

5 *https://search.coe.int/cm?i=0900001680a5ee2f*

av data på et så omfattende nivå nødvendigvis *må* være konvensjonsstridig. Det ligger i systematikken under artikkel 8 at det først må vurderes om det foreligger et inngrep. Deretter må det vurderes om inngrepet er proporsjonalt og nødvendig i et demokratisk samfunn. Dersom myndighetene eksempelvis etablerer en ordning med uavhengig kontroll som kan overprøve enkeltbegjæringer om innsyn og som i seg selv er gjenstand for en viss grad av kontroll, vil slike tiltak i en samlet vurdering kunne tale for at tiltaket er proporsjonalt.

Tilsvarende vil andre momenter kunne spille inn i en slik vurdering. I den omtalte EncroChat-saken la Høyesterett vekt på tjenestens art. Tjenesten og telefonene som ble solgt utelukkende for denne bruken fremsto som spesielt tilrettelagt for kriminalitet. Det fremsto også som om tjenesten i all hovedsak også ble brukt hovedsakelig av kriminelle. Førstvoterende oppsummerer dette slik i avsnitt 42:

> *«Eg er difor samd med tingretten og lagmannsretten i at bruk av ein kryptert kommunikasjonsplattform som i all hovudsak blir nytta av kriminelle, ikkje har krav på vern. Personar som vel å ta i bruk ei slik teneste, må vera klare over moglegheita for overvaking og etterforsking. I slike tilfelle vil det gjennomgåande ikkje vera i strid med norsk rettskjensle å bruke materiale innhenta på denne måten som prov i ei straffesak.»*

> Avgjørelsen i Podchasov-saken står etter min oppfatning som en viktig avklaring på et område der myndigheter og etterforskningsorganer trenger veiledning og opplæring.

Avgjørelsen i Podchasov-saken står etter min oppfatning som en viktig avklaring på et område der myndigheter og etterforskningsorganer trenger veiledning og opplæring. EMD setter her en høy standard. Avgjørelsen fokuserer gjennomgående mer på formelle spørsmål knyttet til lovligheten av det russiske regelverket enn på det materielle spørsmålet om hvorvidt selve overvåkningen i seg selv er et inngrep etter artikkel 8. Dette gir samtidig avgjørelsen større prinsipiell rekkevidde og slagkraft, ved at den er forankret i generelle prinsipper om proporsjonalitet og hensyn til privatlivet. EMD viser i denne saken en god forståelse av de underliggende tekniske spørsmålene, og trekker direkte linjer inn mot hvordan digital kommunikasjon er blitt en integrert del av hverdagen til folk flest.


Wiersholm

Av Rune Opdahl og Håvard Sveier Ottemo

Innledning

Den 12. april 2024 la regjeringen frem forslag til ny ekomlov.[1] Et aspekt ved lovforslaget er ny regel om bruk av informasjonskapsler, bedre kjent som cookies. I det videre skal vi gjennomgå dagens regel og forslaget til ny regel.

Dagens cookie-regel

Ved innføringen av den dagens ekomlov § 2-7 b ble det problematisert hvordan et samtykke skal innhentes for å være gyldig. I proposisjonen la departementet til grunn at det var tilstrekkelig at brukeren ga samtykke gjennom forhåndsinnstillinger i nettleseren, så fremt nettstedet for øvrig ga informasjon om hvordan man brukte informasjonskapsler.[2] Dette vil i praksis si at så lenge brukeren ikke hadde deaktivert informasjonskapsler i sine nettleser-innstillinger, var samtykket ansett gitt, forutsatt at nettsiden hadde en egnet cookie-policy.

Denne forståelsen har trolig forankring i det opprinnelige direktivet 2002/58/EF (ePrivacy-direktivet), som kun stiller krav om at brukeren skulle ha «the right to refuse» informasjonskapsler.[3] Denne ordlyden ble med direktiv 2009/136/EF (endringsdirektivet) i EU byttet ut med «given his or her consent». I fortalepunkt 66 til dette endringsdirektivet er det videre fastslått at «[w]here it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application». Endringsdirektivet er til dags dato ikke innlemmet i EØS-avtalen. Ekomloven ble oppdatert med innføringen av e-koml. § 2-7 b for å likevel forsøke å adressere noen av de nye direktivkravene, selv om ikke alle kravene ble fullt ut imøtegått.[4]

I C-673/17 (Planet49-saken) ble det fastslått at forhåndsavsjekkede bokser ikke er et gyldig samtykke. Et gyldig samtykke til bruk av informasjonskapsler krevde altså etter EU-retten et aktivt samtykke fra brukeren, i samsvar med personvernregelverket for øvrig.

Frem til nå har det altså vært en avvikende rettstilstand mellom EU-rett og norsk rett, ved at førstnevnte krever et aktivt samtykke, mens sistnevnte sannsynligvis kun krever et passivt samtykke (for begge gjelder det et unntak ved nødvendige cookies).

Forslaget til ny cookie-regel

Forslaget til ny bestemmelse om informasjonskapsler har som formål å bringe samtykkekravet etter ekomloven i samsvar med EU-retten. Lovgivers forslag til ny ordlyd er utvetydig: «[s]amtykke skal oppfylle kravene til samtykke i personvernforordningen».[5] Det følger av personvernforordningen at et samtykke, for å være gyldig, må være aktivt. Passive samtykker vil ikke lenger være tilstrekkelig.

Et annet vilkår for et gyldig samtykke er at det er informert. Det følger av forslaget til den nye lovbestemmelsen at det skal gis informasjon om formålet med bruk av informasjonskapslene og hvilke opplysninger som behandles, men begrepet «blant annet» kan tilsi at det også er krav til å gi annen informasjon.

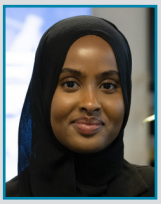
Lovforslaget gir, som EU-retten, unntak fra samtykkekravet for *nødvendige* informasjonskapsler. Det er verdt å merke seg at mens dagens regel omtaler dette som «nødvendige» informasjonskapsler, omtaler forslaget til ny regel dette som «strengt nødvendig». Dette gjøres for å sikre bedre samsvar med ordlyden i kommunikasjonsverndirektivet artikkel 5 nr. 3.

Hva nå?

Den foreslåtte lovendringen er ikke overraskelse. Rettstilstanden i resten av EU har i en god stund vært klar, og Datatilsynet har over lenger tid påpekt gapet mellom norske rett og EU-rett. Det er likevel grunn til å diskutere hvor hensiktsmessig den nye lovregelen vil være. Det er nok få som gir en «frivillig, spesifikk, informert og utvetydig viljesytring»[6] hver gang man blir eksponert for en cookie-popup. En kan derfor spørre seg om den nye lovregelen, som er ment å være personvernfremmende, isteden har motsatt effekt.

Av Rune Opdahl, Partner og Håvard Sveier Ottemo, Trainee og student, Wiersholm/Universitetet i Bergen. Begge arbeider i Advokatfirmaet Wiersholms avdeling for teknologi, media, telekom og immaterialrett.

1 Prop. 93 LS (2023–2024)
2 Prop.69 L (2012–2013) på s. 102
3 2002/58/EF artikkel 5 nr. 3
4 Prop.69 L (2012-2013) på s. 12
5 Prop. 93 LS (2023–2024) på s. 392
6 GDPR artikkel 4 nr. 11



Delphi

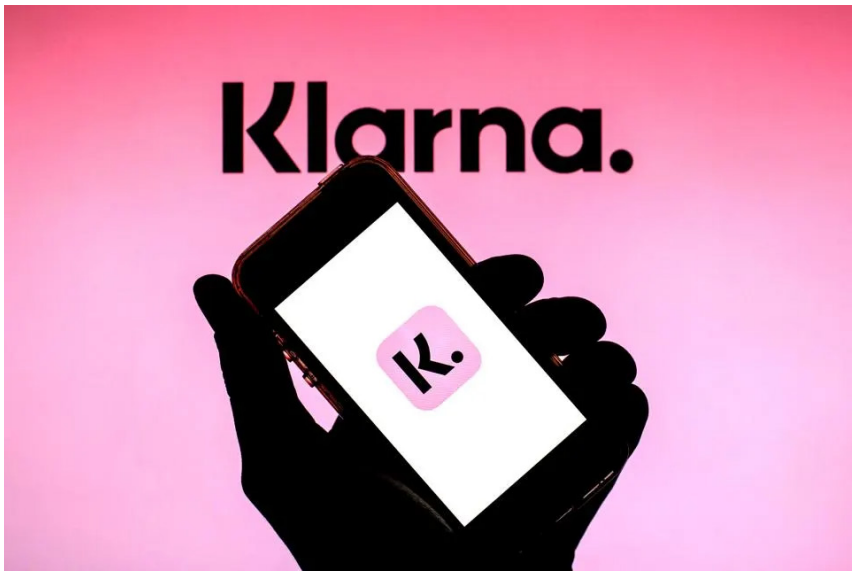
Fatima Abdillahi Farah

Kammarrätten ålägger Klarna Bank AB en sanktionsavgift om 7,5 miljoner kronor för bristande dataskyddsinformation

Kammarrätten i Stockholm meddelade den 11 mars 2024 sin dom avseende Klarna Bank AB:s (Klarna) efterlevnad av informationskravet i dataskyddsförordningen (”GDPR”).

Bakgrunden till domen är att IMY i samband med ett tillsynsärende påförde Klarna en sanktionsavgift om 7,5 miljoner kronor för överträdelse av en rad bestämmelser i GDPR. IMY riktade kritik mot Klarna för att ha lämnat ofullständig och bristande information och i vissa fall helt utelämnat dataskyddsinformation. Bland annat ansåg IMY att Klarna åsidosatt informationskravet genom att inte uppge vilka tredjeländer som varit mottagare av personuppgifter. Beslutet överklagades av Klarna till förvaltningsrätten, som sänkte sanktionsavgiften till 6 miljoner kronor. Domen överklagades så småningom även till kammarrätten. I domen fastställer kammarrätten IMY:s sanktionsavgift om 7,5 miljoner kronor, men håller inte helt med om IMY:s bedömning i alla delar.

En av frågorna som domstolen ställdes inför var om informationen som Klarna lämnat om de registrerades rättigheter uppfyllde kraven i GDPR. Enligt artikel 13.2 i GDPR är den personuppgiftsansvarige skyldig att lämna information om den registrerades rätt att bland annat begära tillgång till, rättelse eller radering av personuppgifter. I den delen fastslår kammarrätten att GDPR endast ställer krav på att den personuppgiftsansvarige informerar de registrerade om förekomster av vissa rättigheter. Till skillnad från både IMY och förvaltningsrätten bedömer Kammarrätten alltså inte att Klarna varit skyldiga att närmare beskriva dessa rättigheter.



Illustrasjon: Thiago Prudencio/SOPA Images/LightRocket via Getty Images) SOPA IMAGES/LIGHTROCKET VIA GETTY IMAGES

Vad gäller frågan om personuppgiftsansvariga är skyldiga att informera om vilka specifika tredjeländer som personuppgifter har överförts till gör domstolen en liknande bedömning som ovan: GDPR ställer inte krav på att personuppgiftsansvariga behöver lämna information om vilka specifika tredjeländer som personuppgifter överförs till, utan det räcker med att endast nämna att det sker tredjelandsöverföringar.

Vidare ställdes frågan om Klarna varit skyldiga att ange vilka svenska respektive utländska kreditupplysningsbyråer som varit mottagare av personuppgifter. I den delen konstaterar kammarrätten att inget i ordalydelsen i artikel i 13.1 e) i GDPR tyder på att det finns en skyldighet att särskilja svenska och utländska kreditupplysningsbyråer.

Kammarrätten slår dock fast att Klarna överträtt informationskravet i artikel 12.1 i vissa delar. Domstolen anger att informationen som lämnats rörande ändamålet med personuppgiftsbehandlingen varit både svårtillgänglig och otydlig. Vidare anger kammarrätten att informationen om rätten till dataportabilitet som fastställs i artikel 20 i GDPR lämnats på ett sådant sätt att det är svårt att förstå att det är separat rättighet. Detta främst eftersom terminologin som Klarna använt sig av är otydligt utifrån terminologin som används i GDPR.

Artikel 5.1 a) i GDPR föreskriver, bland annat, att personuppgifter ska behandlas på ett öppet sätt i förhållande till den registrerade. Till skillnad från både IMY och förvaltningsrätten anser kammarrätten inte att Klarnas överträdelser av informationskravet varit av den omfattning och karaktär att den generella principen om öppenhet åsidosatts.

Domen visar att på mer nyanserad och mindre sträng bedömning av både informationskravet och den grundläggande principen om öppenhet i GDPR. Kammarrättens tolkning av informationskravet innebär att det inte finns en skyldighet att lämna så pass detaljerad information som IMY och förvaltningsrätten har ansett. Rent praktiskt innebär det att personuppgiftsansvariga inte behöver djupdyka i vad varje rättighet innebär i sina integritetspolicyer och dylikt. I stället räcker det med att informera om förekomsten av de rättigheter som följer av GDPR, så länge den informationen är tydlig, lättillgänglig och separerar olika rättigheter från varandra.

Trots detta ålägger kammarrätten en lika hög sanktionsavgift som IMY för de överträdelser som Klarna anses gjort sig skyldiga till, med hänvisning till att sanktionsavgiften ska framstå som en effektiv, proportionell och avskräckande åtgärd. I sammanhanget kan tilläggas att den europeiska dataskyddsstyrelsen, EDPB, kommit med nya riktlinjer om hur administrativa sanktionsavgifter vid överträdelser av GDPR ska beräknas sedan IMY:s ursprungliga beslut i ärendet.

Fatima Abdillahi Farah, Thesis Trainee i Advokatfirman Delphi.

Gorrissen Federspiel

Tue Goldschmieding

Datatilsynets har truffet afgørelse om Tryg Forsikring A/S' oplysningspligt ved personovervågning

Det danske Datatilsyn (»Datatilsynet«) traf den 2. januar 2024 afgørelse i en sag med journalnummer 2022-431-0204. Sagen angik Tryg Forsikring A/S' (»Tryg«) generelle procedurer for opfyldelse af deres databeskyttelsesretlige oplysningspligt i forbindelse med indsamling af personoplysninger ved personovervågning.

Efter Datatilsynets anmodning om en udtalelse, bemærkede Tryg, at selskabet havde en legitim interesse i at kontrollere, at den registreredes krav på erstatning var berettiget, jf. GDPR artikel 6, stk. 1, litra f, og artikel 9, stk. 2, litra f, jf. artikel 6, stk. 1, litra f. Tryg henviste i medfør af undtagelsesbestemmelsen i § 22 i lovbekendtgørelse nr. 289 af 8. marts 2024 (»den danske databeskyttelseslov«) til, at indsamlingen af personoplysninger i forbindelse med personovervågningen ville forspildes, hvis Tryg på forhånd informerede skadelidte (den registrerede) herom.

Tryg informerede tillige Datatilsynet om, at ved bekræftelsen af forsikringssvindel opfyldte Tryg oplysningspligten 30 dage efter afslutning af personovervågningen. Kunne forsikringssvindlen afkræftes, opfyldte Tryg oplysningspligten hurtigt muligt og senest 30 dage efter afslutning af personovervågningen.

Datatilsynet fandt, at Trygs procedurer for opfyldelse af oplysningspligten efter GDPR artikel 14 var inden for rammerne af databeskyttelsesreglerne, herunder GDPR artikel 5, stk. 1, og 14 og den danske databeskyttelseslovs § 22.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/feb/datatilsynet-har-undersoegt-oplysningspligten-hos-tryg-forsikring-as

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/datatilsynet-undersoeger-oplysningspligten-hos-tryg-forsikring-as-

Datatilsynet politianmelder Odsherred Kommune for ikke at leve op til kravene om et passende sikkerhedsniveau i databeskyttelsesforordningen

Det danske Datatilsyn (»Datatilsynet«) oplyste i en pressemeddelelse den 11. januar 2024, at det har politianmeldt Odsherred Kommune for ikke at have levet op til kravene om et passende sikkerhedsniveau, der følger af GDPR, ved ikke at have krypteret harddiskene på kommunens cirka 1200 bærbare computere.

Under behandlingen af en sag angående et brud på sikkerheden af personoplysninger ved et tyveri af en medarbejders bærbare computer, hvor harddisken ikke var krypteret, konstaterede Datatilsynet, at Odsherred Kommune ikke havde krypteret kommunens cirka 1200 bærbare computere i perioden fra d. 18. maj 2018 til d. 10. september 2022. Datatilsynet udtalte, at det efter GDPR artikel 32 oftest er en nødvendig og påkrævet sikkerhedsforanstaltning at kryptere bærbare enheder, herunder bærbare computere, der behandler personoplysninger. Dette understøttes bl.a. af, at kryptering eksplicit nævnes som eksempel på relevant teknisk foranstaltning efter GDPR artikel 32, stk. 1, litra a.

Datatilsynet indstillede Odsherred Kommune til en bøde på 100.000–200.000 kr., og lagde i vurderingen bl.a. vægt på at kryptering af bærbare enheder er en basal og væsentlig sikkerhedsforanstaltning, samt at kryptering må anses for at være en almindelig anvendt teknologi, der har været *best practice* siden 2007. Der var derfor efter Datatilsynets vurdering tale om en alvorlig overtrædelse af kravene til behandlingssikkerhed i medfør af GDPR.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/odsherred-kommune-indstilles-til-boede

Datatilsynet indstiller Netcompany til en bøde på 15 mio. kr.

Det danske Datatilsyn (»Datatilsynet«) oplyste i en pressemeddelelse den 12. januar 2024, at det har politianmeldt Netcompany for at have overtrådt GDPR ved ikke at have sikret et passende sikkerhedsniveau ved udviklingen af mit.dk.

Netcompany, som driver og ejer it-løsningen mit.dk, anvendte ved udviklingen af en komponent i mit.dk en uhensigtsmæssig kodning, der gjorde, at brugere af mit.dk fik uberettiget adgang til andre brugeres digitale post og dermed personoplysninger. Kort efter lanceringen af mit.dk blev kodningen udbedret. Den uhensigtsmæssige kodning blev ikke opdaget ved gennemførelsen af test, herunder kodereview,

statisk kodeanalyse og performancetest, inden lanceringen af mit.dk.

Datatilsynet fandt, at det var en særligt kritisk og åbenbar risiko ved løsningen, at andre brugere fik uautoriseret adgang til digital post, og at der derfor skulle være udarbejdet en konsekvensanalyse, jf. GDPR artikel 35 om konsekvensanalyse.

Datatilsynet politianmeldte og indstillede herved Netcompany til en bøde på mindst 15 mio. kr. for at have overtrådt GDPR, hvilket er den største bøde, Datatilsynet hidtil har indstillet til for en overtrædelse af GDPR.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/netcompany-indstilles-til-boede

Datatilsynet offentliggør ny tilsynsplan for 2024

Det danske Datatilsyn (»Datatilsynet«) har i en pressemeddelelse den 15. januar 2024 offentliggjort de temaer, der vil have et særligt fokus i deres tilsynsarbejde dette år. Datatilsynets aktiviteter omfatter blandt andet vejledning, rådgivning, klagesagsbehandling, internationalt arbejde og målrettede tilsynsaktiviteter.

Temaerne er, blandt andet, brugen af kunstig intelligens, overvågning af ansatte, samt behandlingen af personoplysninger i fælleseuropæiske informationssystemer.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/jan/hvad-fokuserer-datatilsynet-paa-i-2024

Læs Datatilsynets tilsynsaktiviteter her: https://www.datatilsynet.dk/afgoerelser/generelt-om-tilsyn/saerlige-fokusomraader-for-datatilsynets-tilsynsaktiviteter-i-2024

Datatilsynet træffer afgørelser om behandlingssikkerheden ved kommuners brug af AULA

Det danske Datatilsyn (»Datatilsynet«) oplyste i en pressemeddelelse den 16. januar 2024, at de havde truffet afgørelse i fem sager med udvalgte kommuner efter en samlet behandling, som drejede sig om behandlingssikkerheden vedrørende behandlingen af personoplysninger i it-systemet AULA. Datatilsynet havde i 2019 truffet en afgørelse, hvor kommunerne blev anset som dataansvarlige efter GDPR artikel 4, nr. 7.

Kernen i sagen angik kommunernes pligt til at udarbejde en konsekvensanalyse, jf. GDPR artikel 35. Datatilsynet udtalte kritik til tre ud af fem kommuner, hvis konsekvensanalyser ikke levede op til mindstekravene efter GDPR artikel 35, stk. 7. Datatilsynet har rettet kritik af risikovurderingen vedrørende dokumentationskravet om identifikation, nedbringelse af risici samt manglende identifikation og implementering af relevante foranstaltninger. To ud af fem kommunerne modtog imidlertid alvorlig kritik på baggrund af et fuldstændigt fravær af en konsekvensanalyse, hvorfor de fik påbud om at udarbejde sådanne, jf. GDPR artikel 58, stk. 2, litra d.

Den dataansvarlige har efter GDPR pligt til at forholde sig til risikoen for den registreredes rettigheder og frihedsrettigheder og skal identificere risici ved behandling af personoplysninger og sikre et passende sikkerhedsniveau gennem en række foranstaltninger, jf. GDPR artikel 32, stk. 1, artikel 24, stk. 1, og artikel 5. I den forbindelse udtalte Datatilsynet, at idet kommunerne som dataansvarlige vil foretage samme behandlingsaktivitet, kan de med fordel foretage en fælles konsekvensanalyse, henset til at det samme type system, indsamlede personoplysninger, risici involveret, samt leverandør ligger til grund for databehandlingen.

Læs Datatilsynets pressemeddelelse og afgørelser her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/jan/tilsyn-med-kommuner-om-sikkerheden-i-aula

Databeskyttelsesreglerne ikke til hinder for offentliggørelse af AI-model og tilhørende datasæt, såfremt personoplysninger var indhentet og behandlet lovligt

Det danske Datatilsyn (»Datatilsynet«) tog den 19. januar 2024 i en sag med journalnummer 2023-212-0021 stilling til, hvorvidt Sønderborg Kommune lovligt kunne offentliggøre et datasæt som var benyttet til udvikling af en AI model, samt om kommunen lovligt kunne offentliggøre selve AI modellen.

Vedrørende selve AI-modellen kom Datatilsynet frem til, at der ikke var tale om personoplysninger, hvorfor AI-modellen ikke var omfattet af reglerne i GDPR.

Vedrørende datasættet, som var benyttet til udviklingen af AI-modellen, kom Datatilsynet frem til, at der var sket en lovlig indsamling og behandling af personoplysningerne i forbindelse med udviklingen af AI-modellen, der skulle hjælpe kommunen i aktindsigtsager under henvisning til lovbekendtgørelse nr. 145 af 24. februar 2020 (»den danske offentlighedslov«) og lovbekendtgørelse nr. 433 af 22. april 2014 (»den danske forvaltningslov«).

GDPR artikel 6, stk. 1, litra e, udgør behandlingshjemmel for offentlige myndigheders behandling af personoplysninger som led i offentlig myndighedsudøvelse. Det er efter GDPR artikel 6, stk. 3, litra b, jf. stk. 2, en forudsætning, at der foreligger en supplerende national lov, som den dataansvarlige er underlagt og forpligter myndigheden til at udføre en specifik opgave.

Det var Datatilsynets vurdering, at den danske offentligheds- og forvaltningslovs bestemmelser om kommunernes pligt til håndtering af aktindsigtsanmodninger udgjorde et nationalt retsgrundlag og således berettigede behandlingen af personoplysningerne til udviklingen af AI-modellen jf. GDPR artikel 6,

stk. 3, litra b, jf. artikel 6, stk. 1, litra e.

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/offentliggoerelse-af-datasaet-og-ai-model

Datatilsynet udsteder påbud i Chromebook-sag

Det danske Datatilsyn (»Datatilsynet«) traf den 30. januar 2024 afgørelse i en sag, med journalnummer 2023-431-0001, vedrørende brugen af Google Workspace i folkeskolerne. Tilsynet konstaterede, at der ikke er lovhjemmel til at videregive personoplysninger til Google til alle de formål, der praktiseres i dag. Afgørelsen kom i kølvandet på materiale, der blev indsendt af KL på vegne af 53 kommuner.

Datatilsynet fandt, at der mangler en klar hjemmel i lovbekendtgørelse nr. 90 af 29. januar 2024 (»den danske folkeskolelov«) til at videregive elevernes oplysninger til Google til visse formål som vedligeholdelse og forbedring af tjenesterne. Derfor påbød Datatilsynet kommunerne at bringe behandlingen i overensstemmelse med reglerne i GDPR artikel 1, stk. 1, litra a, og artikel 6, stk. 1. Dette kan opnås ved enten at stoppe videregivelsen af personoplysninger til Google til disse formål, få Google til at ophøre med behandlingen af oplysningerne til disse formål, eller ved at Folketinget skaber et klart retsgrundlag for videregivelsen.

Kommunerne skal efterleve påbuddet fra den 1. august 2024, men skal senest den 1. marts indikere, hvordan de har til hensigt at overholde det. Datatilsynet vil herefter informere kommunerne om eventuelle yderligere forhold, der skal behandles inden påbudsfristen, afhængigt af kommunernes tilbagemelding.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/jan/datatilsynet-giver-paabud-i-chromebook-sag

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/datatilsynet-giver-paabud-i-chromebook-sag

Datatilsynet har taget stilling til muligheden for at etablere og dele et datasæt, der skal bruges til udvikling af dansk sprogteknologi

Det danske Datatilsyn (»Datatilsynet«) udtalte sig den 30. januar 2024, efter anmodning fra Alexandra Instituttet, om instituttets mulighed for at etablere og dele datasæt indeholdende lydoptagelser. Sagen har journalnummer 2023-211-0004.

Instituttet ønskede at lave et datasæt, der skulle indeholde lydoptagelser af personer af forskellige køn, aldre og geografiske ophav som oplæser og indtaler danske tekster. Den indtalte tekst ville ikke indeholde personoplysninger, men lydfilen ville være tilknyttet overordnet information om oplæseren, herunder køn, alder og omtrentlig geografisk placering.

Spørgsmålene for Datatilsynet var herefter, om der forelå et behandlingsgrundlag i relation til etablering og deling af sådanne datasæt, om der reelt ville ske anonymisering samt, hvorvidt der var tale om behandling af særlige kategorier af personoplysninger.

Datatilsynet udtalte, at behandlingsgrundlaget fandtes i GDPR artikel 6, stk. 1, litra b, om opfyldelse af kontrakt, idet indspilning af de omhandlede lydoptagelser var den primære kontraktlige ydelse og hovedformålet med aftalen mellem Alexandra Instituttet og den registrerede. Kontraktens hovedformål kunne ikke opfyldes uden indspilningen af lydoptagelserne, hvormed behandlingen kunne ske.

Datatilsynet udtalte desuden, at lydoptagelserne skulle anses for personoplysninger, idet det gjorde det muligt indirekte at identificere personen på optagelserne. Datatilsynet henviste til den stigende adgang til og anvendelse af stemmegenkendelsesværktøjer og kunstig intelligens.

Afslutningsvis udtalte Datatilsynet, at datasættet ikke ville være omfattet af GDPR artikel 9, om forbud mod at behandle særlige kategorier af personoplysninger, idet formålet med behandlingen ikke var entydigt at identificere en person.

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/etablering-og-deling-af-datasaet

Datatilsynet indstiller Privathospitalet Capio A/S til bøde for manglende tilsyn med databehandlere

Det danske Datatilsyn (»Datatilsynet«) har politianmeldt Capio A/S for manglende tilsyn med databehandlere. Det oplyste Datatilsynet i en pressemeddelelse d. 1. februar 2024.

Forud for politianmeldelsen havde Datatilsynet foretaget en undersøgelse af Capio A/S' håndtering af databehandlere, hvor Datatilsynet udvalgte tre tilfældige af privathospitalets databehandlere til at være genstand for undersøgelse.

Resultaterne af Datatilsynets undersøgelse af Capio A/S' tilsyn med de tre databehandlere afslørede, at privathospitalet ikke havde udført det nødvendige tilsyn. Capio A/S´ indledte først deres første tilsyn med hver enkelt databehandler, da Datatilsynet havde påbegyndt deres undersøgelse af privathospitalet.

Datatilsynet vurderede, at privathospitalet ikke kunne dokumentere, at personoplysningerne blev behandlet i overensstemmelse med lovgivningen og på en sådan måde, der sikrede tilstrækkelig beskyttelse af de pågældende oplysninger, selvom de havde valgt at benytte sig af en tredjepart (en databehandler) til at behandle oplysningerne på deres vegne.

Datatilsynet indstillede derfor Capio A/S til en bøde på ikke under 1.500.000 kr. henset til, at der

var tale om en overtrædelse af det grundlæggende databeskyttelsesretlige princip om ansvarlighed og henset til, at overtrædelsen angik et stort antal registrerede, hvis oplysninger var i den særlige kategori af personoplysninger, navnlig følsomme oplysninger.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/feb/privathospitalet-capio-as-indstilles-til-boede

Datatilsynet udtaler sig om rækkevidden af tidligere afgørelse om Aarhus Universitetshospital

Det danske Datatilsyn (»Datatilsynet«) udtalte sig i en pressemeddelelse den 2. februar 2024 om rækkevidden af deres tidligere afgørelse over for Aarhus Universitetshospital i november 2023. Datatilsynet fastslog i afgørelsen, at Aarhus Universitetshospitals offentliggørelse af oplysninger om patienter, herunder billeder på Instagram, ikke kunne ske på baggrund af et samtykke fra patienten, at der ikke fandtes et andet gyldigt retsgrundlag for offentliggørelsen Dette skyldtes særligt det ulige forhold mellem patienten og hospitalet samt patientens typisk sårbare situation under en indlæggelse eller et behandlingsforløb.

Datatilsynet fastslog nu yderligere i pressemeddelelsen, at privathospitaler også skal følge de samme retningslinjer vedrørende offentliggørelse af personoplysninger. Datatilsynet tog i afgørelsen ikke stilling til en række forhold, såsom offentliggørelse af oplysninger efter afslutningen af et behandlingsforløb eller kontrolforløb. I pressemeddelelsen fastslog Datatilsynet, at samtykke i disse tilfælde muligvis kan opnås efter en konkret vurdering af patientens situation.

Datatilsynet udtalte, at det afgørende for vurderingen af, om et gyldigt samtykke kan indhentes, er patientens situation. Borgere i behandlingssituationer er typisk sårbare, og dette kan skabe en ulighed i forholdet mellem borgeren og personalet, hvilket kan påvirke samtykkets frivillighed. Det er blandt andet dette, der åbner muligheden for, at frivilligt samtykke kan gives efter behandlingsforløbet er afsluttet.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/feb/nyt-om-raekkevidden-af-auh-afgoerelsen

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/nov/hospital-kan-ikke-bruge-samtykke-til-at-offentliggoere-billeder-af-patienter-paa-instagram

Datatilsynet forholder sig til Chromebook-sagens relevans for brug af andre cloudservices

Den 28. februar 2024 angav det danske Datatilsyn (»Datatilsynet«) i en pressemeddelelse, at de havde taget stilling til en henvendelse fra Region Syddanmark med journalnummer 2023-431-0012. Henvendelsen skete i forlængelse af Datatilsynets afgørelse i den såkaldte Chromebook-sag, hvor Datatilsynet vurderede, at der ikke var hjemmel til at videregive personoplysninger til Google til alle de formål, som de tidligere blev videregivet til. Region Syddanmark ønskede nu oplyst, hvorvidt Chromebook-sagen har relevans for anskaffelse og brug af andre cloudservices. I dette tilfælde angik spørgsmålet specifikt Microsoft som cloudserviceleverandør.

I Datatilsynets svar til Region Syddanmark lagde de vægt på, at det i Chromebook-sagen fremgik som en grundlæggende forudsætning for lovlig behandling af personoplysninger, at den dataansvarlige havde kendskab til og havde kortlagt, hvilke oplysninger der blev behandlet, samt til hvilke formål. Ifølge Datatilsynet omfattede dette en afdækning af, om cloudserviceleverandøren behandlede personoplysningerne til egne formål.

Ud fra de af Region Syddanmark fremsendte oplysninger vurderede Datatilsynet, at det ikke var klart, om Microsoft ville behandle personoplysningerne til egne formål. Datatilsynet anviste derfor en række forhold, som Region Syddanmark skulle kortlægge og afklare. I den forbindelse understregede Datatilsynet, at det er den dataansvarliges opgave at dokumentere, at behandlingen er lovlig, uanset valget af standardiserede eller skræddersyede løsninger.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/feb/chromebook-sagens-relevans-for-andre-organisationer-og-cloudservices

Læs Datatilsynets svar her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/feb/region-syddanmarks-paataenkte-brug-af-microsoft-365

Datatilsynet træffer afgørelse om brugen af cookie-walls på berlingske.dk

Det danske Datatilsyn (»Datatilsynet«) oplyste den 11. marts 2024 at de havde truffet afgørelse om Berlingske.dks brug af cookie-walls i en sag med journalnummer 2023-431-0010.

Berlingske.dk brugte på sin hjemmeside cookie-walls, der forhindrede brugerne af hjemmesiden i at tilgå indlejret delindhold som eksempelvis et blogindlæg. Brugerne kunne kun tilgå delindholdet, hvis de accepterede Berlingske.dks behandling af sine personoplysninger til statistiske og markedsføringsformål.

For at en samtykkebaseret behandling af personoplysninger kan leve op til kravene efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«), skal behandlingen være baseret på et samtykke til ét eller flere specifikke formål, jf. GDPR artikel 6, stk. 1, litra a, og samtykket skal være frivilligt, specifikt, informeret og utvetydigt, jf. GDPR artikel 4, nr. 11.

Datatilsynet fandt, at Berlingske.dk ikke levede op til GDPR artikel 6, stk. 1, litra a og artikel 4, nr. 11, ved at betinge adgangen til delind-

holdet af behandling af personoplysninger til statiske og markedsføringsformål. Den registrerede havde ikke mulighed for at tilgå indholdet på anden måde, hvorfor Datatilsynet fandt, at der reelt ikke var tale om et frivilligt samtykke. Berlingske blev derfor meddelt påbud om at bringe samtykkeløsningen i overensstemmelse med GDPR's krav til et gyldigt samtykke.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/mar/ugyldigt-samtykke-i-cookie-walls-paa-berlingskedk

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/feb/ugyldigt-samtykke-i-cookie-walls-paa-berlingskedk#_ftn2

Datatilsynet har truffet afgørelser om parkeringsselskabers overholdelse af oplysningspligten

Det danske Datatilsyn (»Datatilsynet«) oplyste i pressemeddelelse den 20. marts 2024, at det havde gennemført en undersøgelse af oplysningspligten hos tre parkeringsselskaber og har nu fuldført tilsynsprocessen med fokus på virksomhedernes overholdelse af oplysningspligten ved udstedelse af parkeringsafgifter.

Datatilsynet valgte at rette deres fokus på tre større parkeringsselskaber og undersøge, hvordan de håndterede oplysningspligten. I to tilfælde udtrykte Datatilsynet kritik, idet selskaberne undlod at informere de registrerede (parkanterne) om behandlingen af deres personoplysninger ved opkrævning af parkeringsafgifter.

Datatilsynet lagde vægt på, at disse selskaber forsømte at informere parkanterne om, hvordan deres personoplysninger blev behandlet efter GDPR artikel 14 i forbindelse med udstedelse af parkeringsafgifter, og fastslog, at sådan information skulle gives senest ved udstedelsen af parkeringsafgiften. Datatilsynet understregede, at den dataansvarlige virksomhed skal træffe aktive foranstaltninger for at sikre overholdelse af oplysningspligten, og det at have oplysningerne tilgængelige på en hjemmeside ikke anses for tilstrækkeligt.

Datatilsynet konkluderede, at et af de undersøgte selskaber opfyldte sin oplysningspligt ved at inkludere en henvisning til virksomhedens persondatapolitik i deres betalingspåkrav. Derved blev de registrerede (parkanterne) rettidigt informeret om behandlingen af deres personoplysninger.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/mar/datatilsynet-har-undersoegt-oplysningspligten-hos-tre-parkeringsselskaber

Læs afgørelsen om Avantpark her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/datatilsynet-har-undersoegt-oplysningspligten-hos-tre-parkeringsselskaber-avantpark

Læs afgørelsen om Oparko her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/datatilsynet-har-undersoegt-oplysningspligten-hos-tre-parkeringsselskaber-oparko-aps

Læs det afsluttende brev om Parkzone her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/datatilsynet-har-undersoegt-oplysningspligten-hos-tre-parkeringsselskaber-parkzone

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

Illustrasjon: Colourbox.com


simonsen vogtwiig

Henning Wahlberg og Rune Ljostad

Kjennelse om bevisfritaket for forretningshemmeligheter i tvist om varemerkeinngrep

Borgarting lagmannsrett avsa 12. april 2024 kjennelse om bevistilgang i sak mellom Mondelez Norge AS (Mondelez) og Orkla Confectionery & Snacks Norge AS (Orkla). Orkla har krevd forbud mot markedsføring og salg av Freia Boble Melkesjokolade, begrunnet i at emballasjen er for lik Nidars Stratos-emballasje. Orkla anfører at dette utgjør inngrep i deres varemerkerett, og brudd på god forretningsskikk.

Ved inngrep i varemerkerett og brudd på god forretningsskikk har den forurettede krav på vederlag og/eller erstatning etter flere ulike alternativer (varemerkeloven § 58 og markedsføringsloven § 48 b tredje ledd), hvor det alternativet som er gunstigst for forurettede skal legges til grunn. Ett av disse alternativene er et «vederlag svarende til vinningen som er oppnådd ved overtredelsen». Orkla anførte at for at det skal være mulig å utmåle en slik vinningsavståelse, er det nødvendig å få tilgang til Mondelez' regnskapsdokumentasjon for å fastslå hva vinningen er.

Begge partene var enige om at slik regnskapsdokumentasjon inneholder forretningshemmeligheter. Etter tvisteloven § 22-10 første punktum er dette underlagt bevisfritak. Etter annet punktum følger det imidlertid at retten likevel kan gi pålegg om at beviset skal gjøres tilgjengelig når den etter en avveining finner det påkrevd. Spørsmålet var altså om lagmannsretten fant dette påkrevd.

Lagmannsretten viste til at et slikt pålegg må være sterkt begrunnet, og må veie hensynet til sakens rette opplysning mot hemmelighold. Retten viste til at lukkede dører og at de tilstedeværende gis pålegg om taushetsplikt kan avbøte noe av skadevirkningene ved å pålegge bevistilgang, men at dette er mindre egnet i saker hvor motparten er en konkurrent. I slike saker vil dessuten terskelen for å gi pålegg om bevistilgang være høyere.

Retten viste også til at reglene om vinningsavståelse ved inngrep i immaterielle rettigheter ble innført i 2013, som ledd i lovendringer som skulle styrke rettighetshaveres stilling ved inngrep. En rettighetshaver som krever vinningsavståelse, må føre bevis for vinningens størrelse, og retten viser til at disse opplysningene vil rettighetshaver som overveiende hovedregel ikke ha tilgang til. Følgelig uttalte retten at rettighetshaver, for å kunne påberope seg vinningsavståelse, har et «sterkt og reelt behov» for bevistilgang. Uten pålegg om bevisfremleggelse ville kravet på vinningsavståelse bli gjort ineffektivt. Det ble også vist til at begjæringen var begrenset til fortjeneste ved ett enkelt produkt innenfor en bredt portefølje av produkter, noe som etter lagmannsrettens syn innebar at ulempen for Mondelez var begrenset.

Etter en samlet vurdering kom derfor retten til at Mondelez måtte fremlegge dokumentasjonen. Deretter ble det vurdert om Mondelez kunne skaffe dokumentasjonen til veie etter tvisteloven § 26-5 første ledd. Retten mente det har formodningen mot seg at ikke Mondelez ikke allerede har denne informasjonen, men mente de uansett kunne skaffe dette til veie fra Mondelez-konsernet uten særlige vanskeligheter.

Saken er publisert i Lovdata under *LB-2024-53756*.

Ny avgjørelse fra Oslo tingrett om vederlag for bruk av bilder

Saken gjaldt vederlag for bruk av fotografi. Et oppstartsselskap hadde i april 2022 lagt ut et blogginnlegg på sine nettsider illustrert med et bilde av fasaden på Norges Bank. Selskapet hadde lagt ut bildet uten tillatelse fra fotografen. Fotografier er vernet etter åndsverkloven § 23, og etter henvendelse fra fotografen ble bildet slettet. Det var enighet om at bruken var uhjemlet og at fotografen hadde krav på et rimelig vederlag for bruken. Uenigheten dreide seg om hva som utgjør et slikt rimelig vederlag.

Et grunnvilkår for vederlag og erstatning etter åndsverkloven § 81 er at inngrepet ble gjort forsettlig eller uaktsomt. Selskapet hadde opplyst at de hadde søkt etter et gratis illustrasjonsbilde til blogginnlegget, og at de trodde bilde kunne brukes gratis. Tingretten var imidlertid ikke enig i dette, som fant at selskapet i det minste hadde opptrådt uaktsomt.

Når det gjelder utmålingen, viste retten til forarbeidene som sier at et rimelig vederlag skal avgjøres ut fra omfanget av bruken, den økonomiske verdien for overtrederen, vanlig bransjestandard eller praksis og andre konkrete forhold. Dersom bransjestandard eller praksis ikke gir veiledning, må det fastsettes ut fra en skjønnsmessig vurdering av hva som ut fra rettighetens verdi utgjør et rimelig vederlag for bruken.

Retten viste til at markedsprisen for slike type bilder vil være sentralt, og at omfanget av bruken var begrenset. Bloggposten var publisert i fire måneder med 120 unike besøkende. Den økonomiske verdien av bruken var derfor beskjeden.

Oslo tingrett har tidligere behandlet to saker om lignende bruk av bilder fra den samme fotografen. Disse gjaldt enkle illustrasjonsbilder for høytidsmarkering og bilder av det norske flagget. Fotografen hadde tidligere krevd et beløp i samsvar med Norsk Journalistslags veiledende satser. Retten mente imidlertid at det ikke var noen automatikk i å bruke disse satsene.

Retten oppfattet bildet av Norges Bank som et nokså generisk bilde, og viste til at flere billedbanker tilbyr lignende bilder enten gratis eller til langt lavere pris enn det fotografen krever. Disse enkeltlisensene lå omkring kr 550 til 625. Retten fant derfor, etter en samlet vurdering, at et vederlag skulle settes til kr 500 ekskl. mva. Retten fant videre at bruken var grovt uaktsom ettersom selskapet ikke hadde gjort noen videre undersøkelser før bruken, og i samsvar med åndsverkloven § 81 annet ledd idømte retten derfor det dobbelte av rimelig vederlag.

Saken er publisert i Lovdata under *TOSL-2023-95386*.

Henning Wahlberg er advokatfullmektig i Advokatfirmaet Simonsen Vogt Wiig AS.

Rune Ljostad er advokat (H) og assosiert partner i Advokatfirmaet Simonsen Vogt Wiig AS og leder firmaets faggruppe for IP. Han har prosedert flere prinsipielle saker innen IP og personvern

Illustrasjon: Colourbox.com

Gorrissen Federspiel

Tue Goldschmieding

Varemærket »Technical Merino« var ikke blot en deskriptiv betegnelse

Sø- og Handelsretten afsagde den 10. januar 2024 kendelse i sagen BS-33943/2023-SHR mellem Herning Fabrics A/S (»Herning Fabrics«) over for OPUS ONE A/S og Geoff Anderson Danmark ApS (»Opus One«). Tvisten i sagen, der var en begæring om forbud og påbud, var, hvorvidt Opus Ones brug af betegnelsen »Technical Merino« for beklædningsgenstande udgjorde en krænkelse af Herning Fabrics EU-varemærkerettigheder, jf. Europa-Parlamentets og Rådets forordning (EU) 2017/1001 af 14. juni 2017 om EU-varemærker (»varemærkeforordningen«) artikel 42, stk. 1, jf. artikel 7, stk. 1, litra c og d.

Sø- og Handelsretten skulle tage stilling til gyldigheden af Herning Fabrics registrerede EU-varemærke »Technical Merino«, og om Opus Ones anvendelse af betegnelsen »Technical Merino« udgjorde en overtrædelse af varemærkerettighederne grundet forvekslingsrisiko, jf. varemærkeforordningens artikel 9, stk. 2, litra b.

Sø- og Handelsretten fandt indledningsvist, at der var en formodning for, at Herning Fabrics havde en gyldig varemærkeret, idet registreringen af figurmærket Technical Merino var sket efter EUIPOs prøvelse af, om varemærket var udelukket fra registrering på grund af beskrivende angivelser. Retten fandt desuden, at Opus One ikke havde løftet bevisbyrden for, at varemærket »Technical Marino« var deskriptiv og dermed ugyldig. Retten fandt heller ikke, at rettighederne var fortabt på grund af manglende reel brug, jf. varemærkeforordningens artikel 18.

Retten fandt herefter, at de Opus Ones brug af betegnelsen »Technical Merino« sandsynligvis udgjorde en krænkelse af sagsøgers varemærkerettigheder, da det skabte forvekslingsrisiko blandt forbrugerne.

På den baggrund besluttede Sø- og Handelsretten at meddele det anmodede forbud og påbud.

Læs kendelsen her: https://domstol.fe1.tangora.com/media/-300011/files/Kendelse_BS-33943-2023-SHR.pdf

Forbrugerombudsmanden har politianmeldt Copenhagen Cartel for overtrædelse af vildledningsforbuddet

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) oplyste i en pressemeddelelse d. 18. januar 2024, at den havde politianmeldt Copenhagen Cartel, for at have markedsført sine produkter med udsagn, der gav forbrugerne indtrykket af, at deres produkter var fremstillet af genanvendte fiskenet og plastisk fra havet i et større omfang, end hvad virksomheden kunne dokumentere.

Virksomheden havde i deres markedsføring brugt udsagn som: »Made from ocean waste« og »Saving the ocean one product at a time«. Dog kunne virksomheden kun dokumentere, at en lille del af deres materiale stammer fra fiskenet og andet plastik, der specifikt er hevet op af havet. Virksomhedens udsagn var i strid med lovbekendtgørelse nr. 866 af 15 juni 2022 (»den danske markedsføringslov«) § 13, om en virksomhed skal kunne dokumentere rigtigheden af oplysninger om faktiske forhold.

Forbrugerombudsmanden vurderede, at de udsagn, som Copenhagen Cartel havde benyttet i sin markedsføring, var egnede til at give forbrugerne et fejlagtigt indtryk af, at virksomhedens produkter udelukkende eller hovedsageligt består af genanvendt plastisk fra havet, og at produkterne bidrog til at redde havet i større omfang, end det reelt var tilfældet.

Efter Forbrugerombudsmandens henvendelse ophørte Copenhagen Cartel med at anvende en del af de påtalte udsagn og deres tidligere markedsføring af udsagnene er blevet fjernet fra alle virksomhedens platforme.

Læs Forbrugerombudsmandens pressemeddelelse her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2024/20240118-forbrugerombudsmanden-politianmelder-copenhagen-cartel-for-overtraedelse-af-vildledningsforbuddet/

Forbrugerombudsmanden har vurderet, at DCC Energi A/S ikke havde dokumenteret CO2-kompensation tilstrækkeligt

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) har i en sag om CO2-kompensation vurderet, at virksomheden der tilbød CO2-kompensationen ikke havde dokumenteret kompensationen tilstrækkeligt, hvilket var i strid med dokumentationskravet og vildledningsforbuddet i lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«). Dette oplyste Forbrugerombuds-

manden i en pressemeddelelse dateret 24. januar 2024.

På Shell-tankstationer, der drives af DCC Energi A/S under licens, kunne kunder vælge at betale ekstra for brændstof, således at de ekstra penge blev brugt til CO2-kompensation gennem støtte til skovbevarelsesprojekter, hvorved skovrydning blev undgået. Kompensationen kunne også opnås ved brug af Shell Card, der ligeledes drives af DCC Energi A/S. Markedsføringen var ifølge Forbrugerombudsmanden egnet til at give forbrugerne det indtryk, at tilvalg af CO2-kompensation kunne kompensere CO2-udledningen fra deres brændstofforbrug.

Forbrugerombudsmanden vurderede, at dokumentationen *sandsynliggjorde*, at skovrydning ville finde sted, hvis skovområderne ikke blev støttet af skovbevarelsesprojekterne. Dog fandt Forbrugerombudsmanden ikke, at skovrydning *faktisk* ville finde sted, hvis skovområderne ikke blev støttet af skovbevarelsesprojekterne. Derfor fandt Forbrugerombudsmanden, at dokumentationskravet i den danske markedsføringslovs § 13 ikke var opfyldt. Det var Forbrugerombudsmandens opfattelse, at markedsføringen var egnet til at vildlede forbrugerne om CO2-kompensationens klimaeffekt, hvilket var i strid med vildledningsforbuddet i den danske markedsføringslovs § 5 og § 6, jf. § 8.

Læs Forbrugerombudsmandens pressemeddelelse her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2024/20240124-ikke-tilstraekkeligt-at-sandsynliggoere-rigtigheden-af-co2-kompensation/

Forbrugerombudsmanden opdaterer deres vejledning om markedsføring for børn og unge

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) oplyste den 1. februar 2024 i en pressemeddelelse, at Forbrugerombudsmanden har opdateret sin vejledning omkring de regler, der gælder for markedsføring for børn og unge under 18 år. Disse regler er en del af lovbekendtgørelse nr. 866 af 15 juni 2022's (»den danske markedsføringslov«) og er designet til at beskytte de unge forbrugere mod skadelige påvirkninger.

Den opdaterede vejledning indeholder eksempler fra danske domme, lovbemærkninger og vejledning fra EU-Kommissionen om urimelig handelspraksis.

Ved markedsføring rettet mod børn og unge anbefaler Forbrugerombudsmanden, at reklamer klart markeres med »REKLAME« i starten af et opslag. Desuden fremgår det af den opdaterede vejledning, at sådan markedsføring ikke må opfordre til vold, indeholde omtale af rusmidler eller uegnede produkter, udføres på profiler, der tilhører eller fremstår som tilhørende børn under 15 år, anvende børn i markedsføring på sociale medier uden for en naturlig sammenhæng, eller direkte opfordre børn til køb eller til at overtale deres forældre til at købe et produkt.

Det er desuden klargjort, hvornår influenter anses for erhvervsdrivende og dermed skal overholde den danske markedsføringslov, og hvad der ikke anses for tilstrækkelig reklamemarkering.

Læs Forbrugerombudsmandens pressemeddelelse her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2024/24020201-forbrugerombudsmanden-saetter-fokus-paa-boern-unge-og-sociale-medier/

Betegnelsen »Kokkedal Slot Copenhagen« udgjorde en forvekslingsrisiko med varemærket »Kokkedal Slot«

Sø- og Handelsretten afsagde den 9. februar 2024 dom i sagen BS-10686/2017-SHR mellem Kokkedal Slot v/Ann Vibeke Lokdam (»Kokkedal Slot«) over for Kokkedal Slot ApS og Slotshotellet ApS (»Slotshotellet«). Sagen angik, om Slotshotellet havde krænket Kokkedal Slots varemærkerettigheder til betegnelsen »Kokkedal Slot« ved at anvende betegnelsen »Kokkedal Slot Copenhagen«, jf. lovbekendtgørelse 2019-01-29 nr. 88 (»den danske varemærkelov«) § 4, stk. 2, nr. 2.

Kokkedal Slot nedlagde påstand om, at Slotshotellet ikke var berettiget til erhvervsmæssig brug af kendetegnet »Kokkedal Slot« i forbindelse med deres virksomhed, der omfattede tilvejebringelse af mad og drikke samt indkvartering og forskellige former for arrangementer.

Sø- og Handelsretten fandt indledningsvist, at anvendelsen af betegnelsen »Kokkedal Slot Copenhagen« udgjorde en krænkelse af varemærket »Kokkedal Slot«, jf. den danske varemærkelovs § 4, stk. 2, nr. 2. Retten lagde særlig vægt på forvekslingsrisikoen mellem de to betegnelser, idet begge parter opererede inden for samme branche og geografisk område, hvilket kunne føre til forvirring blandt forbrugerne. Dette blev ligeledes anset for at være i strid med god markedsføringsskik, jf. lovbekendtgørelse 2022-06-15 nr. 866 om markedsføring (»den danske markedsføringslov«) §§ 3 og 22, jf. tillige lovbekendtgørelse 2023-09-01 nr. 1168 om aktie- og anpartsselskaber (»den danske selskabslov«) § 2, stk. 2, og lov 2014-02-26 nr. 164om internetdomæner (»den danske domænelovs«) § 25.

På den baggrund blev Slotshotellet pålagt at anerkende, at de ikke havde ret til erhvervsmæssig brug af kendetegnet »Kokkedal Slot«, at tilbagekalde og destruere markedsføringsmaterialet og at betale Kokkedal slot erstatning.

Læs dommen her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_-_BS-10686-2017-SHR.pdf

Sag om krænkelse af gummiklodser til brug for håndtering og transport af vindmøllekomponenter ender med frifindelse

Sø- og Handelsretten afsagde den 16. februar 2024 kendelse i sag BS-49516/2023-SHR mellem Dansk Gummi Industri A/S (»DGI«) og A.A.G. Aalborg Gummivarefabrik A/S (»AAG«).

Tvisten i sagen angik, hvorvidt det var godtgjort eller sandsynliggjort, at AAG' gummiklods krænkede DGI's rettigheder baseret på to EU-designregistreringer.

DGI påstod, at AAG havde krænket DGI's rettigheder efter Forordning (EF) nr. 6 /2002 af 12. december 2001 (»designforordningen«), og nedlagde påstand om forbud mod fremstilling, markedsføring og salg af produktet.

Sø- og Handelsretten fandt, at DGI's registrerede design bar stærkt præg af at være funktionelt bestemt, hvorfor beskyttelsesomfanget var snævert.

Derudover fandt retten, at det havde formodningen for sig, at DGI havde en gyldig EU-designrettighed, jf. designforordningens artikel 85, uanset at EUIPO's afgørelse herom var påklaget og under behandling.

Sø- og Handelsretten fandt desuden, at AAG's produkt gav den informerede bruger et andet helhedsindtryk end DGI's designregistreringer, da der forelå visuelle forskelle imellem de to produkter. Dermed fandt retten, at DGI ikke havde sandsynliggjort, at AAG's produkt krænkede DGI's EU-registrerede produkt, jf. designforordningens artikel 10, og at betingelserne for at nedlægge forbud derfor ikke var opfyldt, jf. lovbekendtgørelse nr. 250 af 4. marts 2024 (»den danske retsplejelov«) § 413, nr. 1.

På denne baggrund gav Sø- og Handelsretten ikke DGI medhold i deres påstand om forbud mod salg mv. i Danmark.

Læs kendelsen her: https://domstol.fe1.tangora.com/media/-300011/files/Kendelse_BS-49516-2023-SHR.pdf

Forbrugerombudsmanden slår ned på forsikringsselskabs vildledende og aggressive markedsføring

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) traf den 19. februar 2024 afgørelse i en sag med sagsnummer 22/08714 om et forsikringsselskabs markedsføring.

Forbrugerombudsmanden fandt, at forsikringsselskabet havde overtrådt lovbekendtgørelse nr. 866 af 15 juni 2022 (»den danske markedsføringslov«) bestemmelser ved at anvende vildledende og aggressiv handelspraksis til indhentning af samtykke til markedsføring. Selskabet præsenterede forbrugere, der loggede ind på dets hjemmeside, for en mulighed for at samtykke til at modtage elektronisk markedsføring. Hvis en forbruger valgte »nej«, fremkom en advarsel, der gav indtryk af, at fravalg af markedsføring ville medføre dårligere rådgivning, hvilket ikke var sandt. Dette samtykkeflow blev af Forbrugerombudsmanden vurderet som vildledende og i strid med den danske markedsføringslovs § 5 og § 6, da det fejlagtigt antydede, at optimal rådgivning kun var mulig ved samtykke til markedsføring.

Desuden anså Forbrugerombudsmanden fremgangsmåden for at udgøre en aggressiv handelspraksis, jf. den danske markedsføringslov § 7, da den begrænsede forbrugernes evne til at træffe en informeret beslutning. Forbrugerombudsmanden konkluderede, at samtykket ikke var frivilligt, utvetydigt, informeret og specificeret, og derfor ikke gyldigt ifølge § 2, stk. 14 i den danske markedsføringslov.

Som følge af Forbrugerombudsmandens henvendelse foretog forsikringsselskabet en ændring af det pågældende samtykkeflow og påbegyndte sletning af samtykker indhentet under den ulovlige praksis.

Læs Forbrugerombudsmandens pressemeddelelsen her: https://www.forbrugerombudsmanden.dk/find-sager/sager/markedsfoeringsloven/samtykke-til-markedsfoering-var-ugyldigt-da-samtykket-blev-indhentet-ved-vildledende-og-aggressiv-handelspraksis-og-derfor-ikke-var-frivilligt/

Østre Landsret træffer afgørelse i sag mellem Nord-Smil og Godt Smil om krænkelse af varemærket GODT SMIL

Østre Landsret afsagde den 22. februar 2024 dom i sag BS-24799/2023-OLR mellem Godt Smil Holding ApS (»Godt Smil«) og Tandlægerne Nord-Smil.dk Randers I/S, Tandlægerne Nord-Smil.dk Aarhus ApS og Tandlægerne Nord-Smil.dk Aalborg I/S (»Nord-Smil«). Tvisten drejede sig om, hvorvidt Nord-Smil havde krænket varemærket GODT SMIL ved at anvende denne ordkombination i sin markedsføring, herunder som Google Ads-søgeord. Sø- og Handelsretten havde i første instans givet Godt Smil medhold i krænkelsesspørgsmålet.

Spørgsmålet for landsretten angik navnlig, hvorvidt varemærket GODT SMIL var velkendt og dermed omfattet af den udvidede varemærkebeskyttelse i den danske lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) § 4, stk. 2, nr. 3.

Landsretten fandt, at Godt Smil efter bevisførelsen havde godtgjort, at varemærket var velkendt på tidspunktet for Nord-Smils anvendelse af varemærket. Landsretten lagde vægt på Godt Smils investering i markedsføring samt selskabets generelle markedsføringsstrategi. Herudover lagde landsretten vægt på en due diligence rapport, som på tidspunktet for undersøgelsen belyste at 39% af de adspurgte havde kendskab til Godt Smil, og 10% benyttede sig af en tandlæge fra Godt Smil. Landsretten vurderede, at GODT

SMIL således var velkendt på tidspunktet for udarbejdelsen af rapporten samt på tidspunktet for Nord-Smils brug af varemærket i sin annoncering.

Landsretten tilkendte herefter Godt Smil en erstatning på 250.000 kr.

Læs dommen her: https://domstol.dk/oestrelandsret/aktuelt/2024/2/ankedom-om-kraenkelse-af-varemaerket-godt-smil/

Emballagerne for Amerena Kirsebær produkter var væsentligt forskellige

Sø- og Handelsretten afsagde den 29. februar 2024 dom i sag BS-10372/2023-SHR mellem den italienske fødevareproducent Fabbri 1905 s.p.a (»Fabbri«) og den danske virksomhed Zelected Foods ApS (»Zelected«), der sælger en bred palet af forskellige fødevarer.

Tvisten i sagen angik, hvorvidt Zelected krænkede Fabbris rettigheder efter lovbekendtgørelse nr. 2023 af 20. august 2023 (»den danske ophavsretslov«) og lovbekendtgørelse nr. 426 af 1. juli 2017 (»den danske markedsføringslov«) ved at sælge og markedsføre et Amarena kirsebærprodukt i en emballage, der ifølge Fabbri udgjorde en krænkelse af Fabbris rettigheder.

Fabbri's Amarena kirsebær emballage var kendetegnet ved dens krukkelignende form med blå dekorative elementer på en hvid baggrund, der gav et klassisk udtryk.

Sø- og Handelsretten fandt indledningsvist, at Fabbris produkter og brand besidder et sådant særpræg og en sådan position på det danske marked, at det beskyttes efter § 3 om godmarkedsføringsskik i den danske markedsføringslov.

Vedrørende produkternes visuelle sammenlignelighed fandt Retten, at de to emballager fremstod forskelligartede hvad angik formen, låget og mønsteret. Selvom begge grundmønstre tog udgangspunkt i en klassisk italiensk »faenza-stil«, mente retten at der var væsentlige forskelle på mønstrenes farvetone, placering og størrelse.

Sø- og Handelsretten kom efter en samlet vurdering frem til, at de to emballager adskilte sig i en ikke ubetydelig grad. Der forelå således ikke nogen krænkelse af Fabbris ophavs- og markedsføringsret, og Zelected blev som følge heraf frikendt.

Læs dommen her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-10372-2023-SHR.pdf

Vestre Landsret træffer afgørelse i sag om greenwashing af produkter med svinekød

Vestre Landsret afsagde den 1. marts 2024 dom i sag BS-472/2022-VLR mellem Dansk Vegetarisk Forening og Klimabevægelsen i Danmark og Danish Crown A/S (»Danish Crown«). Tvisten drejede sig om, hvorvidt Danish Crown havde overtrådt lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 5 om vildledende markedsføring ved at bruge udtrykkende »Dansk gris er mere klimavenlig, end du tror« og »Klimakontrolleret gris« i deres markedsføring og på deres produkter.

I forhold til udtrykket »Dansk gris er mere klimavenlig, end du tror« fandt landsretten, at der ikke var tale om en vildledelse i den danske markedsføringslovs § 5's forstand. Landsretten lagde vægt på, at indholdet var tilstrækkelig underbygget ved undersøgelser om CO2-udledning og forbrugere, samt anvendelsen af lignende relative udtryk anvendt i en relevant vejledning.

I forhold til udtrykket »Klimakontrolleret gris« fandt landsretten at Danish Crown ved brugen af dette udtryk havde overtrådt den danske markedsføringslovs § 5 idet det gav forbrugeren et indtryk af, at Danish Crowns produkter var underlagt en vis kvalitativ miljøkontrol og udtrykket derved svarede til et autoriseret miljømærke, som der imidlertid ikke forelå dokumentation for. Landsretten fandt dog, at udtrykket ikke kunne forbydes generelt i al fremtidig markedsføring, da udtrykket var for bredt.

Læs dommen her: https://domstol.dk/vestrelandsret/aktuelt/2024/3/dom-i-sag-om-greenwashing/

Sø- og Handelsretten træffer afgørelse i sag om retten til at markedsføre og gøre anden erhvervsmæssig brug af børnemøbelprodukter

Sø- og Handelsretten afsagde d. 8. marts 2024 kendelse i sag BS-38318/2021-SHR mellem by Klip-Klap ApS (»KlipKlap«) og Pandorakitchen ApS (»Pandorakitchen«). Tvisten drejede sig om, hvorvidt Pandorakitchens markedsføring og salg af en børnestol, en børnesofa og nogle foldemadrasserfoldemadras udgjorde ulovlig produktefterligning af KlipKlaps produkter.

Det centrale spørgsmål var om Pandorakitchens markedsføring og salg tilsidesatte lovbekendtgørelse nr. 426 af 1. juli 2017 (»den danske markedsføringslov«) bestemmelser om god skik og nærgående produktefterligninger, jf. § 3, stk. 1, jf. § 20 og § 5, stk. 2, nr. 10.

KlipKlap gjorde gældende, at deres produkter havde opnået markedsføringsretlig beskyttelse ved, at produkterne havde særpræg og markedsposition som følge af KlipKlaps betydelige markedsføring. De hævdede, at Pandorakitchens produkter, grundet samme skumfyld og næsten identiske dimension, havde det samme helhedsindtryk. KlipKlap gjorde dertil gældende, at Pandorakitchens produkter var frembragt med kendskab til og viden om KlipKlaps produkter.

Retten fastslog, at KlipKlap havde opnået et sådan udtryksmæssigt særpræg at produkterne nød markedsføringsretlig beskyttelse imod meget nærgående efterligninger. Retten lagde vægt på de designelementer, der gav KlipKlaps produkter udtryksmæssigt særpræg, såsom

materialekvalitet, syningsteknik, knapper, form og produktlabels. Retten lagde herefter afgørende vægt på, at disse designelementer, ikke kunne genfindes i Pandorakitchens produkter, som fremstod mere neutrale. På den baggrund og sammenlagt med øvrige detailforskelle af betydningen for det visuelle udtryk, kom frem til, at der ikke forelå en krænkende produktefterligning. Sagen er anket til Vestre Landsret den 22. marts 2024.

Læs dommen her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-38318-2021-SHR.pdf

Forbrugerombudsmanden understreger, at der er forskel på genbrugs- og genanvendt plast

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) havde den 8. marts 2024 i en pressemeddelelse udtalt sig om markedsføringen af produkter fra Aqua d'Or Mineral Water A/S og påpegede, at markedsføring af produkter med påstande om anvendelse af genbrugsplast, når det faktisk drejede sig om genanvendt plast, er potentielt vildledende for forbrugerne. Denne vurdering resulterede i en indskærpelse af vildledningsforbuddet i lovbekendtgørelse nr. 866 af 15 juni 2022 (»den danske markedsføringslov«) over for Aqua d'Or.

Den vildledende markedsføring fandt sted på flaskernes emballage og virksomhedens hjemmeside. Forbrugerombudsmanden konkluderede, at markedsføringen var vildledende, da den gav indtryk af, at flaskerne var blevet skyllet eller rengjort og derefter genbrugt. Denne markedsføring kunne føre til et vildledende indtryk af flaskernes miljøpåvirkning, da flasker lavet af genanvendt plastik har en højere miljøbelastning end flasker lavet af genbrugt plastik.

Forbrugerombudsmanden konkluderede at Aqua d'Or's markedsføring var i strid med den danske markedsføringslovs § 5, som forbyder vildledende markedsføring, sammenholdt med § 8 der fastslår, at vildledning kan påvirke forbrugerens beslutning. Derudover kræver den danske markedsføringslovs § 13, at virksomheder kan dokumentere faktuelle påstande i deres markedsføring.

Læs Forbrugerombudsmandens pressemeddelelse her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2024/202403-08-der-er-forskel-paa-genbrugs-og-genanvendt-plast/

Sø- og Handelsretten træffer afgørelse om den territoriale udstrækning af sanktioner efter varemærkeforordningen

Sø- og Handelsretten afsagde den 14. marts 2024 kendelse i sag BS-38012/2021-SHR mellem Sports Group Denmark A/S og Victor Rackets Ind. Corp over for EPC Alternative Source (»EPC«) og Forza Fighting Gear BV (»Forza«).

Tvisten i hovedsagen angik varemærkekrænkelser. Dog vedrørte kendelsen alene Sø- og Handelsrettens stedlige kompetence til at pålægge sanktioner i form af påbud og forbud med virkning for hele EU's område i henhold til Forordning (EU) nr. 2017/1001 af 14. juni 2014 om EU-varemærker (»varemærkeforordningen«) og Forordning (EU) nr. 1215/2012 af 12. december 2012 (»domsforordningen«), idet dette spørgsmål var udskilt til særskilt afgørelse.

Sagsøgerne påstod, at Sø- og Handelsretten var kompetent til at påkende deres påstande om virkning for hele EU-territoriet med henvisning til domsforordningens artikel 25-26 samt varemærkeforordningens artikel 125, stk. 4. Domsforordningens bestemmelser angår aftaler om værneting og domstolenes kompetence i en medlemsstat, hvortil varemærkeforordningen i nævnte artikel netop med henvisning til disse bestemmelser hjemler en fravigelse af det ellers efter denne forordning gældende bopælskrav ved anlæg af søgsmål.

Sø- og handelsretten fandt, at Domsforordningens artikel 25 og 26 ikke fandt anvendelse i sagen, da Sports Group Denmark ubestridt var indehaver af to EU-varemærker, der blev påberåbt krænket af sagsøgerne.

Derudover fandt retten, at varemærkeforordningens artikel 125, stk. 4, litra b, ikke fandt anvendelse i sagen, da der ikke var indgået en værnetingsaftale mellem parterne, og eftersom EPC og Forzas advokat kun var mødt for at bestride Sø- og Handelsrettens kompetence.

Sø- og Handelsretten fandt desuden, at selvom retten ville have kompetence i medfør af varemærkeforordningens artikel 125, stk. 5, ville rettens kompetence være begrænset til handlinger, der er begået, eller som der er risiko for begået i Danmark, jf. varemærkeforordningens artikel 126, stk. 2.

På denne baggrund afviste Sø- og Handelsretten sagsøgers principale påstande om forbud i hele EU.

Læs dommen her: https://domstol.fe1.tangora.com/media/-300011/files/Kendelse_om_sags%C3%B8gers_principale_p%C3%A5stande__BS-38012-2021-SHR.pdf?rev1

Forbrugerombudsmanden indskærper regler vedrørende onlineplatformes ansvar for bæredygtighedsudsagn

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) indskærpede den 19. marts 2024 i en pressemeddelelse, at onlineplatforme er ansvarlige for de bæredygtighedsudsagn, der anvendes i markedsføringen på deres platforme. Dette ansvar opstår, når onlineplatformene aktivt bidrager til at fremme salget af produkter, som fejlagtigt er betegnet som bæredygtige af virksomhederne på platformene. Forbrugerombudsmandens vurdering er baseret på to sager vedrørende onlineplatformene Miinto A/S og Stylepit.com A/S.

Forbrugerombudsmanden konstaterede, at begge platforme havde

spillet en aktiv rolle i markedsføringen og salget af disse produkter ved at optimere og fremme produkter, hvoraf nogle var fejlagtigt markedsført som bæredygtige. Dette betød, at platformene ikke kunne benytte sig af lovgivningens mulighed for ansvarsfritagelse, som ellers var gældende for platforme, der udelukkende havde en passiv rolle i formidlingen af information.

Forbrugerombudsmanden fremhævede, at begge platforme ikke kun havde markedsført produkter med besparelsesudsagn, som opfordrede forbrugerne til hurtige købsbeslutninger, men også havde anvendt konkurrencer og rabatkoder til at tiltrække kunder. Desuden var visse produkter markedsført med bæredygtighedsudsagn, både i produkttitler og -beskrivelser, uden at platformene efterfølgende havde kunnet dokumentere disse udsagns rigtighed.

Forbrugerombudsmandens samlede vurdering var, at Miinto og Stylepit ikke havde opfyldt dokumentationskravet i lovbekendtgørelse nr. 426 af 1. juli 2017 (»den danske markedsføringslov«) § 13, hvilket havde resulteret i vildledning af forbrugerne.

Læs Forbrugerombudsmandens pressemeddelelse her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2024/20240319-onlineplatforme-er-ansvarlige-for-baeredygtighedsudsagn/

Østre Landsret afsiger dom i sag mellem Resurs Bank og Finanstilsynet samt Forbrugerombudsmanden

Østre Landsret traf den 22. marts 2024 afgørelse i sag BS-10730/2022-OLR vedrørende gyldigheden af det danske Finanstilsyns (»Finanstilsynet«) påbud fra januar 2022 0m rammerne for Resurs Banks kreditværdighedsvurderinger ved ydelse af lån.

Påbuddet lød på et krav om, at Resurs Bank foretog *(i)* en beregning af låntagers rådighedsbeløb for alle lån, *(ii)* en individuel vurdering af rådighedsbeløbets tilstrækkelighed, *(iii)* en beregning af låneudgifter på baggrund af scenarier med højeste ydelse, samt *(iv)* en vurdering af låntagers kreditværdighed på baggrund af fyldestgørende oplysninger, hvilket indebar, at Resurs Bank indhentede dokumenterede oplysninger om låntagers faktiske indtægter og faktiske udgifter.

Derudover indtrådte den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) som del i sagen for at få tilsidesat en konkret kreditaftale som ugyldig, der var indgået mellem Resurs Bank og en forbruger.

Spørgsmålet var navnlig, hvorvidt påbuddet gik ud over rammerne i lovbekendtgørelse nr. 817 af 6. august 2019's (»den danske kreditaftalelov«) § 7 c, stk. 1, om vurdering af forbrugerens kreditværdiged set i lyset af EU-retten Finanstilsynets påbuds blev af landsretten stort set opretholdt og de fandt, at påbuddet ikke gik ud over rammerne i såvel national som EU-lovgivning. Landsretten fandt dog, at den del af påbuddet, der omhandlede Resurs Banks indhentelse af dokumenterede indtægter og faktiske oplysninger var for vidtgående, det et sådant generelt krav ville fratage Resurs Bank deres skøn over, hvornår de havde fyldestgørende oplysninger til brug for kreditværdighedsvurderingen. Desuden blev Resurs Bank frifundet for tilsidesættelse af den konkrete kreditaftale, da Forbrugerombudsmanden ikke havde løftet bevisbyrden tilstrækkeligt.

Læs dommen her: https://domstol.dk/oestrelandsret/aktuelt/2024/3/dom-i-sag-mellem-resurs-bank-og-finanstilsynet-samt-forbrugerombudsmanden/

Bodums Douro-kop udgjorde en ophavsretlig krænkelse af Royal Copenhagens Contrast-kop

Sø- og Handelsretten afsagde den 22. marts 2024 dom i sagen BS-2578/2023-SHR, som omhandlede en tvist mellem Fiskars Finland Oy Ab (»Fiskars«) og Peter Bodum A/S (»Bodum«) vedrørende ophavsrettigheder til designet af Fiskars' Contrast-kop. Tvisten drejede sig om, hvorvidt Bodums fremstilling, salg og markedsføring af Douro-koppen udgjorde en krænkelse af Fiskars' ophavsretlige beskyttelse, jf. lovbekendtgørelse nr. 1093 af 20. august 2023 (»den danske ophavsretslov«) § 2 om den ophavsretlige eneret.

Fiskars, som ejer Royal Copenhagen-brandet, og hermed ophavsrettighederne til Contrast-koppen, argumenterede for, at Bodums Douro-kop i design og udtryk efterlignede deres produkt i en grad, der oversteg grænserne for lovlig inspiration, og dermed krænkede deres ophavsret.

Bodum gjorde heroverfor gældende, at Douro-koppen var resultatet af en selvstændig kreativ proces, der involverede unikke designelementer og æstetiske valg, og at lighederne mellem de to produkter var overfladiske og uundgåelige, givet de funktionelle aspekter ved kopdesign generelt.

Retten fandt, at de samlede karakteristika ved Douro-koppen i for høj grad afspejlede det særlige udtryk, som kendetegner Contrast-koppen, herunder kombinationen og udformningen af materialer samt visse designmæssige valg, som samlet set gav koppen dens særegne udseende.

Bodum blev derfor meddelt forbud om at indstille salget i sin helhed samt tilbagekalde produktet fra markedet, ligesom de yderligere skulle betale erstatning til Fiskars.

Læs dommen her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-2578-2023-SHR.pdf?rev1

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


Selmer

Ståle Hagen og Øystein Kolstad Kvalø

Fra kontraktuell forutsigbarhet til fleksibilitet:

Mer smidige gjennomføringsmodeller i store IT-prosjekter

Fossefallsmetodikkens begrensninger

Kontrakter som bygger på en fossefallsmetodikk, blir ofte valgt i store IT-prosjekter. Fossefallskontrakter kjennetegnes ved sin lineære fremgangsmåte, hvor resultatet av prosjektet er detaljert beskrevet allerede ved kontraktsinngåelsen og leverandøren jobber frem mot en på forhånd avtalt sluttleveranse. Normalt stiller kontrakten krav til fremdrift og det er avtalt fastpris.

Fossefallsmetodikken har en rekke begrensninger, og erfaringer viser at den ofte passer dårlig i store og komplekse IT-prosjekter. For det første er metodikken rigid, og åpner i liten grad for endringer underveis i utviklingsperioden, med mindre det gjennomføres formell endringshåndtering. Kravspesifikasjonen definerer hva som skal leveres, og både kunden og leverandøren må som utgangspunkt forholde seg til den samme spesifikasjonen i hele kontraktsperioden. Den detaljerte kravspesifikasjonen på bestillingstidspunktet tar av naturlige årsaker ikke høyde for læring underveis i prosjektet eller endringer i teknologien, og kunden risikerer derfor at løsningen som leveres er delvis utdatert allerede på leveransetidspunktet.

For det andre må kunden legge ned betydelig med både tid og ressurser for å utforme detaljerte kravspesifikasjoner. For kunder som ikke selv sitter på god og oppdatert teknisk kompetanse, kan det være krevende å gjøre dette nødvendige forarbeidet på en tilfredsstillende måte, uten å bruke lang tid og betydelige ressurser på å kjøpe inn ekstern ekspertise.

For det tredje er mange IT-systemer det vi kan kalle «sosiotekniske systemer» – teknologien skal fungere i samspill med mennesker og måten vi jobber på. Implementering av sosiotekniske systemer krever kontinuerlig læring og tilpasning underveis i spesifikasjons- og utviklingsperioden, noe fossefallsmetodikken i liten grad legger til rette for.

For det fjerde er det vanskelig for leverandører og kunder å få god forståelse for hverandres behov og muligheter gjennom en rigid anskaffelsesprosess. Normalt vil kundens modenhet på egne behov og kunnskap om mulighetene som finnes i leverandørens løsninger være lavere tidlig i prosjektet, på det tidspunktet spesifikasjonen «låses» i kontrakten. I en ideell prosess vil leverandøren og kunden lære av hverandre gjennom spesifikasjons- og utviklingsperioden, men dette legger fossefallsmetodikken i liten grad opp til.

Et ønske om trygghet

Med ovennevnte utfordringer som bakgrunn, kan man spørre seg hvorfor kontrakter som bygger på fossefallsmetodikken likevel blir valgt i store IT-prosjekter. En sentral del av svaret ligger nok i kundens ønske om trygghet. Gjennom detaljerte kravspesifikasjoner ønsker kunden forutsigbarhet om hvilken løsning som skal leveres, og en mulighet for å peke på leverandøren hvis løsningen ikke oppfyller de avtalte kravene.

To rettssaker om heving av store IT-kontrakter fra de senere årene viser likevel at det ikke nødvendigvis er rett frem for en kunde å komme seg ut av en kontrakt der leverandøren ikke oppfyller de fastsatte kravene. Den ene saken gjaldt heving av avtale om levering av et ERP-system mellom kunden Fellesskjøpet og leverandøren Infor.[1] Den andre saken gjaldt heving av avtale om levering av IKT-løsning for innkreving av bompenger mellom kunden Statens vegvesen og leverandø-

1 Avgjort i Eidsivating lagmannsretts dom 13. juli 2021. Lovdata: *LE-2018-76187-3*.

ren IBM, også omtalt som «Grindgut-saken».[2] I begge disse sakene tapte kundene til slutt saken, og hevingene ble ansett urettmessige. Sakene er redegjort for i tidligere utgaver av Lov&Data, se utgave nr. *nr. 154 2/2023*, *nr. 152 4/2022* og *nr. 147 3/2021*. Vi vil derfor kun trekke ut noen poenger om hvordan vi mener sakene illustrerer at fossefallskontrakter ikke nødvendigvis gir den ønskede kontraktuelle tryggheten kunden søker.

Avtalen mellom Felleskjøpet og Infor var basert på standardavtalen SSA-T, mens avtalen mellom Statens vegvesen og IBM var basert på standardavtalen PS2000. SSA-T er en klassisk fossefallskontrakt, mens PS2000 er en seriefossefallskontrakt hvor flere kravspesifikasjoner og delleveranser følger løpende i utviklingsfasen.

I begge sakene kom lagmannsrettene til at leverandørene hadde misligholdt kontrakten gjennom forsinkelser og mangler. Samtidig hadde kundene i begge sakene vist løsningsvilje og forsøkt å drive prosjektene fremover, til tross for leverandørens mislighold. Dette ble av retten vektlagt i negativ retning for kunden, ettersom denne fleksibiliteten langt på vei ble tolket som en aksept av leverandørens mislighold og avkall på misligholdsbeføyelser.

Begge sakene endte med store erstatningskrav og sakskostnadskrav i disfavør av kundene, til tross for bruken av kontrakter som i utgangspunktet skal plassere en betydelig del av leveranseansvaret på leverandørene.

Mer smidige gjennomføringsmodeller som løsning?

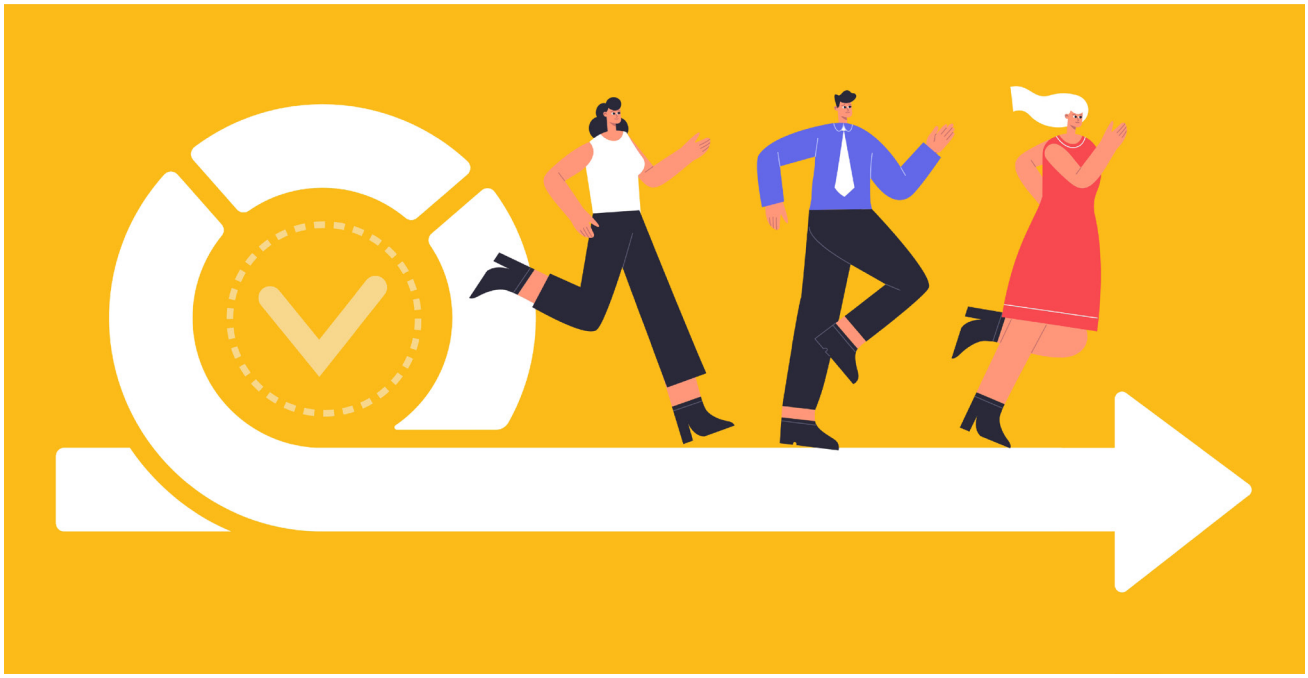
Smidige (agile) gjennomføringsmodeller tilbyr en alternativ tilnærming som kan være bedre egnet til å håndtere kompleksiteten, behovet for å absorbere læring og usikkerheten i store IT-prosjekter. Slike kontraktstyper pålegger leverandøren en innsatsforpliktelse heller enn en resultatforpliktelse, og kunden og leverandøren forutsettes å jobbe tett sammen gjennom prosjektet for å utforme og levere den beste løsningen for kunden.

Smidige gjennomføringsmodeller har som overordnet mål å skape forretningsverdi underveis, heller enn å på forhånd fastsette en detaljert plan for prosjektet. Fokuset er fremdeles å utvikle løsninger med god kvalitet, men detaljene spesifiseres løpende og ikke før prosjektet starter. Kunden slipper samtidig å bruke mye tid og ressurser på å utforme detaljerte kravspesifikasjoner i forkant av oppstart. Kunden må riktig nok bruke ressurser underveis i prosjektet på det løpende samarbeidet med leverandøren, men vår erfaring er at dette samarbeidet gir større verdi enn ressursene som legges ned i å utforme detaljerte kravspesifikasjoner. Dessuten viser erfaringene med fossefallsmetodikken at kunden også i disse prosjektene i praksis må bruke mye ressurser på formell oppfølging av leverandøren underveis, til tross for at mye av arbeidet i utgangspunktet skal være gjort gjennom utforming av kravspesifikasjonen og kontrakten.

Smidige kontrakter

Det klare utgangspunktet for kontrakter som skal regulere smidige gjennomføringsmodeller, er at de på en tenkt ansvarslinje ligger langt nærmere bistandskontrakter enn fossefallskontraktene. Dette innebærer at disse gjennomføringsmodellene ikke er egnet for kunder som ønsker å overføre betydelige deler av det kontraktuelle ansvaret

2 Avgjort i Borgarting lagmannsretts dom 14. oktober 2022. Lovdata: *LB-2020-82571-2*.



Illustrasjon: Colourbox.com

for leveransen til leverandøren. Det er likevel noen mekanismer som kan og bør legges inn i kontrakter som regulerer smidige gjennomføringsmodeller.

For det første bør kontraktene beskrive et formål med prosjektet, men kun på et veldig overordnet nivå, og uten å spesifisere konkrete krav til funksjonalitet. En sentral del av mange smidige modeller er at kunden underveis i prosjektet prioriterer funksjonaliteten som skal utvikles, og dette fungerer dårlig sammen med en kontrakt som inneholder konkrete krav til funksjonalitet.

For det andre bør gjennomføringsmodellen beskrives, slik at partene har en felles forståelse og forplikter seg til å jobbe etter samme metodikk. Dette inkluderer blant annet samspillet mellom kundens ansvar for og arbeid med produktkøen, og leverandørens ansvar for gjennomføring av detaljspesifisering, utvikling og testing i utviklingsiterasjonene (sprintene).

For det tredje bør det stilles en del ikke-funksjonelle krav som leverandøren forplikter seg til å oppfylle for all funksjonalitet som tas ut av produktkøen og inn i utviklingsiterasjonene. Dette kan eksempelvis være krav til helhetlig arkitektur, kompatibilitet, infrastruktur, sikkerhet og vedlikeholdbarhet.

Til sist bør kontrakten angi hvilke ressurser kunden og leverandøren forplikter seg til å stille med, enten dette er navngitte ressurser eller konkrete kompetanseprofiler. Hvor mye de enkelte ressursene skal jobbe må også avtales. Ettersom smidige modeller ikke er veldig rigide, må det også være mulig å opp- og nedskalere og omprioritere ressursbruken i prosjektet.

Dessverre ser vi at de standardkontraktene som er tilgjengelige i det norske markedet og som utgir seg for å understøtte smidige gjennomføringsmodeller, fremdeles inneholder elementer fra den tidligere fossefallstilnærmingen, slik at de i praksis ikke fungerer etter sin hensikt. Det er også en betydelig utfordring at det inngås kontrakter basert på fossefallsmetodikken, men hvor partene blir enige om å jobbe smidig. Hvorfor dette er problematisk, er et tema som fortjener sin egen artikkel.

En løsning for alle IT-prosjekter?

Som vi har vist ovenfor, er det mange fordeler med smidige gjennomføringsmodeller i IT-prosjekter.

Fra enkelte kunders perspektiv vil den største ulempen med denne kontraktstypen være den reduserte kontraktuelle forutsigbarheten, men i lys av utfallet i de to nevnte rettssakene kan man spørre seg om hvor reell denne forutsigbarheten har vært tidligere.

Det er ikke dermed sagt at smidige gjennomføringsmodeller er løsningen for alle typer IT-prosjekter. Metoden egner seg særlig for de store og komplekse prosjektene, hvor det er vanskelig å forutsi hvordan et best mulig sluttresultat ser ut. Det er også en viktig forutsetning at kunden har kompetanse og kapasitet til å sette opp et tilstrekkelig mottaksprosjekt på sin side, ettersom behovet for et tett og omfattende samarbeid med leverandøren er en avgjørende suksessfaktor. Fossefallsmetodikken har fremdeles livets rett, men er slik vi ser det bedre egnet for mindre komplekse og mer oversiktlige prosjekter, hvor det i mindre grad oppstår behov for endringer underveis i prosjektet.

For ordens skyld opplyses det om at Advokatfirmaet Selmer bistod Felleskjøpet i forbindelse med hevingsprosessen og rettssaken i tvisten mot Infor.

Øystein Kolstad Kvalø er advokatfullmektig i Advokatfirmaet Selmer, og bistår klienter med regulatoriske spørsmål innenfor blant annet telekom, teknologi, digitalisering og personvern.

Gorrissen Federspiel

Tue Goldschmieding

Klagenævnet for udbud træffer afgørelse om ændring af mindstekrav i IT-udbud

Det danske Klagenævn for udbud (»klagenævnet for udbud«) afsagde den 30. november 2023 kendelse med journalnummer 23/03579 mellem Assemble A/S (»Assemble«) over for Hørsholm Kommune. Sagen angik, om Hørsholm Kommune i forbindelse med et udbud havde overtrådt reglerne i lovbekendtgørelse nr. 1564 af 15. december 2015 (»den danske udbudslov«).

I forbindelse med en udbudsrunde havde Hørsholm Kommune efter et indledende forhandlingsforløb ændret formuleringen af sin kravsspecifikation. Udbuddet blev efterfølgende vundet af Assembles konkurrent. Assemble gjorde derefter gældende, at ændringerne i kravspecifikationen udgjorde en ændring af ufravigelige mindstekrav og dermed en ændring af udbudsmaterialets grundlæggende elementer, hvilket var i strid med ligebehandlingsprincippet i den danske udbudslovs § 2 samt § 66, stk. 5 om forbuddet mod ændringer af de grundlæggende elementer i udbudsmaterialet.

Klagenævnet citerede i afgørelsen forarbejderne til den danske udbudslovs § 2, hvoraf bl.a. fremgik, at ændringer af mindstekrav som klart udgangspunkt kunne karakteriseres som ændringer af grundlæggende elementer. Klagenævnet udtalte videre, at bevisbyrden for, at ændringerne ikke var egnede til at fordreje konkurrencen mellem tilbudsgiverne, påhvilede Hørsholm Kommune.

Hørsholm Kommune havde ikke løftet denne bevisbyrde, og efter en samlet vurdering fandt klagenævnet for udbud, at kommunen ikke havde overholdt betingelserne i den danske udbudslovs § 2 og § 66, stk. 5, hvorefter beslutningen om at tildele kontrakten til Assembles konkurrent blev annulleret.

Læs kendelsen her: https://klfu.naevneneshus.dk/media/documents/Assemble_AS_mod_H%C3%B8rsholm_Kommune.pdf

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

Illustrasjon: Colourbox.com

Wikström & PARTNERS

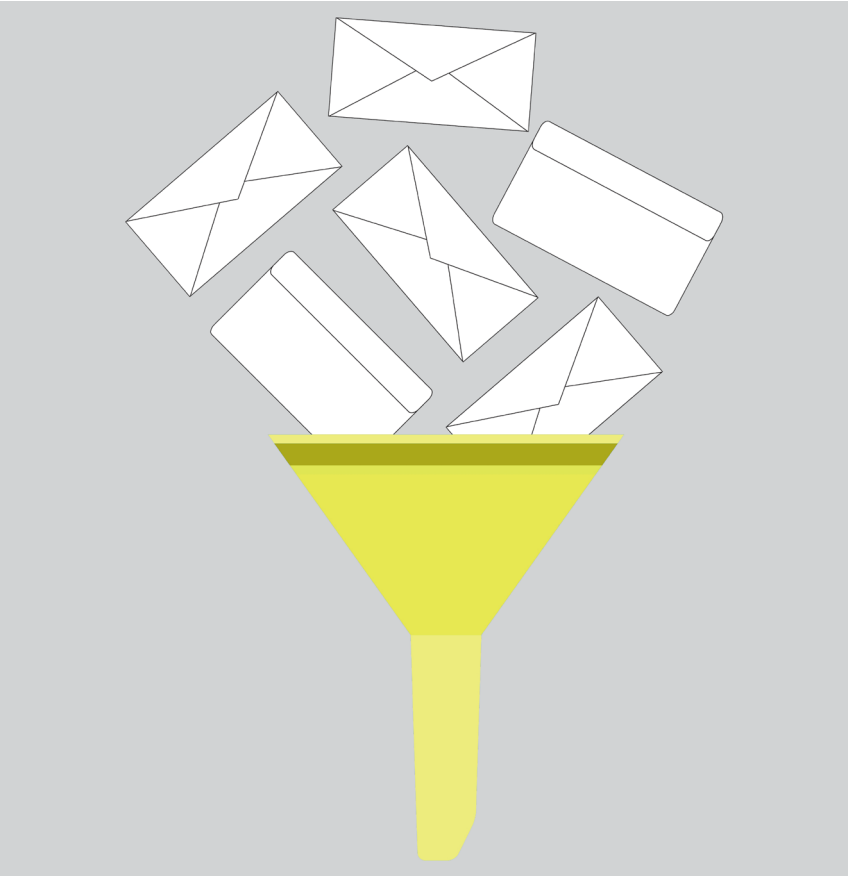
Karin Tilly och Anton Karlsson

”Spamfiltret” – ett e-postmeddelande som fastnat i en myndighets skräppostfilter ska anses inkommet

Högsta domstolen fastslog i mål ”Spamfiltret”,[1] att ett överklagande av ett beslut ska anses ha inkommit i rätt tid, även om överklagandet levererades till myndigheten först efter att överklagandetiden löpt ut på grund av att handlingen hade fastnat i den mottagande myndighetens spamfilter.

Västra Gästriklands samhällsbyggnadsnämnd (VGS) meddelade den 24 mars 2021 beslut om rättelseföreläggande samt byggsanktionsavgift avseende viss fastighet. Beslutet överklagades sedermera av klagandena, men avvisades genom beslut[2] som för sent inkommet. Överklagandet skickades in via e-post till mottagande myndighet den 5 maj 2021 kl. 23:57, innan överklagandetiden hade löpt ut, men fastnade i myndighetens spamfilter och levererades till myndighetens mottagningsfunktion först en halvtimme därefter, den 6 maj 2021 kl. 00:27. Mot bakgrund av att sista dag för klagandena att inkomma med överklagandet var den 5 maj 2021, och överklagandet inkommit till kommunens mejlserver först den 6 maj 2021, bedömdes överklagandet som för sent inkommet. Beslutet att avvisa överklagandet har sedermera varit föremål för överklagande, och slutligen nått Högsta domstolen, som meddelade dom den 3 januari 2024.

Högsta domstolen inledde med att konstatera att en handling enligt 22 § förvaltningslagen (2017:900) ska anses ha inkommit till myndigheten den dag som handlingen har nått myndigheten eller en behörig befattningshavare. Domstolen noterade att enligt förarbetena till 22 § förvaltningslagen ska en handling som skickats via e-post anses ha inkommit till mottagande myndighet när den finns tillgänglig för



Illustrasjon: Colourbox.com

1 Mål P-124-23.
2 Dnr VGS-BY-2020-328.

myndigheten eller en behörig befattningshavare på myndighetens server i datanätverket. Regleringen har utformats så att onödiga rättsförluster i möjligaste mån ska undvikas för den enskilde. Domstolen fastställde att ett e-postmeddelande har inkommit i rätt tid om det har skickats till den anvisade adressen, och inom tiden för överklagandet nått den mottagande myndighetens datanätverk, oavsett hur myndigheten har organiserat sin hantering av skräppost eller liknande. Överklagandet i förevarande fall hade nått myndighetens datanätverk inom överklagandetiden, varför Högsta domstolen slog fast att överklagandet ska anses ha inkommit i rätt tid, oberoende av hur myndigheten har organiserat sin hantering av skräppost och liknande.

En handling som lagras i en extern molntjänst för endast teknisk bearbetning eller teknisk lagring anses inte vara allmän

Högsta förvaltningsdomstolen meddelade den 20 februari 2024 dom i mål 3530–23 avseende var och ens rätt att ta del av allmänna handlingar hos myndigheter. Högsta förvaltningsdomstolen gjorde bedömningen att en handling som en myndighet inom ramen för sitt interna arbete delat via en extern molntjänst, endast som ett led i en teknisk bearbetning eller teknisk lagring, inte ska anses som inkommen eller upprättad hos den myndigheten enligt tryckfrihetsförordningen. Av den anledningen är inte heller handlingen att betrakta som allmän enligt tryckfrihetsförordningen. Den aktuella handlingen hade skapats inom ramen för ett pågående ärende, och medan ärendet pågått, delats via Microsoft Teams, i syfte att projektgruppen skulle kunna redigera dokumentet tillsammans.

TechSverige har publicerat ett nytt standardavtal för välfärdsteknik och trygghetsskapande teknik

TechSverige har publicerat ett nytt standardavtal för välfärdsteknik och trygghetsskapande teknik. TechSverige utgör en medlemsorganisation för företag inom tech-sektorn, med uppdraget att tillsammans med medlemmarna skapa bästa möjliga förutsättningar för en konkurrenskraftig svensk tech-bransch. TechSverige har ca 1 400 medlemsföretag, och har publicerat flertalet standardavtal anpassade för tech-sektorn, bland annat Allmänna bestämmelser om Molntjänster, Allmänna bestämmelser om IT-Underhåll och Allmänna bestämmelser om IT-Infrastrukturtjänster.

Det nya standardavtalet, Allmänna bestämmelser Välfärdsteknik och tjänster, är framtaget mot bakgrund av att ett antal medlemsföretag har identifierat ett stort behov av ett standardavtal för välfärdsteknik och trygghetsskapande teknik. En särskild komplexitet har identifierats vid leveranser som ska innehålla både tjänst, mjukvara och hårdvara, där det finns behov av tydlighet och verktyg vid avtalsförhandlingen. Intentionen har varit att utveckla ett förhållandevis balanserat standardavtal, som reglerar allt från parternas åtaganden, ansvar samt servicenivåer, genom en särskild bilaga.

Karin Tilly, biträdande jurist, Wikström & Partners Advokatbyrå i Stockholm, specialiserade på IT, IP och dataskydd.

Anton Karlsson, biträdande jurist, verksamma vid Wikström & Partners Advokatbyrå i Stockholm och specialiserade på IT, IP och dataskydd.


Schjødt

Andreas A. Johansen og Anna Katrine Olberg Eide

Kontraktsrettslig skråblikk på bruk av innsamlet data

I stadig økende grad preges næringslivet og nyhetsbildet av saker om deling eller annen bruk av innsamlet data. Data har som kjent blitt omtalt som den nye oljen. I uraffinert form har både oljen og data liten verdi. Verdiskapningen ligger nettopp i resultatet en kan oppnå ved å sammenstille, analysere og kombinere data på en hensiktsmessig og gunstig måte. Det er forsøket på denne verdiskapningen som har preget nyhetsbildet i den siste tiden, gjennom et KI-kappløp mellom de store aktørene i næringslivet. Kappløpet er også oppmuntret av myndighetene i Norge, som blant annet har satt av en milliard kroner til forsking på kunstig intelligens.[1] Samtidig vil selskaper som ønsker å ta del i kappløpet eller bruke KI-løsninger stå overfor en rekke juridiske problemstillinger.

Generelt synes det å være en bred oppfatning om at utviklingen av kunstig intelligens kan gi et positivt tilskudd til både samfunnet som sådan og næringslivet. Bruken av innsamlet data reiser imidlertid en rekke komplekse juridiske problemstillinger. Disse problemstillingene har ikke bare en personvernrettslig side, men også en kontraktsrettslig side. Hvordan skal bedrifter som analyserer og samler inn store mengder data for utvikling og innovasjon sikre at bruken av data skjer på en etisk og ansvarlig måte? Og hvordan skal bedrifter sikre seg mot at egen data brukes på en måte som er egnet til å skade egen virksomhet? Hvordan bør avtaler som har en berøringsside mot KI utformes for å beskytte individers og næringslivets interesser på en best mulig måte? I denne artikkelen vil vi se på enkelte av de kontraktsrettslige sidene ved bruk av data i KI-løsninger.

Overordnet kan det skilles mellom kontrakter som inngås mellom bedrifter og forbrukere, såkalte «B2C»-forhold (**business-to-consumer**), og kontrakter som inngås mellom bedrifter, såkalte «B2B»-forhold (**business-to-business**). I B2C-segmentet står personvern svært sentralt. De klart fleste sett med data vil her inkludere personopplysninger. I B2B-segmentet vil det i større grad være tale om data som ikke utgjør personopplysninger, eller hvor det personvernrettslige for eksempel kan reguleres gjennom en databehandleravtale. Det blir da også større rom for en «friere» avtaleregulering av bruk av data. Kontraktsretten har derfor i praksis størst plass i B2B-forhold, men vi vil likevel nedenfor starte med noen betraktninger også om B2C.

Den kontraktsrettslige siden i et B2C-forhold er velkjent for de fleste. Det er hovedregelen snarere enn unntaket at forbrukeren aksepterer tjenestens vilkår uten å ha lest vilkårene. Disse vilkårene vil svært ofte gi selskapet kontraktsrettslig grunnlag til et visst omfang av deling eller annen bruk av data. Selv om det foreligger et kontraktsrettslig grunnlag for å samle inn og bruke dataen, vil dataen som innsamles fra en forbruker nesten uten unntak inneholde personopplysninger. Når personopplysninger samles inn eller behandles, kreves det i tillegg et behandlingsgrunnlag etter personvernforordningen artikkel 6 og i enkelte tilfeller også artikkel 9.

Personvernforordningen artikkel 6 oppstiller flere behandlingsgrunnlag, deriblant avtale. Selv om det er inngått en avtale mellom selskapet og individet, er imidlertid ikke dette ensbetydende med at selve avtalen kan utgjøre et rettslig grunnlag for behandlingen av personopplysninger. For at avtalegrunnlaget skal kunne brukes, må behandlingen være nødvendig for å oppfylle avtalen med individet. Dette er tolket dithen at den behandlingsansvarlige (i vårt tilfelle selskapet) må kunne demonstrere at kontraktens hovedinnhold ikke kan oppnås uten den aktuelle behandlingen. Her er det

1 https://www.regjeringen.no/no/aktuelt/regjeringen-med-milliardsatsing-pa-kunstig-intelligens/id2993214/

ikke tilstrekkelig at behandlingen er gjort til en del av avtalen (f.eks. «bundlet» inn i vilkårene), eller at behandlingen er svært nyttig for selskapet. Det sentrale er om behandlingen er «objektivt uunnværlig for å gjennomføre et formål som er integrert del av den kontraktsmessige ytelsen til individet».[2] Behandling av personopplysninger for utvikling og trening av KI-verktøy vil derfor svært sjeldent eller aldri være strengt nødvendig for å oppfylle en avtale med individet i et B2C-forhold. Selve avtalen kan derfor ikke utgjøre det rettslige grunnlaget for behandlingen av personopplysninger i slike tilfeller. I personvernmiljøet er det i dag også uenighet om hvilket alternativt grunnlag som faktisk kan brukes. Vi vil imidlertid ikke gå nærmere inn på denne diskusjonen.

Bruk av data kan også være omstridt i «B2B»-forhold (**business-to-business**). Rettigheter til bruk av data kan reise flere problemstillinger knyttet til utforming av ansvarsreguleringer, håndtering av informasjonssikkerhet, regulering av eierskap til data, osv.

Følgende **eksempel** kan illustrere problemstillingen:

Et teknologiselskap selger en teknologi som samler inn data om produksjonen eller produksjonsmiljøet til et industriselskap. Gjennom denne dataen kan industriselskapet lære mer om egen produksjon og på den måten effektivisere driften og/eller oppnå økt kvalitet for produktet som selges. I avtalen mellom teknologiselskapet og industriselskapet, vil teknologiselskapet stort sett alltid ha sikret at de immaterielle rettighetene til teknologien forblir hos teknologiselskapet. Derimot kan reguleringen av *bruken av dataen* som teknologien samler inn, være mindre gjennomtenkt.

Partene vil normalt ha avtalt at industriselskapet kan bruke dataen. Det er gjerne hele poenget, og industriselskapets rett til slik bruk kan derfor også være mer implisitt. Men det kan være uklart om denne bruken er *eksklusiv*, eller om også teknologiselskapet kan bruke dataen til *sine* formål. Teknologiselskapet ønsker typisk gjerne å bruke dataen som treningsgrunnlag for sin egen KI/teknologi, slik at KI-en utvikler seg til det bedre og øker sin konkurransedyktighet. Hvis KI-en f.eks. plukker opp at industriselskapet oppnår økt salg på bestemte klokkeslett eller forbedret kvalitet ved bruk av en bestemt ingrediens eller metode, er dette informasjon KI-en vil besitte når industriselskapets konkurrenter senere kjøper den samme eller neste generasjon av teknologien. Veien kan da være kort til at dataen direkte eller indirekte gjøres kjent for konkurrenten. Et annet problem ved teknologiselskapets bruk av dataene, kan være at dataene fra industriselskapet kan være underlagt konfidensialitetsforpliktelser overfor industriselskapets øvrige kontraktsmotparter, f.eks. industriselskapets kunde eller underleverandør. Teknologiselskapets bruk av dataen til kan altså i flere henseender være direkte i strid med industriselskapets interesse.

Det er viktig å ta hensyn til problemstillinger som dette når avtalen utformes. Et eksempel på en avtaleregulering som *gir* teknologiselskapet slik rett, kan f.eks. lyde slik:

> *"[Teknologiselskapet] may use Customer Data to enhance and provide services, including the use of machine learning algorithms to improve functionality and performance"*

Industriselskapet bør ikke, i alle fall ikke uten videre, akseptere slike avtaleklausuler hvis det kan bli et forretnings- eller konkurransesensitivt problem at KI-en lærer dataen som samles inn. Samtidig vil det ofte være lite interessant for teknologiselskapet å inngå en avtale som helt forbyr selskapet å bruke dataen, all den tid fremtidig salg av teknologien forutsetter videreutvikling. Dette er imidlertid ikke binært: Det finnes avtaletekniske løsninger som ligger imellom at teknologiselskapet gis ubegrenset rett og ingen rett til bruk av dataen. I den grad det er mulig, bør en slik løsning tilstrebes for å ivareta begge parters interesser.

Potensiell bruk og deling av **forretningshemmeligheter** vil være et helt sentralt moment ved vurderingen av hvordan en slik avtale bør utformes.

I forretningshemmelighetsloven § 2 er en forretningshemmelighet definert slik:

> Med forretningshemmeligheter menes opplysninger som
> a. er hemmelige i den forstand at opplysningene ikke som helhet, eller slik de er satt sammen eller ordnet, er allment kjent eller lett tilgjengelig
> b. har kommersiell verdi fordi de er hemmelige
> c. innehaveren har truffet rimelige tiltak for å holde hemmelige

Dersom forretningshemmeligheter ukritisk mates inn i en KI-løsning, uten kontraktmessige reguleringer, kan opplysningene potensielt miste sin status og sitt vern som forretningshemmelighet under forretningshemmelighetsloven, med de følgekonsekvenser det får. Avtaleteknisk er det fullt mulig å ekskludere forretningshemmeligheter (og annen informasjon som vil vernes om) fra teknologiselskapets bruksrett. Dette kan for eksempel gjøres gjennom en innsnevring av definisjonen av "Customer Data" i kontraktseksemplet gitt ovenfor. Praktiseringen av dette er imidlertid trolig mer utfordrende.

Et annet kommersielt hensyn som må tas, er hvorvidt det kan forsvares at annen generell **innsikt og know-how** som ikke utgjør forret-

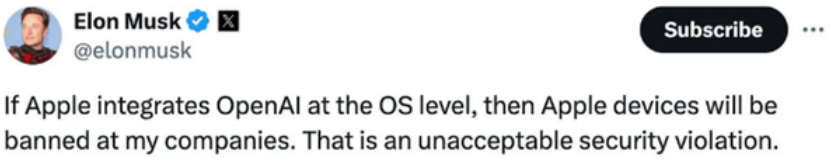
2 Sak C-252/21 *Meta*

ningshemmeligheter etter forretningshemmelighetsloven kan brukes for å videreutvikle et KI-produkt hvis dette kan komme konkurrenter til gode. Av denne årsaken ser vi at flere og flere bedrifter implementerer interne forbud og retningslinjer mot bruk av KI-verktøy.

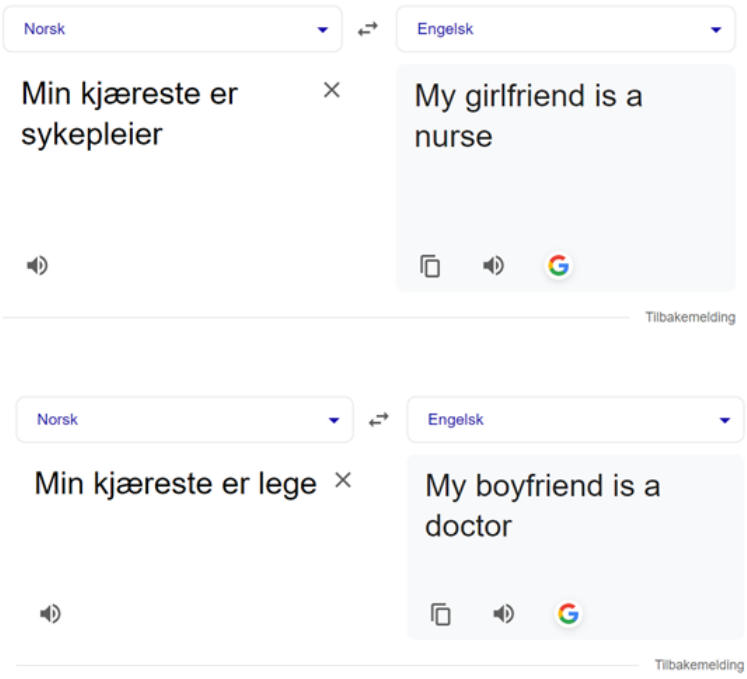
Denne typen sikkerhetsrisiko knyttet til bruk av data for trening av KI-verktøy har vært høyaktuelle den siste tiden. Et eksempel på det siste er Apple, som 10. juni 2024 offentliggjorde at selskapet skal bruke data lagret lokalt på din iPhone blant annet til å etablere et personlig tilpasset skriveverktøy og til å forbedre «Siri»-funksjonen. Dette gjøres gjennom en nysatsing som Apple snedig nok har kalt Apple Intelligence. Ambisjonen er blant annet at «Siri» skal utvikles fra å være en lenge utdatert og lite nyttig funksjon, til et skikkelig KI-verktøy som i langt større grad forstår hva du spør og hvilke svar du er ute etter – basert på dine egne data lagret på telefonen. Siden dataen lagret lokalt på telefonen likevel ikke gir godt nok treningsgrunnlag for Siri, vil Apple i tillegg bygge inn ChatGPT (utviklet av OpenAI) i iPhone og andre Apple-produkter. Elon Musk, hvis motiver er usikre og troverdighet er omstridt, var raskt ute med å kritisere Apples annonserte løsning.

En ytterligere problemstilling som gjør seg gjeldende særlig i B2B-forhold, er reguleringen av **ansvar**. Bruk av KI-løsninger har flere iboende risikoelementer ved seg. Som kjent kan KI-verktøyet være unøyaktig, ta direkte feil eller gi svar og resultater som innehar **utvalgsskjevheter** (såkalt «bias»). Slike utvalgsskjevheter er allerede velkjente for de fleste. Oversettelsesprogrammer som Google translate har lenge vært kritisert for å inneha tilbøyeligheter for utslagsskjevheter. Et kjent og konkret eksempel finnes til høyre.

Selv om eksemplet ovenfor kan virke nokså «uskyldig», oppstår det en rekke problemstillinger knyttet til reguleringen av ansvaret i tilfeller hvor næringslivet skal ta i bruk KI-løsninger. Det kan være vanskelig å oppdage slike underliggende feil og fordommer, som likevel kan få større konsekvenser. Amazon besluttet eksempelvis for noen år siden å stanse eksprementeringen med et KI-basert rekruteringssystem fordi det ble oppdaget at rekruteringssystemet foretrakk menn foran kvinner.[3] I et tenkt tilfelle hvor en slik løsning faktisk ble brukt, vil et selskap potensielt kunne gjøre seg skyldig i et ubevisst lovbrudd, herunder likestillings- og diskrimineringsloven. Dette vil igjen reise det kontraktrettslige spørsmålet: Hvis kunden kommer i ansvar for dette og dermed lider et økonomisk tap, kan kunde kreve dette økonomiske tapet erstattet fra KI-leverandøren?



I utgangspunktet vil det være kunden som er ansvarlig, både for eventuell foretaksstraff ilagt av myndighetene og potensielle erstatningskrav fra kandidater som mener seg forbigått. En videreføring av dette ansvaret i form av krav mot KI-leverandøren, kan komme på tale hvis nevnte "bias" utgjør et brudd på avtalen mellom selskapet og KI-leverandøren. Det kan i teorien også tenkes at kunden fremmer krav om erstatning mot KI-leverandøren på *deliktsgrunnlag*, samt at kandidaten fremmer *direktekrav* mot kunden. Slike tilfeller er imidlertid neppe særlig praktiske. Skulle det oppstå tvist om et slikt spørsmål, vil det også oppstå vanskelige bevismessige vurderinger: Ville egentlig kunden kommet til et annet resultat om KI-verktøyet ikke hadde utvalgsskjevheter, eller hvis kunden



3 https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G/

ikke brukte KI-verktøyet overhodet? Har kunden implementert tilstrekkelige tiltak på sin side for å redusere den kjente risikoen knyttet til slik «bias», osv.?

Et annet eksempel som kan trekkes frem, er hvordan den kontraktsrettslige ansvarsfordeling bør være i tilfeller hvor KI-verktøyet genererer resultater som krenker **tredjeparters immaterielle rettigheter**. Generative KI-løsninger er trent for å generere nye data, og vil ofte være trent på store mengder data (bilder, tekst og annet innhold) som er hentet fra internett. Treningsdataen kan derfor være beskyttet av immaterielle rettigheter. Når slike KI-løsninger brukes for å generere nytt innhold, oppstår det en risiko for at det genererte innholdet er for likt beskyttet treningsdata og at bruken av det genererte innholdet derfor kan medføre krenkelser av tredjeparters immaterielle rettigheter.

Treningsdata fra internett kan også være underlagt lisensbestemmelser, som for eksempel open source-lisenser. Flere open source-lisenser, som for eksempel GPL-lisensen, oppstiller krav om at avledede verk må distribueres under samme lisens. Slike lisensvilkår kan være problematiske i en kommersiell sammenheng, hvor selskaper typisk ønsker å bevare egen kildekode proprietær og distribuere slik kildekode under egen lisens. Vi har erfaring med selskaper som har blitt møtt med krav fra open source-lisenshavere om at bruken av slik kildekode er i strid med lisensvilkårene. I tilfeller vil det være snakk om et potensielt opphavsrettslig brudd som kan gi grunnlag for krav på økonomisk kompensasjon og opphør av bruken, hvor selve utskiftningen av kildekoden kan være både tid- og ressurskrevende.

I immaterialrettslovgivningen er ikke utvist skyld et vilkår for å fastslå en krenkelse. Dersom det genererte innholdet er likt nok, vil bruken av KI-løsningen med andre ord kunne resultere i krav om at bruken opphører og økonomisk kompensasjon. Denne risikoen er særlig stor dersom KI-modellen er trent på et begrenset datasett. Fra et kontraktsrettslig perspektiv vil utgangspunktet være at kunden er ansvarlig for egen bruk av innholdet som er generert fra KI-løsningen.

halBedrifter som ønsker å ta i bruk KI-løsninger i egen virksomhet bør derfor ha et bevisst forhold til denne risikoen når det inngås avtale med en KI-leverandør. For eksempel kan det være aktuelt å innta reguleringer som sikrer at KI-leverandøren har inngått riktige lisenser for bruk av treningsdataen, eller at KI-løsningen ikke skal trenes på spesifikt innhold som for eksempel open source-lisensiert kildekode. Det vil også være aktuelt å implementere avtalereguleringer som sikrer at kunden holdes skadesløs for potensielle brudd på tredjeparters immaterielle rettigheter.

Andreas A. Johansen er Partner i Advokatfirmaet Schjødt, hvor han spesialiserer seg i kontraktsrett og tvisteløsning, herunder knyttet til IT-kontrakter.

Anna Eide er Senior Associate i Advokatfirmaet Schjødt. Hun arbeider særlig med IP, IT og teknologi.

Illustrasjon: Colourbox.com

LOVDATA

Produksjon: Aksell AS