Lov & Data

September 2025
Nr. 163 3/2025

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.

Lov & Data

Layout: Aksell AS

Leder

Vi behöver digitaliseringsklar lagstiftning – men inte till vilket pris som helst

Hur kan lagstiftning utformas för att inte bli ett hinder för digital innovation? Det är en fråga som allt fler lagstiftare ställer sig – och som står i centrum för den växande diskussionen om digitaliseringsklar reglering både inom OECD och EU. I norden har Danmark varit ett föregångsland, och också Norge har riktlinjer för ett digitaliseringsvänligt regelverk.

Inom EU kan intresset för digitaliseringsklar lagstiftning ses mot bakgrunden av EU:s digitala agenda, som sätter ambitiösa mål för bl.a. digital infrastruktur, kunnande och offentliga tjänster. Under de senaste åren har EU-kommissionen lanserat flera initiativ för att främja digitalisering, med särskilt fokus på en europeisk dataunion. Syftet är att möjliggöra sektorsövergripande dataanvändning som drivkraft för tillväxt och samhällsutveckling. Detta kräver lagstiftning som är framtidsanpassad. dvs. som är anpassad till en föränderlig verksamhetsmiljö och som beaktar den teknologiska utvecklingen.

Kommissionen har också nyligen antagit nya riktlinjer för lagstiftningsarbetet, och en verktygslåda för bättre lagstiftning lanserades 2023. Verktygslådan innehåller en metod för digitaliseringsklar reglering (*digital-ready policymaking*). För att lagstiftningen ska vara digitaliseringsklar krävs ett nytt arbetssätt. Tvärvetenskapliga team – där jurister, teknikspecialister och policyexperter samarbetar – måste säkerställa att lagar utformas med användaren i centrum och är anpassad för automatisering och integrering i digitala system. Regelverken bör överensstämma med befintlig digital politik och bygga på principen att data bara samlas in en gång och sedan återanvänds. Samtidigt måste lagstiftningen vara flexibel nog att möta den snabbt föränderliga IT-utvecklingen, främja innovation och möjliggöra användning av ny teknik. Kort sagt: lagar måste möjliggöra

Viveca Still

digitalisering från början – inte anpassas i efterhand.

Utvecklingen inom EU:s offentliga förvaltning – både på institutionsnivå och i medlemsländerna – styrs idag av förordningen om ett interoperabelt Europa (EU) 2024/903. Förordningen kräver att en interoperabilitetsbedömning görs innan beslut fattas om nya eller väsentligt ändrade bindande krav som påverkar informationsflöden mellan offentliga sektorns organisationer inom EU och därmed påverkar deras informationssystem. EU-kommissionen har valt att tillämpa förordningen på ett ambitiöst sätt och kräver att interoperabilitetsbedömningar ska genomföras som en integrerad del av varje lagstiftningsinitiativ. Det här är en mycket välkommen utveckling.

Det är värt att notera att förordningen ändå inte ställer krav på att interoperabilititet faktiskt måste uppnås – detta är något som kan åstadkommas antingen på frivillig väg eller genom att ställa juridiskt bindande krav genom en EU-rättsakt. Inte heller innehåller förordningen i sig själv några krav på att kommissionen eller medlemsländerna ska genomföra en digitaliseringsvänlig politik eller anta riktlinjer för att uppnå en digitaliseringsklar lagstiftning.

Riktlinjer för digitaliseringsklar lagstiftning måste anpassas till nationella lagstiftningsprocesser och regelverk – och samtidigt lämna utrymme för det politiska beslutsfattandet.

I Finland pågår för närvarande ett intensivt arbete med att utveckla riktlinjer för digitaliseringsklar lagstiftning inom ramen för ett av regeringen tillsatt projekt för att identifiera och undanröja hinder för digitalisering inom den offentliga förvaltningen. Samtidigt som projektet arbetar med att röja befintliga hinder, är målet att också utveckla effektivare metoder för att främja digitalisering redan i lagberedningsskedet och proaktivt förhindra att nya digitaliseringshinder uppstår.

Det finns i Finland sedan tidigare element i lagberedningsinstruktionerna, etablerade samarbetsmodeller och lagbaserade skyldigheter att beakta bl.a. interoperabilitet och inverkan på informationssystem inom den offentliga förvaltningen. Däremot finns ännu inga koherenta riktlinjer för eller krav på att man vid lagberedningen systematisk beaktar och befrämjar möjligheten till digitalisering. Det är sådana riktlinjer man nu vill skapa.

> Riktlinjer för digitaliseringsklar lagstiftning måste anpassas till nationella lagstiftningsprocesser och regelverk – och samtidigt lämna utrymme för det politiska beslutsfattandet.

En gemensam nämnare för de initiativ som syftar till digitaliseringsklar lagstiftning är att de ofta avspeglar politiska ambitioner att effektivisera den offentliga förvaltningen. I Finland, liksom i många andra länder, finns förhoppningar om att ökad automatisering ska leda till kostnadsbesparingar och förbättrad service. Digitaliseringsklar lagstiftning handlar därför inte enbart om lagteknik – det är också ett verktyg för att systematiskt granska och utveckla lagstiftning med sikte på effektivisering genom digitala lösningar.

Det politiska intresset för artificiell intelligens (AI) är särskilt stort just nu. Många ser potentialen i AI för förvaltningsbeslut, men i Finland har man ännu inte identifierat områden där AI-baserat beslutsfattande anses lämpligt. Det har i Finland visat sig att det i de flesta fall är regelbaserad automation – snarare än avancerad AI – som eftersträvas av myndigheterna. Kanhända minskar riskerna med AI i takt med teknologins utveckling, vilket i så fall kan öppna för nya tillämpningar även inom den offentliga sektorn.

Det verkar uppenbart att det finns behov av att man systematisk analyserar möjligheterna till digitalisering (och effektivisering) inom den offentliga förvaltningen. Riktlinjer för en digitaliseringsklar lagstiftning behöver dock anpassas till varje lands respektive lagstiftningsprocesser och regelverk. Det är självklart att möjligheterna till digitalisering inte ska kunna leda till försämrat rättsskydd för medborgare, företag och andra organisationer – med andra ord måste förvaltningen även framöver styras av principerna om en god förvaltning och beakta rättsstatsprinciper och grundläggande rättigheter. Det är samtidigt viktigt att riktlinjer för digitaliseringsklar lagstiftning utformas så att de lämnar tillräckligt utrymme för politiskt beslutsfattande. De bör stödja lagstiftningsprocessen utan att påverka innehållet i politiska bedömningar eller styra sakfrågor som bör avgöras demokratiskt.

Viveca Still,
juris doktor, lagstiftningsråd.
Finsk redaktør.

Ny cybersäkerhetslag – den svenska regeringens förslag till införlivande av NIS2-direktivet

Av Agne Lindberg, Petri Dahlström og Klara Thyrén

Agne Lindberg

Petri Dahlström

Klara Thyrén

Den 12 juni 2025 presenterade den svenska regeringen lagrådsremissen om en ny cybersäkerhetslag. Förslaget bygger på den statliga utredning som lades fram under 2024 (SOU 2024:18 Nya regler om cybersäkerhet). Lagen omfattar både privata och offentliga aktörer inom de sektorer som pekats ut som samhällskritiska enligt NIS2-direktivet. Remissen visar hur regeringen föreslår att direktivet, vars syfte är att uppnå en hög cybersäkerhetsnivå för att förbättra den inre marknadens funktion, ska genomföras i svensk rätt. Efter Lagrådets granskning väntas en proposition läggas fram under hösten 2025, och den nya cybersäkerhetslagen föreslås träda i kraft den 15 januari 2026.

En mer direktivnära implementering

Regeringen föreslår en implementering som i högre grad än utredningens förslag följer NIS2-direktivets struktur och terminologi, vilket kan underlätta såväl tillämpning som tillsyn. Myndigheten för samhällsskydd och beredskap (MSB) ges en central roll i tillämpningen av lagen.

Ett centralt ställningstagande är att lagens krav ska gälla hela organisationen, även om bara en del av verksamheten bedrivs inom NIS2-direktivets tillämpningsområde. Anledningen är att en mer begränsad tillämpning riskerar att urholka regelverkets syfte och effektivitet. Att verksamheten endast bedrivs inom en del av organisationen påverkar därför inte lagens tillämplighet.

För enskilda verksamhetsutövare gäller som huvudregel ett storlekskrav som motsvarar ett medelstort företag, vilket innebär att verksamheten måste sysselsätta minst 50 personer eller ha en årsomsättning som överstiger 10 miljoner euro för att omfattas. Från denna huvudregel finns dock undantag – vissa av lagen särskilt utpekade enskilda verksamhetsutövare omfattas oavsett storlek, och MSB ges dessutom en uttrycklig roll att peka ut mindre aktörer som bedöms särskilt kritiska för samhällets funktion.

> Ett centralt ställningstagande är att lagens krav ska gälla hela organisationen, även om bara en del av verksamheten bedrivs inom NIS2-direktivets tillämpningsområde.

I övrigt följer lagrådsremissen i huvudsak utredningens förslag, men regeringen gör vissa justeringar. Utredningen föreslog att vissa verksamhetsutövare som omfattas av bilagorna till NIS 2-direktivet och som är etablerade i Sverige ska omfattas av lagen, oavsett om de uppfyller storlekskravet, med hänvisning till deras särskilda samhällsbetydelse. Regeringen delar

i huvudsak denna bedömning men gör på vissa punkter en annan avvägning än utredningen.

Utredningen menade att en förutsättning bör vara att verksamheten är väsentlig för att upprätthålla kritiska samhälleliga och ekonomiska funktioner. Regeringen anser emellertid att det i stället bör krävas att verksamhetsutövaren är den enda leverantören i Sverige av en tjänst som är nödvändig för sådana funktioner. Enligt regeringen stämmer kravet på att verksamhetsutövaren ska vara den enda leverantören av en sådan tjänst bättre överens med direktivets utformning.

Utredningen föreslog vidare att samtliga statliga myndigheter skulle omfattas av lagen. Regeringen gör en mer begränsad tolkning av direktivet och föreslår i stället att endast statliga myndigheter med beslutskompetens som kan påverka den fria rörligheten inom EU, samt vissa ytterligare myndigheter som regeringen utser, ska omfattas. Vilka statliga myndigheter som anses uppfylla kriteriet beror på om deras beslut kan påverka den fria rörligheten på längre sikt. Detta innebär att det för varje myndighet krävs en individuell bedömning av om den omfattas av lagens tillämpningsområde. Vidare framgår att kommuner, regioner och kommunalförbund omfattas och klassificeras som väsentliga verksamhetsutövare under förutsättning att de når upp till storlekströskeln för ett medelstort företag.

Krav på säkerhetsåtgärder

Organisationer åläggs att vidta både tekniska och organisatoriska säkerhetsåtgärder. Med detta avses exempelvis riskhantering, incidentberedskap, kryptering och säkerhet i leveranskedjan. Dessa ska vara riskbaserade, proportionerliga och lämpliga i relation till risken. Regeringen lyfter vidare fram att krishantering ska ses som en egen del av cybersäkerhetsarbetet. Det innebär att organisationer inte bara ska förebygga och upptäcka incidenter, utan också aktivt planera för hur de ska agera om en kris inträffar. Utredningen föreslog vidare att lagen skulle innehålla ett uttryckligt krav på ett systematiskt och riskbaserat informationssäkerhetsarbete. I lagrådsremissen saknas detta krav, men regeringen framhåller att verksamhetsutövare trots detta förväntas arbeta systematiskt. Vi konstaterar att det kommer att vara svårt att uppfylla kraven enligt NIS2-direktivet om man inte arbetar systematiskt och riskbaserat, exempelvis genom att följa ISO 27000-standarden.

När det gäller kravet på säkerhet i leveranskedjan skiljer sig regeringens förslag från utredningens. Även om kravet på säkerhet i leveranskedjan tar sikte på förhållandet till direkta leverantörer måste, enligt regeringen, även risker hos underleverantörer beaktas. Kraven omfattar hela systemens livscykel, från förvärv och utveckling till underhåll. Med förvärv avses fall där en organisation tar över ett system med äganderätt. Men regeringen framhåller att säkerhetskraven gäller även när man inte äger systemet, till exempel vid utkontraktering och licensiering. Sammantaget visar detta att säkerhetsansvaret sträcker sig längre än till den egna organisationen.

Vi konstaterar att det kommer att vara nödvändigt för verksamheter att genomföra systematiska risk- och sårbarhetsanalyser. På grundval av dessa analyser avgörs vilka konkreta säkerhetsåtgärder som ska vidtas, samtidigt som det är viktigt att dokumentera och motivera skälen till varför vissa åtgärder bedöms tillräckliga. En analys bör dessutom regelbundet revideras och uppdateras för att säkerställa att säkerhetsåtgärderna förblir ändamålsenliga och aktuella.

Nyheter om utbildning, anmälan, tillsyn och ledningsförbud

Ett tydligt exempel på regeringens mer försiktiga linje är utbildningskraven. Utredningen föreslog att alla anställda skulle erbjudas cybersäkerhetsutbildning, men regeringen anser att det inte är motiverat och begränsar därför kravet till ledningen. Samtidigt måste verksamhetsutövare vidta flera säkerhetsåtgärder, såsom grundläggande cyberhygien, utbildning i cybersäkerhet och personalsäkerhet. Regeringen understryker att dessa åtgärder redan uppmuntrar till regelbunden utbildning även för övriga medarbetare.

Vidare följer regeringen i stort utredningens modell med sektorsvisa tillsynsmyndigheter, men föreslår samtidigt några viktiga justeringar och förtydliganden. Bland annat ska tillsynsmyndigheter kunna vidta åtgärder mot viktiga verksamhetsutövare redan när det finns ”anledning att anta” att reglerna inte följs – en lägre tröskel än utredningens ”befogad anledning”. En annan nyhet är att anmälan om verksamhet som omfattas av lagen inte ska göras till respektive tillsynsmyndighet, utan till en ny central myndighet som regeringen ska utse.

Vidare förtydligas förutsättningarna för meddelande av förbud att inneha ledningsfunktion. Om en väsentlig verksamhetsutövare bryter mot centrala skyldigheter – exempelvis att utse företrädare, anmäla verksamheten, vidta säkerhetsåtgärder, genomföra utbildning eller rapportera incidenter – kan tillsynsmyndigheten ansöka om att en befattningshavare förbjuds att inneha ledningsfunktion. I lagrådsremissen tydliggörs att förbudet endast gäller just väsentliga verksamhetsutövare. För att ett sådant förbud ska kunna beslutas krävs att överträdelsen är allvarlig och att personen agerat uppsåtligen eller grovt oaktsamt.

Vägen framåt – ekonomiska effekter och långsiktiga fördelar

Den föreslagna cybersäkerhetslagen representerar en omfattande transformation av det svenska cybersä-

kerhetslandskapet, och den slutliga utformningen kommer att vara avgörande för hur framgångsrikt Sverige lyckas stärka sin cybersäkerhet i enlighet med EU:s ambitioner.

Införandet av den nya lagen förväntas medföra betydande ekonomiska konsekvenser och ett ökat resursbehov för både verksamhetsutövare och tillsynsmyndigheter. Regeringen uppskattar att över 1 500 företag i Sverige med totalt omkring 500 000 anställda kan komma att påverkas av den nya lagen och tillhörande föreskrifter. Den största kostnaden för enskilda verksamhetsutövare bedöms vara kopplad till de säkerhetsåtgärder som måste vidtas.

En konsekvent nivå av cyberresiliens bland centrala verksamhetsutövare kan dock leda till kostnadsbesparingar på längre sikt. EU-kommissionen har uppskattat att införandet av bestämmelserna i NIS2-direktivet kan leda till en minskning av kostnaderna för cyberincidenter med 11,3 miljarder euro inom unionen. Med rätt implementering och tillräckliga resurser är således förhoppningen att den nya lagen ska bidra till att skapa en mer resilient digital infrastruktur som gynnar både näringslivet och samhället i stort.

Agne Lindberg , delägare och ansvarig för Delphi Business Advisory verksamhetsgrupp som inkluderar Tech & IP. Verksam inom tech juridik med särskilt fokus på IT-avtal, informationssäkerhet, immaterialrätt och dataskydd.

Petri Dahlström, verksam i Delphis tech & IP-grupp och främst specialiserad inom informationssäkerhet, kommersiella avtal, immateriella rättigheter och gaming.

Klara Thyrén, verksam i Delphis tech & IP-grupp och arbetar huvudsakligen med kommersiella avtal, dataskydd, IT och immaterialrätt.

Illustrasjon: Colourbox.com

Digital inkludering og EUs tilgjengelegheitsdirektiv (EAA)[1]

Av Sigbjørn Råsberg

Vi lever ei eit gjennomdigitalisert samfunn. Dei fleste av oss nyter godt av fruktene vellukka digitalisering gir oss, slik som auka fleksibilitet, automatisering, raskare prosessar osb. Dette gjer at vi raskare får svar på søknadar, slepp å gå frå hus til hus med nabovarsel og har full tilgang til foreldrepermisjonssøknaden nær sagt kvar og kva tid som helst. Føresetnaden er likevel at vi tek i bruk dei digitale løysingane som gir desse moglegheitene.

Ein del personar ønskjer ikkje å vere digitale. Dei lever heilt fint utan desse fruktene. Det er heilt greitt. Meir problematisk er det då med dei som ønskjer å ta i bruk dei digitale løysingane, men ikkje er i stand til å gjere det fordi dei opplever at den digitale verda ikkje slepp dei inn.

Digitaliseringa av samfunnet tvingar slik fram eit fokus på digital inkludering for å sikre at flest mogleg av dei som ønskjer det kan ta nytte av fordelane digitaliseringa gir.

Ofte blir det sett likskapsteikn mellom digital inkludering og kompetanseheving av sluttbrukaren i form av datakurs for eldre, hjelpetelefonar, servicetorg osb. Å byggje grunnleggjande digital dugleik er avgjerande for dei som treng det, men tek i lita grad innover seg behova til dei som er digitale, men som opplever at løysingane ikkje er utforma på ein måte som gjer at dei kan ta dei i bruk.

For å seie det på ein annan måte: Digital inkludering handlar ikkje berre om å endre brukaren, men

Sigbjørn Råsberg

også om å byggje gode og brukarsentrerte ikt-løysingar som er utforma på ein slik måte at flest mogleg kan ta dei i bruk. Dette inkluderer mellom anna universell utforming (UU), brukaroppleving (UX), brukargrensesnitt (UI), klarspråk, tillit osb.

Digital inkludering knytast opp mot fleire av FNs berekraftsmål,[2] men har også eit forretningsaspekt i form av at vinsten av å digitalisere ein prosess er større både for tenesteeigaren og borgarane når flest mogleg får nytte av løysingane.

Kven må inkluderast digitalt?

Samla er det lagt til grunn at om lag 20 % av innbyggjarane i Noreg har ei form for fysisk eller psykisk funksjonsnedsetjing.[3] Av desse er det igjen 70 % som rapporterer at dei har utfordringar med bruk av teknologi.[4]

Det er likevel ikkje slik at det berre er desse som har nytte av brukarsentrerte ikt-løysingar. Mange av tilpassingane er nyttige for alle. Det mest openberre er nok klarspråk og intuitivt brukargrensesnitt, men dei fleste av oss kjem i ulike samanhengar gjennom kvardagen og livet til å ha stor glede av universell utforming, då funksjonstap kan vere varig, mellombels og situasjonsbestemt.

> Digital inkludering handlar ikkje berre om å endre brukaren, men også om å byggje gode og brukarsentrerte ikt-løysingar som er utforma på ein slik måte at flest mogleg kan ta dei i bruk.

Til dømes er det å vere døv eller ha tinitus tilstandar som gir varige utfordringar med høyrselen. Då er lyd som einaste informasjonskjelde problematisk. Den same utfordringa vil mange i kortare periodar, td.

1 Artikkelen er ei komprimert skriftleggjering av føredraget forfattaren heldt for Norsk forening for juss og EDB 26. mai 2025

2 Mål 4 om utdanning, gjennom delmål 4.5 og 4.a)
Mål 8 om anstendig arbeid og økonomisk vekst
Mål 9 om innovasjon og infrastruktur, gjennom delmål 9.1
Mål 11 om berekraftige byar og samfunn, gjennom delmål 11.2
Mål 16 om fred og rettferd, gjennom delmål 16.10

3 DFØs Innbyggerundersøkelse frå 2021 spørsmål AQ418

4 Tilsynet for universell utforming av ikt: «Erfaringer med bruk av ikt-løsninger blant personer med funksjonsnedsettelser» 16. juni 2020, *https://www.uutilsynet.no/kartlegginger/erfaringer-med-bruk-av-ikt-losninger-blant-personer-med-funksjonsnedsettelser/941*

grunna ein øyreinfeksjon. Høyrselstap kan også vere situasjonsbestemt, typisk når vi er i eit støyande område eller ein stad det ikkje høver seg å spele av lyd.

Tilsvarande er td. demens, utviklingshemming og hjerneskade varige kognitive funksjonsnedsetjingar, men personar i td. livskriser som samlivsbrot og alvorleg sjukdom kan oppleve mange av dei same utfordringane. Tilsvarande kan stress og lite søv gje ein situasjonsbestemt redusert kognitiv funksjon.

Det same gjer seg gjeldande også for andre funksjonsnedsetjingar som syn, språk og motorikk. Dette viser at tiltak for digital inkludering er nødvendig for nokon, men bra for alle.

EU som motor for digital inkludering

Vi er midt i det EU har utropt som det digitale tiåret. Saman med mellom anna det digitale kompasset og EU-deklarasjonen om digitale prinsipp og rettar er målet å leggje til rette for digital transformasjon som møter både innbyggjaranes og verksemdenes behov på ein forsvarleg måte. Det er mellom anna legg vekt på digital inkludering som ein suksessfaktor for vellukka digitalisering av samfunnet og at alle skal kunne ta del i digitaliseringa.[5] Dette, og tidlegare initiativ, har gjort EU til drivaren for regulering og standardisering på området.

Det første regulatoriske steget var EUs webdirektiv (WAD),[6][7] som innførte nye tekniske krav for appar, nettstadar, intranett og ekstranett i offentlege verksemder, samt krav om tilgjengelegheitserklæring for appar og nettstadar.

I EU tok WAD til å gjelde trinnvis for offentlege verksemder. Først 23. september 2019 for nettstadar som var publiserte 23. september 2018 eller seinare. Vidare tok regelverket til å gjelde for alle nettstadar uavhengig av publiseringstidspunkt 23. september 2020. Til sist tok regelverket til å gjelde for alle appar frå 23. juni 2021.

Prosessen med å ta WAD inn i EØS-avtalen vart noko forseinka, som gjorde at det ikkje tok til å gjelde i Noreg før 1. februar 2023.[8] På Island er framleis ikkje WAD gjennomført i nasjonal, noko som har ført til at ESA har teke Island inn for EFTA-domstolen for brot på EØS-avtalen.[9]

EUs tilgjengelegheitsdirektiv (EAA)

Sjølv om EAA[10] vart banka gjennom i EU 2,5 år etter WAD, er det ikkje tvil om at desse direktiva går hand i hand. Begge stiller tekniske krav til universell utforming av iktløysingar, og ei vanleg misforståing er at WAD regulerer offentleg sektor, medan EAA regulerer privat sektor. I praksis er dette til ei viss grad riktig, men formelt regulerer EAA utvalde produkt og tenester – uavhengig av om dei er tilbydde av offentlege eller private verksemder. Det kan slik variere mellom land om pliktsubjekta er offentlege eller private aktørar. Særleg gjeld dette enkelte typar produkt og tenester knytt til transport.

Ei anna utbreidd misforståing, som eg til dels er med på å spreie tidlegare i denne teksten, er at EAA har som føremål å bidra til digital inkludering. Realiteten er at EAA *hovudsakleg* er eit indre marknad-direktiv og at føremålet er å leggje til rette for frihandel.[11] Dette forklarer kvifor EAA ikkje regulerer heile brukarreiser, som ville vore naturleg om EAA hovudsakleg var eit rettigheitsdirektiv. I staden regulerer EAA utvalde produkt, tenester og det felles-europeiske naudnummeret 112,[12] noko som kan opplevast fragmentert, usamanhengande og inkonsekvent for sluttbrukarane.

Produkta som er omfatta av EAA er:[13]

- Maskinvare- og operativsystem til datamaskiner for forbrukarar
- Betalingsterminalar
- Minibankar, billettmaskiner, innsjekkmaskiner og interaktive informasjonskioskar[14] når dei yter tenester som er omfatta av EAA
- Smarttelefonar ol. for forbrukarar
- Smartskjermar, dekodarar ol. for forbrukarar
- Lesebrett

Tenestene som er omfatta av EAA er:[15]

- Elektroniske kommunikasjonstenester[16]
- Audiovisuelle medietenester
- Nettstadar, appar, elektroniske billettar, reiseinformasjon og interaktive sjølvbeteningstermina-

5 European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01) Kapittel II

6 Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies

7 Sjå Bärlund og Råsberg: «Nytt i nytt direktiv: EUs webdirektiv setter nye tilgjengelighetskrav til nettsteder og apper», Juridika Innsikt, 12. august 2022, *https://juridika.no/innsikt/nytt-i-nytt-direktiv-eus-webdirektiv-setter-nye-tilgjengelighetskrav-til-nettsteder-og-apper*

8 Jf. Endr. i forskrift om universell utforming av informasjons- og kommunikasjonsteknologiske (IKT)-løsninger del II

9 *https://www.eftasurv.int/newsroom/updates/esa-takes-iceland-court-failing-implement-eea-rules-accessibility-public-websites*

10 Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services

11 Sjå særleg EAA art. 1 og fortalens punkt 1

12 Jf. art. 2

13 Jf. art. 2 (1)

14 Unnateke terminalar som er installerte som ein integrert del av køyretøy, fly, skip og rullande materiell.

15 Jf. EAA art. 2 (2)

16 Unnateke reine maskin-til-maskin-tenester

lar[17] for transport i luft, skinner, buss og vatn[18]
- Banktenester for forbrukarar
- E-bøker og tilhøyrande programvare
- E-handel

Dei tekniske krava kjem av EAA art. 4, som igjen viser til Vedlegg I. Her er det stilt opp ei rekkje overordna krav, slik som at informasjon skal vere tilgjengeleg via meir enn éin sensorisk kanal, automatar skal tilby tekst-til-tale-teknologi og moglegheit til å kople til personlege høyretelefonar og krav til klarspråk.

Desse tekniske krava skal også nyttast som krav til universell utforming etter anskaffingsforskrifta § 15-2 og forsyningsforskrifta § 11-2, i anskaffingar av varer og tenester som er regulerte av EAA.[19]

Krava i Vedlegg I kjenner vi i stor grad igjen frå operasjonaliseringa av WAD. Mange av krava er såpass overordna at det kan vere krevjande å operasjonalisere dei. Dette må sjåast i samanheng med at EAA byggjer på «den nye metoden», som vil seie at direktivet stiller opp overordna tekniske krav og ein referanse til harmoniserte standardar. Samsvar med dei harmoniserte standardane gir ein presumsjon om samsvar med dei overordna krava.[20] Samsvar med standarden er likevel ikkje einaste måten å møte dei tekniske krava, men i praksis vil det for dei fleste vere det enklaste, særleg mtp. å også møte krava til dokumentasjon av samsvar med krava i direktivet.[21]

Kommisjonen har gitt dei europeiske standardiseringsorganisasjonane eit mandat[22] for revidering av tre eksisterande[23] og utarbeiding av tre nye[24] standardar som skal harmoniserast. Allereie i mandatet var det lagt opp til ferdigstilling av standardane frå tre månadar til 1,5 år etter regelverket tok til å gjelde i EU. I skrivande stund er arbeidet delvis forseinka, noko som gir store utfordringar for både industrien og myndigheitsorgana i deira operasjonalisering av krava.

Med nokre unntak,[25] må dei økonomiske aktørane[26] sikre at produkta og tenestene som er omfatta av direktivet – og som dei tilbyr, produserer eller gjer tilgjengeleg på marknaden – er i samsvar med dei tekniske krava.[27]

I tillegg til dei reint tekniske krava, stiller EAA også opp krav til at tenestetilbydarar utarbeider nødvendig informasjon i samsvar med Vedlegg V og forklarer korleis tenesta møter krava til universell utforming.[28] Produsentar av produkt må på same måte sikre at dei er i samsvar med krava, utarbeider teknisk dokumentasjon i samsvar med Vedlegg IV og påfører CE-merke viss produktet er i samsvar med krava.[29][30] Importørar og distributørar har også ei plikt til å kontrollere at produsenten etterlever sine plikter.[31]

I den grad økonomiske aktørar ikkje klarer å gjere tiltak for å kome i samsvar med krava pliktar dei å med ein gong informere myndigheitsorganet.[32]

Unntak

Som vanleg er det ingen reglar utan unntak. Viss vi ser vekk frå dei meir spesielle unntaka,[33] stiller EAA i utgangspunktet opp to generelle unntak som kan krevjast av alle økonomiske aktørar for alle produkt og tenester som oppfyller vilkåra.[34] I begge tilfelle må den økonomiske aktøren dokumentere kvifor unntak gjer seg gjeldande og gjere dokumentasjonen tilgjengeleg for myndigheitsorganet på førespurnad.[35]

Vesentleg endring

Direktivet går ikkje i detalj om kva som utgjer ei vesentleg endring, men refererer til grunnleggjande endringar som verkar inn på produktet eller tenestas «basic nature». Sjølv om det står igjen å operasjonalisere dette unntaket, er det naturleg å forstå unntaket som at dei tekniske krava må kome i vegen for føremålet med produktet eller tenesta, og at terskelen slik blir veldig høg.

Uhøveleg byrde

Ulikt vesentleg endring, er unntaket for uhøveleg byrde i stor grad konkretisert Vedlegg VI gjennom tre alternative grunnlag. Dette heimlar

17 Unnateke terminalar som er installerte som ein integrert del av køyretøy, fly, skip og rullande materiell brukt til passasjertransport
18 Unnateke transport i byar og forstadar, samt regionale transporttenester, der det berre er krav til interaktive sjølvbeteningsterminalar
19 EAA art. 24 (1), jf. direktiv 2014/24/EU art. 42(1) og direktiv 2014/25/EU art. 60(1)
20 Jf. EAA art. 15 (1)
21 Jf. EAA Kapittel III, jf. Vedlegg IV, og Kapittel IV, jf. Vedlegg V
22 M587
23 EN 301 549 Accessibility requirements for ICT products and services EN 17161:2019 Design for All og EN 17210 Accessibility and usability of the built environment
24 Ikkje-digital informasjon knytt til produkt, hjelpetenester til produkt og tenester, samt ein standard for naudkommunikasjon
25 Unntaket for mikroverksemder som tilbyr tenester, jf. art. 4 (5) er særleg aktuelt
26 Produsentar, autoriserte representantar, importørar og distributørar av produkt, samt tenestetilbydarar, jf. EAA art. 3 (21)
27 Jf. EAA art. 4 (1)
28 Jf. EAA art. 13
29 Jf. EAA art. 7
30 Sjå også 2022/C 247/01 Commission notice – The 'Blue Guide' on the implementation of EU product rules 2022
31 Jf. EAA art. 8 og 9
32 Jf. EAA art. 7 (8), 9 (8), 10 (5) og 13 (4)
33 Til dømes ulike unntak for mikroverksemder og konkrete former for innhald på nettstadar og appar, jf. EAA art. 2 (4)
34 Jf. EAA art. 14
35 Jf. EAA art. 14 (2) og (3)

unntak når det å gjere produktet eller tenesta i samsvar med krava vil vere uhøveleg kostbart/tyngjande sett opp mot:

1. dei totale kostnadane knytt til produsere, distribuere eller importere produktet eller tilby tenesta
2. fordelane personar med funksjonsnedsetjingar oppnår
3. nettoomsetjinga hos den økonomiske aktøren

Vurderingane er skjønnsmessige, og det står igjen å operasjonalisere terskelen, men det er rimeleg å leggje til grunn at den er høgare for nye produkt og tenester enn for eksisterande.

Illustrasjon: Colourbox.com

Marknadsovervaking og tilsyn

Med krav kjem også kontroll og myndigheitsorgan. EAA stiller krav om marknadsovervaking med produkt[36] og tilsyn med tenester[37]. Dette inneberer mellom anna kontroll av om produkt og tenester er i samsvar med dei tekniske krav, dokumentasjonen av desse, samt om vilkåra er oppfylte for eventuelle unntak som er gjort gjeldande.

Direktivet gir myndigheitsorgana slagkraftige verktøy, slik som pålegg om å rette feil på produkt og trekkje produktet frå marknaden. I siste omgang kan dei gje produktet marknadsnekt og varsle Kommisjonen og dei andre medlemslanda.[38]

EAA art. 29 slår fast at det skal vere høvelege og effektive verktøy for å sikre samsvar med krava til produkt og tenester, inkl. klage og domstolstilgang. Vidare slår art. 30 fast at ein nasjonalt skal etablere føringar for sanksjonar og at desse skal vere effektive, proporsjonale og avskrekkande. Dette heimlar mellom anna bøter. Utmåling må sjåast i samanheng med fortalens (98), som slår fast at sanksjonane skal vere så strenge at dei ikkje fungerer som eit alternativ til å møte krava.

Status for gjennomføring av EAA i Norden

For EU-landa Sverige, Danmark og Finland tok EAA til å gjelde 28. juni 2025.

> EAA er enno ikkje teke inn i EØS-avtalen og det er slik framleis uklart kva tid det skjer og slik når regelverket tek til å gjelde for EFTA-landa.

For EFTA-landa Noreg og Island er situasjonen annleis. EAA er enno ikkje teke inn i EØS-avtalen og det er slik framleis uklart kva tid det skjer og slik når regelverket tek til å gjelde for EFTA-landa.

I Noreg er det Kultur- og likestillingsdepartementet som er ansvarleg for gjennomføringa av EAA. Her har arbeidet i praksis stått stille sidan høyringa hausten 2021. Bakgrunnen for dette er særleg usikkerheit kring om EAA er eit minimumsdirektiv eller totalharmoniserande, og kva det vil seie for verkeområdet for dagens regelverk[39] og forholdet til FN-konvensjonen for menneske med nedsett funksjonsevne (CRPD).

Forseinka EFTA-gjennomføring har likevel ikkje noko å seie for norske og islandske verksemder som har ein marknad i EU for sine produkt og tenester. Desse må tilpasse seg krava i EAA for å framleis ha tilgang til marknaden i EU. I mangel på ferdige harmoniserte standardar må desse etter beste evne setje seg inn i dei nasjonale føringane i EU-landa dei opererer i, basert på dei overordna krava i Vedlegg I, og om mogleg støtte seg til siste versjonsnummer av standardane som er under revisjon.

Sigbjørn Råsberg er jurist frå Universitetet i Bergen og Háskólinn í Reykjavík, og jobbar som seniorrådgjevar i Digitaliseringsdirektoratets Tilsyn for universell utforming av ikt.

36 Jf. EAA kapittel VIII
37 Jf. EAA kapittel IX
38 Jf. EAA art. 20

39 Forskrift om universell utforming av ikt-løsninger har til dels vidare verkeområde enn EAA, særleg for automatar

Kommentar til artikkel om Birkenstock-saken

Av Camilla Vislie

Advokatene Nicholas Foss Barbantonis og Henning Wahlberg har i *Lov & Data* uttalt seg om en dom fra den høyeste domstolen (Bundesgerichthof) i Tyskland i den såkalte Birkenstock-saken, der domstolen kom til at utformingen ikke var beskyttet av opphavsretten. Begrunnelsen var i korte trekk at Birkenstock-sandalen ikke oppfylte kravene til et «verk» i opphavsrettslig forstand, fordi den ikke kunne kategoriseres som kunst, men som ren design.

Artikkelforfatterne hevder at Birkenstock-avgjørelsen «illustrerer den grunnleggende forskjellen mellom kunstneriske og funksjonelle elementer i et verk (…). Birkenstock hadde ikke sannsynliggjort en tilstrekkelig utnyttelse av det kunstneriske spillerommet. Det kunne ikke godtgjøres at Birkenstock-sandalene skilte seg kunstnerisk fra den ordinære utformingen av ergonomiske sandaler som allerede var kjent på 1960- og 1970-tallet, som er tidspunktet de aktuelle modellene ble skapt.»

Etter en gjennomgang av norsk rettspraksis om verkshøydekravet for brukskunst (Rt. 1962 s. 964 (Wegner), Rt. 2012 s. 1062 (Tripp Trapp), Rt. 2013 s. 822 (Ambassadør) og *HR-2017-2165-A* (Il Tempo Gigante). Rt. 2013 s. 822 (Ambassadør) konstaterer artikkelforfatterne at avgjørelsene vektlegger opphaverens frie og kreative valg som grunnlag for opphavsrettslig vern, men hevder samtidig også at «det Birkenstock-avgjørelsen tilfører, er en mer presis sondring mellom kunstneriske og funksjonelle elementer, og en tydeligere definisjon av hva som kreves for at et verk skal oppnå beskyttelse.»

Camilla Vislie

Det er lett å være enig med Barbantonis og Wahlberg i at Birkenstock-avgjørelsen er interessant. Påstanden om at den bidrar til å «klarlegge grensene for opphavsrettsbeskyttelse for brukskunst etter opphavsrettsdirektivet» og tilfører «en mer presis sondring mellom kunstneriske og funksjonelle elementer, og en tydeligere definisjon av hva som kreves for at et verk skal oppnå beskyttelse», må imidlertid tas med en klype salt. Dommen kan heller ikke bidra til å heve terskelen for å oppnå opphavsrettsbeskyttelse for brukskunst, slik det hevdes i artikkelen. Det ville tvert imot være feil hvis norske domstoler skulle følge premissene i den tyske dommen.

Den tyske domstolen tar riktig utgangspunkt i at begrepet opphavsrettslig beskyttet verk og det nødvendige nivået av originalitet er autonomt, og må tolkes og anvendes enhetlig i hele EU. Det er også riktig at gjenstanden må være original i den forstand at den utgjør «opphavsmannens egen intellektuelle frembringelse». En gjenstand er original hvis den reflekterer opphaverens personlighet ved å uttrykke hans eller hennes frie kreative valg. Hvis utformingen derimot er bestemt av tekniske hensyn eller andre begrensninger som ikke gir rom for å ta kunstneriske valg, kan det derimot ikke legges til grunn at gjenstanden har den nødvendige originalitet, og det faktum at en gjenstand har en estetisk effekt er som sådan ikke relevant. Alt dette er ukontroversielt, og følger av EU-domstolens praksis, blant annet i sakene Levola Hengelo (C-310-17), Cofemel (C-683/17) og Brompton Bicycle (C-833/18).

> Dommen kan heller ikke bidra til å heve terskelen for å oppnå opphavsrettsbeskyttelse for brukskunst, slik det hevdes i artikkelen.

Senere i premissene faller imidlertid den tyske domstolen ut av EU-sporet og refererer til eldre tysk rettspraksis, der det avgjørende har vært om (fritt oversatt og forkortet) «gjenstandens estetiske innhold har nådd et slikt nivå at personer som er mottagelige for kunst og rimelig kjent med kunstvurdering vil kunne si at det er snakk om en 'kunstnerisk prestasjon' – den estetiske effekten av designet kan kun rettferdiggjøre opphavsrettsbeskyttelse hvis den er basert på en kunstnerisk prestasjon og uttrykker dette». Det må altså være snakk om «kunst» i en kunstkritikers øyne, noe som reflekterer en særegen tysk tilnærming til opphavsrettsbeskyttelse, og setter en svært høy terskel for originalitet.

For å få dette til å stemme med den EU-rettslige normen, skriver domstolen at denne særtyske terskelen «i det vesentlige» må anses som harmonisert med det autonome EU-rettslige verksbegrepet. Det kan neppe være riktig.

Uansett er det nå to forente saker fra Sverige og Tyskland som venter på avgjørelse fra EU-domstolen som vil få vesentlig større betydning for grensedragningen for opphavsrettslig vern for brukskunst. Spørsmålene som er forelagt EU-domstolen i Mio (C-580/23), og konektra (USM Haller) (C-795/23) går rett i kjernen av opphavsretten og gjelder blant annet kravene til verkshøyde og hvordan originalitet skal vurderes på området for industriell design. Når EU-domstolen avsier dom i de forente sakene, vil vi forhåpentligvis få en ny og viktig avklaring av dette spørsmålet.

Generaladvokaten var i sin uttalelse 8. mai i år avvisende til å bruke begrepet «kunstnerisk verdi» når det gjelder opphavsrettsbeskyttelse av industriell design: «Det (…) oppstår en risiko for forvirring når begrepene 'kunstnerisk' eller 'estetisk' brukes for å karakterisere de valg som opphaveren har gjort eller resultatet av hans eller hennes frembringelse. (..) slike vurderinger (er) ikke relevante i opphavsretten: beskyttelse er på ingen måte betinget av den kunstneriske (eller andre) kvaliteten på verket, heller ikke for så vidt gjelder brukskunstverk. Etter min mening er det derfor mer hensiktsmessig å holde seg til ordene 'frie og kreative valg som reflekterer opphaverens personlighet'.»

Illustrasjon: Colourbox.com

Uttalelsen følger på dette punktet opp EU-domstolens praksis i sakene som er nevnt over, Den nevnte tyske tilnærmingen er derfor ikke aktuell, med mindre EU-domstolen skifter retning i dette spørsmålet.

Camilla Vislie (H) er partner i Thommessens avdeling for immaterialrett, og arbeider med rådgivning og tvisteløsning innenfor teknologidrevne bransjer.

Unyttige databehandleravtaler

Av Jaime Espantaleón

1. Roller

I enhver situasjon det behandles opplysninger om fysiske personer møter man flere aktører som kan være involvert i behandlingen. Den viktigste er den som er direkte berørt av behandlingen, den registrerte, som «eier» egne opplysninger. Opplysninger regelverket verner om. Dernest har vi den behandlingsansvarlige som har det personvernmessige ansvaret overfor førstnevnte om håndteringen av vedkommendes opplysninger. Denne bestemmer formålet med behandling personopplysninger, og hvordan behandlingen bør skje. Ofte vil en finne en eller flere databehandlere knyttet til behandlingsansvarlig etter avtale. Noen ganger finnes dessuten «mottakere». Disse kan for eksempel være andre behandlingsansvarlige som det utleveres personopplysninger til. Videre kan *tredjeparter* være aktuelle rollehavere. Disse siste er andre personer enn den registrerte, behandlingsansvarlige eller databehandleren, som har berettigede interesser i behandlingen.

Personvernforordningen definerer på samme måte som det tidligere regelverket, personverndirektivet, alle disse aktørene. Resultatet er mer eller mindre godt, men i realiteten gis bare tre roller oppmerksomhet; den registrerte (the Good), den behandlingsansvarlige (the Bad) og databehandleren (the Ugly). Den første er rettighetssubjektet, mens de øvrige er pliktsubjekter.

I denne artikkelen gis det en forenklet oversikt over dette trekantforholdet, for deretter å sentrere drøftelsen rundt hvorfor databehandlerforhold innad i staten ikke gir mening.

Jaime Espantaleón

2. Ansvarsforhold

Personvernforordningen, som gir uttrykk for EUs sekundærlovgivning, er en utpensling av den grunnleggende menneskeretten om respekt for privatliv og familieliv i artikkel 8 i menneskerettskonvensjonen og i artikkel 8 i EUs Charter om grunnleggende rettigheter. Forordningen verner bare om fysiske rettighetssubjekter. Juridiske er utelatt, selv om disse har krav på privatlivets vern etter EMK-konvensjonen.

Den registrerte (the Good) har således etter det europeiske regelverket rett på at behandlingen av personopplysninger skjer etter grunnleggende normer, er lovmessig, rettferdig, transparent, nødvendig, formålstjenlig og sikker. Det har krav på å bli informert, å få kopi av egne data, ha mulighet til å gi egne opplysninger til andre, motsette seg behandlingen, kreve retting og sletting eller begrensning mv.

Ansvaret for at behandlingen skjer i tråd med prinsippene, samt for å tilrettelegge for utøvelsen av alle disse rettighetene hviler på den behandlingsansvarlige (the Bad). Det er denne som bærer pliktene etter forordningen. Den må påse at behandlingen skjer i tråd med prinsippene, at den er lovlig, transparent, nødvendig, mv. Den må informere, gi kopi, rette, slette, begrense, overføre, mv., og sikre opplysningene. Organisatoriske og tekniske tiltak skal implementeres og dokumenteres både løpende og før utvikling av løsningene som behandler personopplysninger. Behandlingsansvarlig må samtidig velge med omhu databehandleren (the Ugly) den setter ut behandlingen til. Den må inngå en avtale eller annet rettslig bindende instrument som angir rammene for databehandlerens opptreden.

> Offentlige myndigheter under staten, kan ikke opptre som databehandlere for hverandre.

Databehandleren har i utgangspunktet tre sentrale plikter. Den må holde seg innenfor databehandleravtalen eller tilsvarende rettslig bindende dokument den inngår med behandlingsansvarlig; den må sørge for å inngå tilsvarende avtaler med underdatabehandlere, og den må sikre personopplysningenes med hensyn til konfidensialitet, tilgjengelighet og integritet.

Vi bruker ikke mer tid på dette nå. Vi trenger heller ikke gå inn på rolleavklaring, det vil si identifisere hvem bestemmer over formål og midler, hvem behandler personopplysninger på vegne av hvem. I det følgende vil det drøftes hvorfor ulike offentlige statlige myndigheter

i Norge ikke kan opptre som databehandlere overfor hverandre, og at databehandleravtaler innad i Staten ikke oppfyller de EØS-rettslige forpliktelsene gitt i personvernforordningen. Med andre ord, offentlige myndigheter under staten, kan ikke opptre som databehandlere for hverandre.

3. Begrepene databehandler og behandlingsansvarlig

Først om jussen. Forordningen fastsetter i artikkel 4.7 hvem som kan være behandlingsansvarlig. Dette er «*en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ*…» Dernest, i artikkel 4.8, hvem som kan være databehandler. En «*databehandler*» [kan være] *en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige*».

En ordlydskonform og sammenhengende tolkning av disse to begrepene kan tilsi at en offentlig myndighet (databehandler) kan opptre på vegne av en annen offentlig myndighet (behandlingsansvarlig). Denne slutningen er likevel ikke riktig for offentlige myndigheter som inngår i samme rettssubjekt. Vilkåret om adskilte rettssubjekter fremgår av forarbeidene til personverndirektivet (se punkt. 4 under) veiledninger fra europeiske ekspertorganer (pkt. 5) og teorien (pkt. 6). Mer sentralt følger vilkåret av den rettslige forventingen i forordningen om at forholdet controller-processor må kontraheres mellom partene med bindende virkning (pkt. 7).

4. Forarbeider til personverndirektivet – om begrepene

EF-kommisjonens forslag til nytt direktiv av 13. september 1990 ga ikke en definisjon av «databehandler». Forslaget definerte kun «*controller of the file*». Denne var parten med kompetanse til å «*decide what will be the purpose of the file, which categories of personal data will be stored, which operations will be applied to them and which third parties may have access to them*».

Teksten henviste videre til «*data processing service bureaux*» uten noe mer detaljering. Spørsmålet om databehandlere ble ikke viet noe særlig oppmerksomhet. Det fremgikk likeledes av merknadene til forslag til artikkel 22 om «*processing on behalf of the controller of the file*» at databehandleren måtte være en «*third party*», i forhold til behandlingsansvarlig. En som behandlet «*on behalf of the controller of the file*». Databehandleren må være bundet av en «*kontrakt*».

Begrepet *processor* ble innført i 1993 etter parlamentets behandling av forslaget. I merknadene i teksten kunne nå man lese at en processor var en «*outside processor, a legally separate person acting on his behalf*».

5. Uttalelse fra artikkel 29-arbeidsgruppen og veiledning fra EDPB

Spesialorganer nedsatt etter hhv. personverndirektivet, artikkel 29, og personvernforordningen, artikkel 68, har kommet med en uttalelse og en veiledning om begrepene og rollene behandlingsansvarlig og databehandler. Disse dokumentene er viktige rettskilder for forståelsen av direktivet og forordningen. Disse organene er ekspertrådgivere overfor Kommisjonen og medlemslandene. EU-domstolen legger ofte stor vekt på disse uttalelsene og veiledningene.

I begge dokumenter understrekes det at databehandleren må være en annen juridisk person enn behandlingsansvarlig. I artikkel 29-arbeidsgruppens uttalelse av 16. september 2010 om begrepene behandlingsansvarlig og databehandler skrives følgende:

> *«Therefore, two basic conditions for qualifying as processor are on the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf.»*

I personvernrådets veiledning 07/2020 av 7. juli 2021 videreføres denne forståelsen, på side 25.

«*Two basic conditions for qualifying as processor are: a) being a separate entity in relation to the controller*…». Vilkåret "*legally*" er ikke nevnt. Det er imidlertid utvilsomt at vilkåret fortsatt gjelder.

Dette fremgår implisitt av følgende avsnitt:

> *«A separate entity means that the controller decides to delegate all or part of the processing activities to an external organisation. Within a group of companies, one company can be a processor to another company acting as controller, as both companies are separate entities. On the other hand, a department within a company cannot be a processor to another department within the same entity.»*

6. Teori

Vi kan heller finne noen akademiske uenigheter rundt vilkåret om at databehandlere må være forskjellige juridiske personer. Kuner, Bygrave mfl. skriver for eksempel i A commentary til GDPR en analyse av begrepet processor at «*a processor must be an entity that is legally separate from the controller. …At the same time, controllers may also undertake processing operations themselves, in which case there is no separate legal subject (i.e. processor) involved with regard to those specific operations.*» McGillivray, i Government Cloud Procurement, side 111, skriver det samme.

Kontraktskravet i regelverket forutsetter likeledes eksistensen av to ulike rettssubjekter.

7. Rettslig bindende avtale

Det følger av artikkel 28 nr. 3 første punktum i personvernforordningen at «*[b]ehandling utført av en databehandler skal være underlagt en avtale eller et annet rettslig dokument i henhold til unionsretten eller medlemsstatenes nasjonale rett som er bindende for databehandleren med hensyn til den behandlingsansvarlige*».

En databehandleravtale må dermed være **rettslig bindende mellom partene**, databehandleren og behandlingsansvarlig, for å være i samsvar med forordningen.

Bestemmelsen definerer riktignok ikke hva som kan utgjøre en avtale etter forordningen. Avtalen må i det minste oppgi gjenstand, formål, varighet, og art med behandlingen, typer personopplysninger og kategorier av registrerte. I tillegg må det fremgå hvilke rettigheter og plikter behandlingsansvarlig har. Alle elementene i bestemmelsens andre ledd, eks. taushetsplikt, sikkerhetstiltak, bistandsplikt, mv. må reguleres i tillegg. Forordningen fastsetter imidlertid neppe noen gyldighetsvilkår. En er i stedet henvist til EU-retten eller nasjonalrettens regler for å fastslå avtalens gyldighet, herunder avtalens bindende karakter mellom partene.

EUs regelverk regulerer i liten grad rettslige forhold slik som kontraktens gyldighet. Det finnes enkelte kontraktsbegreper i forbrukerlovgivning, offentlige anskaffelser, og konkurranseretten. Rettsforholdet er primært nasjonalt anliggende, jf. subsidiaritetsprinsippet mellom landene og EU-organene. Hva som er en bindende avtale, vil dermed først og fremst bero på en tolkning av nasjonal kontraktsrett (pkt. 8 under) i de ulike EØS-landene.

8. Hva sier avtaleretten i Norge og andre europeiske land?

Norsk avtalelov har ingen legal definisjon av hva en rettslig bindende avtale er.

I juridisk litteratur, legger Woxholth i «Avtalerett» til grunn at: «*en rettslig bindende avtale foreligger først når to eller flere parter er blitt enige om å stifte eller endre et rettsforhold seg imellom, herunder at rettsforholdet bringes til opphør. Det som særpreger en rettslig bindende avtale, er at den kan gjennomføres ved domstolenes hjelp – enten ved at det avsies dom for at parten skal oppfylle avtalen.*»

På samme måte uttaler Selvig i «Kontraktsretten» at: «*kontrakten er rettslig bindende, betyr at de regler og krav til partenes handlemåte som kontrakten fastsetter, kan håndheves ved rettsapparatets hjelp overfor en part som ikke etterlever bestemmelsene frivillig*».

Rettstradisjonen i Frankrike og i andre europeiske land regulerer hva avtalene er, og hvilke vilkår som gjør dem gyldige. I common law forutsetter en avtales gyldighet at det foreligger tilbud og aksept mellom ulike parter, intensjon om å inngå avtalen, og «consideration». Tysk rett krever en utveksling av tilbud og aksept.

Det vil overgå alle våre ambisjoner med denne artikkelen å skulle gi en fullstendig fremstilling av vilkårene om avtalens rettslige bindende karakter i Europa. Vi legger til grunn her at fellesnevneren i den europeiske rettstradisjonen er at kontrakter forutsetter at det foreligger minst to forskjellige parter som frivillig forplikter seg til å yte noe overfor hverandre, eller til å endre og opphøre en ytelse. Det er altså ikke rettslig mulig å inngå avtaler med en selv.

Siden avtalebegrepet forekommer i personvernforordningen kan vi ikke utelukke at EU-domstolen blir forelagt tolkningsspørsmål om det, og at rettspraksis fra Luxembourg blir avgjørende. På området offentlige anskaffelser har EU-domstolen gitt viktige avklaringer om vilkårene som underligger kontraktsbegrepet (pkt. 9). Disse gir gode holdepunkter for vurdering av innholdet i en rettslig bindende avtale eller annet rettslig dokument – *kontraktsvilkåret* – etter artikkel 28.3 i personvernforordningen.

9. Hva sier rettspraksis fra anskaffelsesretten?

Rettspraksis innenfor anskaffelsesretten bør etter vår mening gis relevans ved tolkning av kontraktsvilkåret i personvernforordningen. Kontraktsvilkårets kjerne er den samme uavhengig rettsområdet, og anskaffelsesretten er tross alt et gren innenfor kontraktsretten.

Anskaffelsesreglene definerer offentlige kontrakter som «*gjensidig bebyrdende kontrakter* …», jf. definisjonen i anskaffelsesdirektivet artikkel 2. 5. En databehandleravtale etter personvernforordningen er også «*gjensidig bebyrdende*». Det er ikke en ensidig erklæring fra behandlingsansvarlig. Dette kan også utledes av forutsetningen om at behandlingsansvarlig foretar et «valg» av databehandler. En den frivillig knytter seg til som medhjelper for behandlingsaktivitetene sine.

EU-domstolen har uttalt at det gjensidige bebyrdende elementet i den offentlige kontrakten kjennetegnes ved at det medfører kontraktsforpliktelser for to eller flere parter som kan begjæres oppfylt med domstolenes hjelp, jf. sak C-367/19, avsnitt 26.

> *«….the fact remains that the reciprocal nature of a public contract necessarily results in the creation of legally binding obligations on both parties to the contract, the performance of which must be legally enforceable…»*

I *Helmut Müller,* sak C 451/08, EU:C:2010:168, avsnitt 62, ble dette uttrykt enda tydeligere.

> *«Since the obligations under the contract are legally binding, their execution must be legally enforceable. In the absence of rules provided for under European Union law, and in accordance with the principle of procedural autonomy, the detailed rules governing implementation of those obligations are a matter for national law.»*

EU-domstolen har videre uttalt at en offentlig kontrakt må inngås mellom separate rettssubjekter. I Stadt Halle, C-26/03, avsnitt 47 uttales følgende:

> *«In the spirit of opening up public contracts to the widest possible competition, as the Community rules intend, the Court has held, … that that directive is applicable in the case where a contracting*

authority plans to conclude a contract for pecuniary interest with an entity which is legally distinct from it, whether or not that entity is itself a contracting authority..»

I nyere rettspraksis fremgår dette vilkåret av EU-domstolens dom i Comune di Lerici, sak C 719/20, avsnitt 33.

Andre rettskilder innen det samme fagområdet støtter opp under hovedtesen i denne artikkelen om at databehandleravtaler forutsetter minst to atskilte rettssubjekter (pkt. 10).

10. Veiledning fra NHD og ESA

I gjeldende veiledning fra Nærings- og handelsdepartementet om offentlige kontrakter står det, i samsvar med argumentasjonen som er fremført foran, følgende:

«For at det skal foreligge en kontrakt i anskaffelsesregelverkets forstand må avtalen være inngått mellom to selvstendig rettssubjekter. Det betyr for eksempel at en avtale mellom to statlige direktorater ikke er en gjensidig bebyrdende kontrakt i dette regelverkets forstand, da begge er en del av staten og anses som del av samme rettssubjekt.»

I ESAs avgjørelse av 25 september 2002 med referanse 170/02/COL i en klagesak som gjaldt ytelser fra Statens vegvesen til Kystverket, var ESA enig i statens anførsler. Organet konkluderte med at

«…The Government of Norway stated that Norway considered that since central government and its ministries constituted a single legal entity, they must be perceived as a single contracting authority, Whereas the Authority has found no grounds to question that statement…»

og videre at

«Whereas examination by the Authority of the justifications put forward by Norway leads to the conclusion that the aforementioned Acts [anskaffelsesdirektivene] do not apply to situations where one ministry, or its subsidiary department, performs a service or supplies goods for another ministry, or its subsidiary department, as they must be considered to be part of the «State».

Resonnementet er ikke vanskelig å følge. Dette må også gjelde tilsvarende for avtaler mellom en databehandler og en behandlingsansvarlig. Vi ser nå på hovedspørsmålet – hypotesen – i saken (pkt. 11).

11. Kan et statlig direktorat være databehandler for et departement?

Statlige organer kan, så lenge de deler på den samme juridiske person, verken opptre som databehandlere for hverandre eller inngå rettslig bindende avtaler i tråd med artikkel 28. nr. 3.

Staten opptrer rettslig i de aller fleste sammenhengene som én juridisk person.

«Staten er én og samme part selv om søksmål rettes mot ulike departementer. En dom for et erstatningskrav mot staten ved Justis- og beredskapsdepartementet er for eksempel til hinder for at samme krav reises mot staten ved Finansdepartementet», Tore Schei mfl., Tvisteloven. Lovkommentar, i merknader til partsevne.

Søksmål mot staten anlegges mot staten ved vedkommende departement. Det er ikke departementet som får partsstilling, men det konkretiserer hvem som er statens representant i saken, jf. Ot.prp. nr. 51 (2004-2005), side 368.

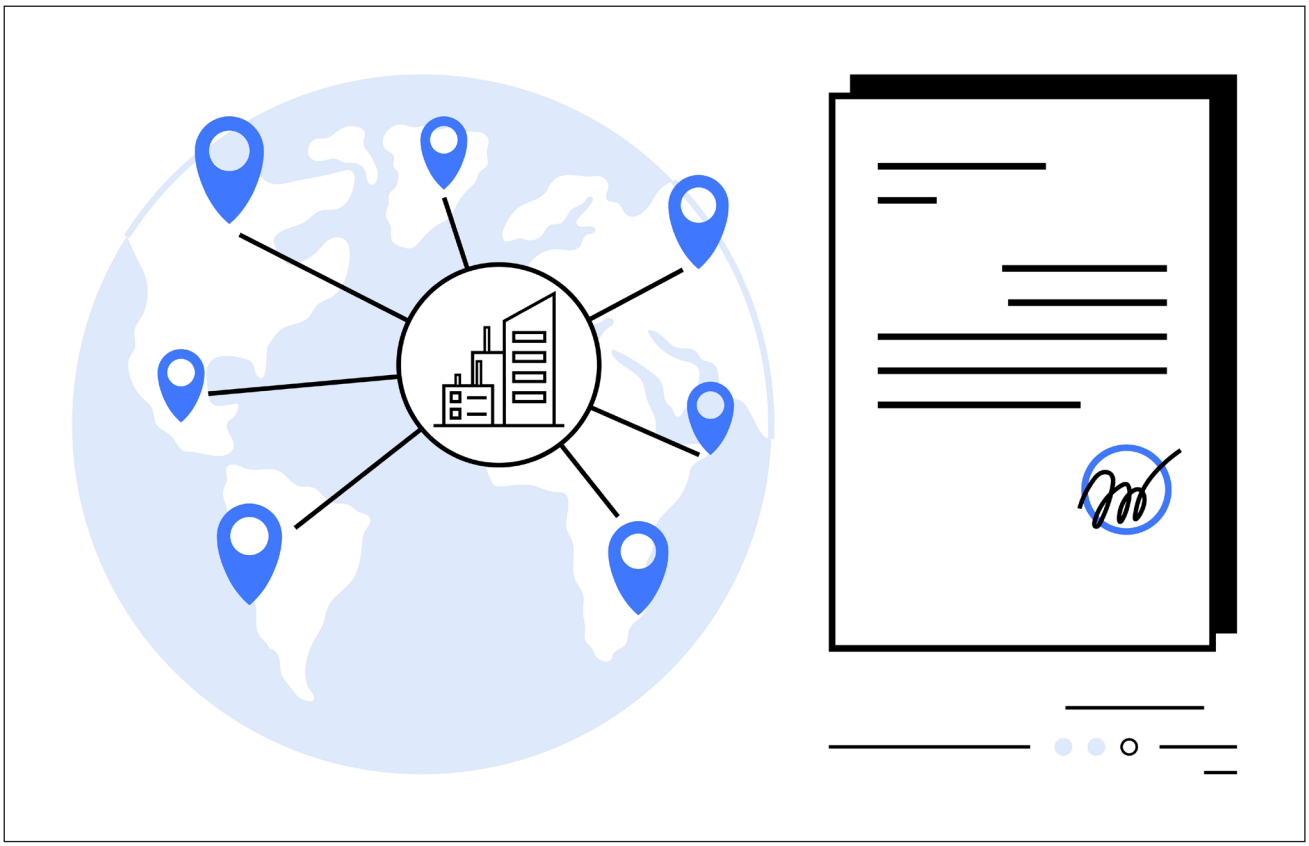
Skoghøy, tvisteløsning, skriver at «*… Under tvistemålsloven av 1915 hadde virksomheter som ble drevet av staten eller av en kommune eller fylkeskommune, bare alminnelig partsevne dersom virksomheten var organisert som selvstendig rettssubjekt, eller det ved særskilt lovbestemmelse var fastsatt at virksomheten hadde partsevne.» og «I den utstrekning dette ikke var tilfellet, måtte saken anlegges av eller mot staten eller den kommune eller fylkeskommune som hadde organisert virksomheten.»*

Det er altså klart at staten opererer som én juridisk person, et selvstendig rettssubjekt, og at staten ikke kan anlegge sak mot seg selv, med mindre det følger av særskilt lovbestemmelse at adgangen foreligger. Dette betyr jo, for det som interesserer denne fremstillingen, at ulike statlige forvaltningsorganer bare har én og samme juridisk person, og ergo mangler evnen til å opptre som databehandlere for hverandre, eller til å inngå bindende avtaler som ikke kan håndheves av domstolene.

12. Anbefaling og rettslige konsekvenser

Vi har konkludert med at statlige organer, enten i hierarkiske eller horisontale linjer, ikke kan opptre som databehandlere fordi de er samme juridisk person. Anbefalingen blir følgelig at i stedet for at det inngås unyttige databehandleravtaler, fastsettes skriftlige instrukser eller retningslinjer mellom de ulike forvaltningsorganene som påviser for den registrerte og tilsynsmyndighetene at de tar ansvaret for personopplysningene på alvor. En risiko ved å la inngåtte databehandleravtaler stå er at to forskjellige forvaltningsorganer kan gis overtredelsesgebyr for samme brudd på behandling av personopplysninger etter personopplysningsloven § 26. Det ene forvaltningsorganet i egenskap av behandlingsansvarlig og det andre som databehandler.

Det kan anføres at det følger av argumentasjonen foran at flere forvaltningsorganer i staten også opptrer som én behandlingsansvarlig. Det finnes likevel gode holdepunkter i personvernforordningen, jf. artikkel 4.7 for å fastholde at forvaltningsorganene i tilfellet anses som «offentlig myndighet» i begrepets forstand uten at det stilles vilkår om å være egne rettssubjekter. Alternativet ville medført konsekvenser for muligheten til å ha ordninger om felles behandlingsansvar innad i staten.



Illustrasjon: Colourbox.com

Relasjonen mellom behandlingsansvarlige forvaltningsorganer er ulik forholdet databehandler–behandlingsansvarlig. Det er blant annet ikke krav om inngåelse av *rettslig bindende avtaler* mellom behandlingsansvarlige etter art. 26 i personvernforordningen for behandling av personopplysninger i felleskap. Det foreligger dessuten en bred oppfatning om at ulike statlige forvaltningsorganer kan opptre som selvstendig behandlingsansvarlige selv om de tilhører samme rettssubjekt.

Kravet om egen juridisk person overfor behandlingsansvarlig ville medført vanskelige sjongleringsøvelser ved ileggelse av overtredelsesgebyr når flere behandlingsansvarlige i realiteten operer under samme hatt. Er staten ved departement X og staten ved direktorat Y som blir ilagt overtredelsesgebyr eller bare staten? Gebyrer blir uansett i neste sving innkrevd samlet av staten ved Statens innkrevingssentral.

> Det som er viktig er å fastlegge hvem som bærer ansvaret for behandlingsaktivitetene, for en etterfølgende vurdering av hvorvidt gjennomføring av ansvaret oppfyller fastsatte rettslige normer.

Vi velger å parkere diskusjonen her. Påstanden om at en offentlig myndighet, som selvstendig behandlingsansvarlig måtte ha egen rettslig handleevne, adskilt fra handleevnen til andre behandlingsansvarlige offentlige myndigheter ville kollidert med regulering av behandlingsansvaret i utallige lover og forskrifter.

For den registrerte (the Good) i denne historien er det uten betydning om databehandleravtaler inngått mellom forskjellige forvaltningsorganer i staten anses som nulliteter. Det som er viktig er å fastlegge hvem som bærer ansvaret for behandlingsaktivitetene, for en etterfølgende vurdering av hvorvidt gjennomføring av ansvaret oppfyller fastsatte rettslige normer. Den gode kan håndheve sin rett til personvern mot staten uansett.

Jaime Espantaleón er jurist, og har jobbet med personvern, avtalerett og EØS-rett i mange år i privat virksomhet og i offentlig forvaltning. Artikkelen er kun uttrykk for mine personlige ytringer.

Forsvarlig bruk av kunstig intelligens i pasientjournaler – løfter og hallusinasjoner

Av Julia Brodshaug og Lars Kristian Morka

KI-verktøy som Noteless og Medbric, er allerede tatt i bruk av over to tusen helseaktører i Norge i dag[1]. De kan bidra til mer utfyllende og nyanserte journalnotater, redusere arbeidsmengden til helsepersonell ved å generere utkast til svar, og fungere som beslutningsstøtte for å velge optimal behandling for den enkelte pasient[2]. For pasienter kan dette bety raskere og mer informert helsehjelp[3, 4, 5]. Samtidig innebærer teknologien en betydelig risiko. Feil bruk av journalføringsverktøy med KI, mangelfull utvikling og system-hallusineringer, kan true pasientsikkerheten og svekke tilliten til helsetjenesten. Spørsmålet blir hvordan en slik risiko skal defineres og reguleres rettslig, blant annet i lys av AI Act og GDPR.

Julia Brodshaug

Lars Kristian Morka

> Feil bruk av journalføringsverktøy med KI, mangelfull utvikling og system-hallusineringer, kan true pasientsikkerheten og svekke tilliten til helsetjenesten.

Forsvarlighetskravet innen norsk rett stiller strenge krav til helsehjelpen som gis, og hvordan pasientinformasjon skal håndteres, jf. blant annet helsepersonelloven § 4. Kravet er dynamisk, og regnes som en rettslig standard, jf. Ot.prp. nr. 13 (1998–99) på side 216. Bruk av kunstig intelligens i helsehjelp, herunder bruk av KI i journalføring, vil derfor være underlagt dette kravet. Videre vil en slik bruk av kunstig intelligens underlegges en rekke annen lovgivning, blant annet EUs forordning om kunstig intelligens (AI Act) og GDPR (personvernforordningen). Videre følger det en rekke krav til pasientjournalen gjennom pasientjournalloven.

Hvilken risiko utgjør kunstig intelligens i journalføring for pasientens helse?

AI act ble endelig vedtatt av EU i fjor sommer, og er det første enhetlige regelverket som regulerer bruken og utviklingen av kunstig intelligens[6]. Regelverket blir innført i norsk rett, og har dermed stor be-

1 Medbrick. (u.å.). Hos oss har helsepersonell første og siste ord [Om oss]. Medbrick. Lest august 2025, fra *https://www.medbrick.no/om-oss*.

2 Helsedirektoratet. (2025). Report on large language models in Norwegian health and care services: Risks and adaptations to Norwegian conditions. Helsedirektoratet. Lest august 2025, fra *https://www.helsedirektoratet.no/rapporter*.

3 Johansson, C. U. (2025). Fastlegen om bruk av kunstig intelligens: – Fått mer tid til å puste. Tidsskrift for Den norske legeforening, 145(4). *https://doi.org/10.4045/tidsskr.25.0138*.

4 Ayers, J. W., Poliak, A., Dredze, M., Smith, M. E., Chase, H. S., McCoy, J. P., … & Ramamani, R. (2023). Comparing physician and artificial intelligence chatbot responses to patient questions posted to a public social media forum. JAMA Internal Medicine, 183(6), 589–596. *https://doi.org/10.1001/jamainternmed*.

5 3. Tai-Seale, M., Baxter, S. L., Vaida, F., Walker, A., Sitapati, A. M., Osborne, C., Diaz, J., Desai, N., Webb, S., Polston, G., Helsten, T., Gross, E., Thackaberry, J., Mandvi, A., Lillie, D., Li, S., Gin, G., Achar, S., Hofflich, H., Sharp, C., Millen, M., & Longhurst, C. A. (2024). AI-Generated Draft Replies Integrated Into Health Records and Physicians' Electronic Communication. *JAMA Network Open, 7*(4):e246565. *doi:10.1001/jamanetworkopen.2024.6565*.

6 European Parliament. (2023). EU AI Act: first regulation on artificial intelligence [Nettside]. European Parliament. Lest august 2025, fra *https://www.europarl.europa.eu/topics/eu-ai-act*.

tydning for hvordan bruk og utvikling av kunstig intelligens skal reguleres i Norge[7].

Artikkel 6 i AI Act kapittel 3, jf. vedlegg I og III, definerer høyrisikosystemer. Et høyrisikosystem vil blant annet være systemer som klassifiseres som medisinsk utstyr etter AI Act vedlegg I, jf. AI Act artikkel 6 (1). Videre vil KI-systemer som påvirker tilgangen til ulike former for helsehjelp i utgangspunktet defineres som høy risiko[8]. AI Act stiller omfattende krav til bruken av slike systemer. Blant annet må systemene brukes i tråd med sin tiltenkte funksjon, overvåkes kontinuerlig i klinisk bruk, og være preget av åpenhet om virkemåte og begrensninger[9]. Slike krav kan bremse utviklingen av KI i helsehjelp, men kan samtidig bidra til å sikre at teknologien anvendes i samsvar med det som er forsvarlig. Det vil derfor ha stor betydning for implementeringen av KI i journalføring, samt pasientsikkerheten, hvor stor risiko slike systemer innebærer.

Det rettslige utgangspunktet er at et notetakingssystem med KI i generell forstand ikke er et høyrisikosystem etter AI-act eller regnes som medisinsk utstyr[10]. Spesielt bekymringsfullt er det imidlertid hvis et slikt KI-verktøy også anbefaler diagnosekoder eller bidrar til beslutninger i helsehjelp uten tilstrekkelig regulering. Bruk av et slikt system til å føre pasientjournal, kan innebære en betydelig større risiko for alvorlige konsekvenser.

Verktøy på markedet i dag, som blant annet Stenoly, foretar automatisk risikovurdering, forslag til differensialdiagnoser og intelligent sammenfatning av pasienthistorikk. Videre skriver selskapet på sine egne hjemmesider at deres verktøy gir detaljerte medisinske anbefalinger[11]. Dette vil potensielt kunne påvirke pasientbehandlingen i stor grad, og dermed også utgjøre en betydelig risiko for den enkelte pasient.

> Det rettslige utgangspunktet er at et notetakingssystem med KI i generell forstand ikke er et høyrisikosystem etter AI-act eller regnes som medisinsk utstyr.

Videre vil store språkmodeller (LLM-er) brukt i journalføring generelt ta med seg risikoen for hallusinasjoner, «svart boks» problematikk og transkriberingsfeil. Hallusinasjoner oppstår når KI feiltolker dataene den mates med, eller når den møter uventede mønstre eller endringer, for eksempel ved overtrening på spesifikke datasett[12]. Dette er ikke bare «misforståelser»: KI kan fabrikkere nytt innhold som ikke er sagt. En studie av OpenAIs tale-til-tekst-modell Whisper viste at omtrent én prosent av transkripsjoner inneholdt hallusinerte setninger[13]. Hallusinasjoner, transkriberingsfeil og lignende feil, kan gjøre at KI modeller forverres over tid – et fenomen kalt «drift»[14], som er til stede i prediktive modeller. Dette kan utgjøre en betydelig risiko for den enkelte pasient.

I tillegg karakteriseres store språkmodeller ofte som «svarte bokser», ettersom verken sluttbrukere eller utviklere kan redegjøre fullt ut for hvordan en spesifikk respons blir generert. Den begrensede graden av transparens, forklarbarhet og tolkbarhet innebærer at «svart boks» problematikken fremstår som en grunnleggende utfordring knyttet til anvendelsen av slike modeller[15].

Samtidig kan man på den andre siden fremheve at ingen verktøy er helt uten risiko, og at bruk innen helse ikke i seg selv alltid vil føre til at et verktøy med KI må reguleres som et høyrisikosystem[16]. Det følger blant annet et unntak av AI Act kapittel 3 artikkel 6 (3). Unntaket sier at selv der et KI-system i utgangspunktet kunne blitt regnet som et høyrisikosystem etter vedlegg III, så gjelder ikke dette der blant annet systemet ikke utgjør en betydelig risiko for skade på helse, sikkerhet eller grunnleggende rettigheter til fysiske personer, inkludert ved å ikke vesentlig påvirke utfallet av beslutningstaking. Det

7 Regjeringen. (2024). Forordning om kunstig intelligens (KI-forordningen) [Nettside]. Regjeringen. Lest juli 2025, fra *https://www.regjeringen.no/ki-forordningen.*

8 Artificial Intelligence Act (Regulation (EU) 2024/1689), Official Journal version of 13 June 2024, chapter III, article 6 (2) Annex III (5).

9 Artificial Intelligence Act (Regulation (EU) 2024/1689), Official Journal version of 13 June 2024, chapter III section 2.

10 Artificial Intelligence Act (Regulation (EU) 2024/1689), Official Journal version of 13 June 2024, chapter III.

11 Stenoly, «En komplett løsning for moderne helsevesen», 2025, *Løsninger for medisinsk journalføring - Stenoly (lest august 2025).*

12 Helsedirektoratet. (2025). Risks in large language models [Nettside]. Helsedirektoratet. Lest august 2025, fra *https://www.helsedirektoratet.no/risks-in-large-language-models.*

13 FAccT '24. (2024). Careless Whisper: Speech-to-Text Hallucination Harms. I Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (s. 1672–1681). *https://doi.org/10.1145/3630106.3658996.*

14 Bayram, A., & Kassler. (2022). From concept drift to model degradation: An overview on performance-aware drift detectors. Knowledge-Based Systems. *https://doi.org/10.1016/j.knosys.2022.108632.*

15 U.S. Department of Commerce. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0). https://doi.org/10.6028/NIST.AI.100-1.*

16 Artificial Intelligence Act (Regulation (EU) 2024/1689), Official Journal version of 13 June 2024, chapter III.

følger videre av bestemmelsen at dette kan være tilfellet der blant annet KI-systemer er ment til å forbedre en allerede fullført menneskelig handling[17]. Det samme gjelder der KI-systemet skal gjøre en forberedende oppgave til en vurdering[18], eller der KI-systemet er ment å utføre en avgrenset prosedyremessig oppgave[19]. Unntakene gjelder ikke ved profilering, jf. AI Act kapittel 3 artikkel 6 (3) siste ledd.

Sammenfatningsvis vil vi derfor fremheve at selv om journalverktøy med KI kan innebære fordeler for pasienten, så innebærer det også potensielt en høy risiko som må reguleres deretter, jf. AI Act og norsk helselovgivning for øvrig.

Hvilken risiko utgjør KI i jounalføring for pasientens personvern?

I tillegg til å kunne innebære en høy risiko for den enkelte pasient sin helsehjelp, kan bruk av journalføringsverktøy med KI utgjøre en risiko for den enkelte pasient sitt personvern etter personvernforordningen (GDPR), jf. personopplysningsloven og pasientjournalloven.

Det følger av pasientjournalloven § 1 at selve formålet med loven er todelt og fremhever at behandlingen av den enkelte pasient sine helseopplysninger skal skje på en forsvarlig og effektiv måte, samtidig som pasientens personvern og øvrige rettigheter er ivaretatt. Bestemmelsen viser at regelverket må tolkes i lys av både personvernregelverket og grunnleggende prinsipper i helselovgivningen for øvrig[20].

GDPR er en risikobasert rettsakt, i likhet med AI Act. Dette innebærer at det er risikoen ved et system som avgjør hvor mange krav det underlegges.

Det følger av GDPR artikkel 9 at helseopplysninger er en særlig kategori av personopplysninger som det i utgangspunktet er forbudt å behandle, med mindre et av behandlingsgrunnlagene i artikkelens punkt to kommer til anvendelse (eksempelvis uttrykkelig samtykke). Journalverktøy med KI som behandler slike opplysninger, vil derfor som utgangspunkt innebære høy risiko etter GDPR, og reguleres deretter.

> Der journalverktøy med KI påvirker avgjørelser i et behandlingsforløp i betydelig grad, basert på utilsiktede prediksjoner som bygger på en person sine personlige forhold, kan det oppstå en profilering eller lignende som i utgangspunktet er forbudt.

Videre følger det av GDPR artikkel 22 at den «registrerte» ikke kan utsettes for en «avgjørelse» som «utelukkende er basert på automatisert behandling» som videre har «rettsvirkning» eller lignende som i «betydelig grad» påvirker vedkommende[21]. Der journalverktøy med KI påvirker avgjørelser i et behandlingsforløp i betydelig grad, basert på utilsiktede prediksjoner som bygger på en person sine personlige forhold, kan det oppstå en profilering eller lignende som i utgangspunktet er forbudt. KI-modeller kan nemlig oppnå høy nøyaktighet på treningsdata, men mislykkes i å lære de egentlige mønstrene, og i stedet basere seg på tilfeldige korrelasjoner eller utilsiktede snarveier fra selve dataene[22]. Dette kan i teorien påvirke avgjørelser om en enkelt pasient sin helse i betydelig grad, basert på tilfeldige korrelasjoner, som kjønn, alder, religion og lignende.

Selv om et journalverktøy med KI kan være ment som en beslutningsstøtte og skal ses over av egnet helsepersonell, er det nemlig et kjent psykologisk fenomen at mennesker kan ha «overdreven tiltro til maskiner»[23]. Dette innebærer at dersom ulike helseaktører oppfatter AI-systemet som svært nyttig, og det samtidig gir tilsynelatende hjelpsomme (eller «behagelige») forklaringer, kan de bli enda mer tilbøyelige til å stole ukritisk på det, noe som kan føre til vurderingsfeil[24]. Dette er avgjørelser som i stor grad kan påvirke livet til den enkelte pasient. Forskning på «tankeløs etterlevelse» viser at mennesker ganske ubevisst eller automatisk stoler på informasjon som blir gitt, der-

17 Artificial Intelligence Act (Regulation (EU) 2024/1689), Official Journal version of 13 June 2024, chapter III article 6 (3) b.

18 Artificial Intelligence Act (Regulation (EU) 2024/1689), Official Journal version of 13 June 2024, chapter III article 6 (3) d.

19 Artificial Intelligence Act (Regulation (EU) 2024/1689), Official Journal version of 13 June 2024, chapter III article 6 (3) a.

20 Stubø, Marit, «Karnov lovkommentar: pasientjournalloven», Lovdata Pro, 2023, § 1 (lest juli 2025).

21 General Data Protection (Regulation (EU) 2016/679), Official Journal version of 27 April 2016.

22 General Data Protection (Regulation (EU) 2016/679), Official Journal version of 27 April 2016 artikkel 22 (2).

23 Klingbeil, A., Grützner, C., & Schreck, P. (2024). Trust and reliance on AI — An experimental study on the extent and costs of overreliance on AI. Computers in Human Behavior. *https://doi.org/10.1016/j.chb.2024.108352*

24 Harbarth, L., Gößwein, E., Bodemer, D., & Schnaubert, L. (2025). (Over) Trusting AI recommendations: How system and person variables affect dimensions of complacency. Interacting with Computers, 41(1), 391–410. *https://doi.org/10.1080/10447318.2023.2301250.*

som den virker tilstrekkelig plausibel[25]. På lignende måte bekrefter Anaraky et al. 2020[26] disse funnene ved å vise at deltakere følger systemets første forslag uavhengig av innholdet i de medfølgende begrunnelsene, selv da de medfølgende begrunnelsene gikk imot det første forslaget.

På den andre siden, kan man argumentere for at beslutningsstøtteverktøy innen helse på generelt grunnlag vanskelig kan sies å ta en «avgjørelse». Følgelig vil en del slike verktøy som utgangspunkt falle utenfor ordlyden i GDPR artikkel 22. Videre foreligger det unntak fra forbudet, blant annet der det foreligger uttrykkelig samtykke[27]. Tematikken reiser imidlertid viktige spørsmål rundt risiko og hva som egentlig utgjør en «avgjørelse», og kan komme på spissen i et presset helsevesen hvor avgjørelser må tas raskt og journalen allerede har en nøkkelfunksjon.

Sammenfatningsvis vil vi til denne tematikken fremheve at kunstig intelligens i journalføring kan innebære en høy risiko for den enkelte pasient sitt personvern, og at teknologien dermed må underlegges strenge krav til forsvarlighet og regulering etter GDPR og norsk helselovgivning forøvrig.

Illustrasjon: Colourbox.com

Avsluttende bemerkninger

Den raske innføringen og bruken av kunstig intelligens i norsk helsevesen, spesielt i forbindelse med pasientjournaler og konsultasjoner, kan ha store fordeler. De kan bidra til å frigjøre mer tid og ressurser i et presset helsevesen, og bidra til mer utfyllende og detaljerte journalnotater. Når dette er sagt, innebærer også teknologien alvorlige fallgruver og risikoer. Både AI Act, GDPR og norske helselover stiller krav til forsvarlig behandling av både pasienters helse og deres helseopplysninger og vil sette rettslige skranker for både bruken og utviklingen av en slik teknologi i dag og i tiden som kommer. Denne artikkelen er ment som en kort innføring i bruken av KI i journalføring i dag, og som et utgangspunkt for rettslig diskusjon i tiden som kommer.

Julia Brodshaug – jurist i Helfo og Lars Kristian Morka, analytiker i Helfo.

25 Langer, E. J., Blank, A., & Chanowitz, B. (1978). The mindlessness of ostensibly thoughtful action: The role of «placebic» information in interpersonal interaction. *Journal of Personality and Social Psychology*, *36*(6), 635–642. *https://doi.org/10.1037/0022-3514.36.6.635*.

26 Anaraky, R. G., Knijnenburg, B. P., & Risius, M. (2020). Exacerbating mindless compliance: The danger of justifications during privacy decision making in the context of Facebook applications. *AIS Transactions on Human-Computer Interaction*, *12*(2), 70–95. *https://doi.org/10.17705/1thci.00129*.

27 General Data Protection (Regulation (EU) 2016/679), Official Journal version of 27 April 2016 artikkel 22 (2).

Kravet i AI Act om innføring av policy for å overholde opphavsrett mv.

Av Ove A. Vanebo og Mikkel Lassen Ellingsen

1. Innledning

1.1 Hva handler artikkelen om?

Bruk og utvikling av kunstig intelligens (heretter «KI») innebærer en stor risiko for å bryte regler som skal beskytte opphavsrett eller nærstående rettigheter. Eksempelvis vil det i mange tilfeller brukes opphavsrettslig vernet materiale for å utvikle (f.eks. for å trene) KI-systemer eller -modeller, og frembringelse av tekst eller bilder vil også ofte innebære at beskyttede verk benyttes i prosessen. Problemstillingen erkjennes i EUs forordning om kunstig intelligens[1] (heretter «AI Act») fortalepunkt 105:

> *«KI-modeller for allmenne formål, spesielt store generative KI-modeller, som er i stand til å generere tekst, bilder og annet innhold, skaper unike muligheter til nyskaping, men også utfordringer for kunstnere, forfattere og andre opphavere og for hvordan det kreative innholdet deres opprettes, distribueres, brukes og forbrukes. Utvikling og trening av slike modeller krever tilgang til store mengder tekst, bilder, video og andre data. Teknikker for tekst- og datautvinning kan brukes i stor utstrekning i denne sammenhengen til å innhente og analysere slikt innhold, som kan være beskyttet av opphavsrett og nærstående rettigheter.»*

Dersom materiale er beskyttet, oppstår følgende problem, jf. samme talepunkt: «*All bruk av opphavsrettsbeskyttet innhold krever tillatelse fra den berørte rettighetshaveren med mindre relevante opphavsrettslige unntak og begrensninger gjelder.*»

Ove A. Vanebo

Mikkel Lassen Ellingsen

En slik særlig relevant begrensning finnes i tekst- og datautvinningsunntakene i artikkel 3 og 4 i direktiv (EU) 2019/790 (heretter «DSM-direktivet»), der det åpnes for storskala automatisert tekst- og datautvinning («text and data -mining») av opphavsrettslig vernet materiale til bruk i trening av KI-modeller – med mindre rettighetshaver på tilstrekkelig vis har reservert seg mot dette (gjennom en såkalt «opt-out» eller «forbeholdelse av rettigheter» som det heter i den foreløpige norske oversettelsen av AI Act).

Selv om AI Act ikke direkte regulerer opphavsrettigheter, inneholder artikkel 53 forpliktelser for leverandører av «*KI-modeller for allmenne formål*». Slike KI-modeller (som på engelsk gjerne omtales som GPAIM – «general-purpose AI models») kjennetegnes særlig av «*allmenngyldigheten og evnen til å utføre et bredt spekter av særskilte oppgaver på en kompetent måte*», jf. fortalepunkt 97. Typiske eksempler er ulike former for språkmodeller.

> Selv om AI Act ikke direkte regulerer opphavsrettigheter, inneholder artikkel 53 forpliktelser for leverandører av «*KI-modeller for allmenne formål*».

For ordens skyld nevner vi at KI-*modeller* er noe annet enn KI-*systemer*. KI-modeller er enkelt sagt *algoritmer*, dvs. «oppskriftene» eller prosedyreinstruksene som brukes for at systemer skal løse bestemte oppgaver. Fortalepunkt 97 fastslår at: «*Selv om KI-modeller er sentrale komponenter i KI-systemer, utgjør de ikke KI-systemer i seg selv.*» Blant annet må KI-modeller «*tilføyes ytterligere komponenter, som for eksempel et brukergrensesnitt, for å bli KI-systemer.*» Det slås videre fast at «*KI-modeller er vanligvis integrert i og utgjør en del av KI-systemer.*»

1 EUs forordning om kunstig intelligens (AI Act, på norsk KI-forordningen), reg. EU/1684/2024.

For å ivareta opphavsrett mv., følger det av AI Act artikkel 53 nr. 1 bokstav c at «*Leverandører av KI-modeller for allmenne formål skal … innføre en framgangsmåte for å overholde unionsretten om opphavsrett og nærstående rettigheter, og særlig for å identifisere og etterleve, herunder ved hjelp av den nyeste teknologien, forbeholdelse av rettigheter i samsvar med artikkel 4 nr. 3 i direktiv (EU) 2019/790*».

Denne teksten utforsker og belyser hvem forpliktelsene gjelder, hva slik «fremgangsmåte» eller «policy» innebærer og hvordan forordningen skal etterleves i praksis.

1.2 Særlig om regler for god praksis

AI Act legger opp til at det kan lages regler for god praksis, *Codes of Practice*, for å etterleve kravene til å lage en policy. Reglene er et frivillig verktøy, som er utarbeidet av uavhengige eksperter i en prosess med et stort antall interessenter/stakeholders. EU-kommisjonen og styret for kunstig intelligens (AI Board) har bekreftet at slike Codes of Practice kan være et passende (frivillig) verktøy for leverandører av GPAI-modeller for å demonstrere/påvise samsvar med KI-loven.[2]

I denne sammenheng er det særlig hensiktsmessig å vise til en ny *Code of Practice for General-Purpose AI Models,* Copyright Chapter, som er utgitt av en egen arbeidsgruppe.[3] Vi vil under ta utgangspunkt i denne når vi beskriver hva en policy bør inneholde, og vil for enkelthetens skyld bare omtale den som *Code of Practice*. Det er i teorien antatt at hvis leverandører ikke etterlever en slik harmonisert Code of Practice, vil leverandøren selv bære risikoen for å vise at de har alternative, adekvate måter å overholde sine forpliktelser på.[4]

Vi gjør oppmerksom på at *Code of Practice s*elv påpeker at *«adherence to the Code does not constitute conclusive evidence of compliance with these obligations under the AI Act».*[5]

2. Hvem (og hvor) gjelder plikten til å innføre policy for?

Det er «leverandører» som er underlagt plikten om å innføre en policy. Ifølge KI-forordningens artikkel 3 nr. 3 er leverandører:

> *«en fysisk eller juridisk person, en offentlig myndighet, et byrå eller ethvert annet organ som utvikler et KI-system eller en KI-modell for allmenne formål, eller som får utviklet et KI-system eller en KI-modell for allmenne formål og bringer det eller den i omsetning eller tar KI-systemet i bruk under eget navn eller varemerke, mot betaling eller vederlagsfritt»*

Det er relativt greit å peke ut hvem som klart omfattes av definisjonen. I verdikjeden er det imidlertid ikke alltid opplagt hvem som anses som leverandører av KI-modeller.

Ulike «oppstrømsleverandører», som håndterer dataskraping, gjennomsøking og levering av opplæringsverktøy og datasett – men som ikke produserer selve modellen – vil normalt falle utenfor pliktene i artikkel 53.[6] «Nedstrømsleverandører» vil derimot oftere kunne omfattes, blant annet enkelte leverandører av KI-systemer. Når leverandøren av en KI-modell for allmenne formål integrerer en egen modell i *sitt* eget KI-system som gjøres tilgjengelig på markedet eller tas i bruk, bør denne modellen anses for å være brakt i omsetning, jf. fortalepunkt 97. Ifølge AI Act bør da forpliktelsene for modeller i forordningen fortsatt gjelde i *tillegg til f*orpliktelsene for KI-systemer.[7] Nedstrømsleverandører kan derfor omfattes av AI Acts forpliktelser for modelleverandører ved «vertikal integrasjon», der KI-modeller integreres i egne systemer som tilbys på markedet. KI-systemer som integrerer *andre leverandørers modeller* vil derimot i utgangspunktet falle utenfor forpliktelsene som er pålagt modellleverandører i henhold til artikkel 53.[8]

Hva gjelder *hvor* AI Act gjelder, dvs. *stedlig* virkeområde, følger det av artikkel 2 nr. 1 bokstav a at AI Act gjelder for «*leverandører som bringer i omsetning eller tar i bruk KI-systemer eller bringer KI-modeller for allmenne formål i omsetning i Unionen, uansett om disse leverandørene er etablert eller lokalisert i Unionen eller i et tredjeland*».

Fortalepunkt 106 fastslår for øvrig at:

> *«Enhver leverandør som bringer en KI-modell for allmenne formål i omsetning i Unionen, bør oppfylle denne forpliktelsen, uavhengig av i hvilken jurisdiksjon de opphavsrettslig relevante handlingene som ligger til grunn for treningen av disse KI-modellene, finner sted. Dette er nødvendig for å sikre like vilkår for leverandører av KI-modeller for allmenne formål, der ingen leverandør bør kunne oppnå et konkurransefortrinn på unionsmarkedet ved å anvende lavere opphavsrettsstandarder enn de som er fastsatt i Unionen.»*

Dersom man leser fortalepunktet bokstavelig, vil dette innebære at f.eks. en japansk leverandør av KI-modeller (som utvikler og trener modellen sin i Japan) blant annet må

2 AI Act artikkel 53 nr. 4. Se også EU-kommisjonen, The General-Purpose AI Code of Practice. Lest 6. september 2025: *https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai*

3 *https://ec.europa.eu/newsroom/dae/redirection/document/118115*

4 N. E. Vellinga og Jeanne Mifsud Bonnici, *Article 53 Obligations for Providers of General-Purpose AI Models*. I: Ceyhun Necati Pehlivan, Nikolaus Forg, Peggy Valcke, *The EU Artificial Intelligence (AI) Act : A Commentary*, 2024, s. 856.

5 Code of Practice, Objectives (punkt A)

6 João Pedro Quintais, *Copyright, the AI Act and Extraterritoriality*, The Lisbon Council, Policy brief, juni 2025, s. 8.

7 AI Act fortalepunkt 97.

8 Quintais 2025 s. 8.

respektere opt-out-mekanismen i DSM-direktivets artikkel 4 nr. 3 dersom leverandøren senere vil plassere modellen på EU-markedet.[9] I et slikt tilfelle vil ikke DSM-direktivets regulering anvendes direkte, men AI Act vil kreve at reguleringen respekteres gjennom policy-kravet. Denne løsningen er ikke ukontroversiell da den i så fall vil gjøre europeisk opphavsrett (indirekte) gjeldende med tilbakevirkende kraft, f.eks. for trening som i utgangspunktet er gjennomført lovlig i tredjeland.[10] Selv om dette kan virke fremmed fra et opphavsrettslig perspektiv, er det dog ikke helt ulikt hvordan f.eks. EUs produktansvarsregelverk fungerer.

Et mindre inngripende tolkningsalternativ er imidlertid at trening av den japanske KI-modellen (i Japan) ikke er omfattet av DSM-direktivet (eller europeisk opphavsrett for øvrig) i utgangspunktet, og at forpliktelsen i artikkel 53 nr. 1 bokstav c i AI Act dermed heller ikke kan begrense retten til senere å sette modellen på EU-markedet.[11] En slik tolkning synes vanskelig å forene med fortalepunkt 106, men er i større grad i tråd med tradisjonelle prinsipper om opphavsrettens territorielle anvendelsesområde.

Hvordan dette skal forstås og anvendes står igjen som et av mange krevende og ubesvarte spørsmål i AI Act.

3. Hva er en «fremgangsmåte»?

Den (foreløpige) norske oversettelsen av AI Act bruker uttrykket «fremgangsmåte». Trolig er det mer hensiktsmessig å ta utgangspunkt i den engelskspråklige utgaven, som benytter begrepet «policy». Dette er interessant nok også brukt i det norske høringsnotatet som gjelder gjennomføringen av AI Act i norsk rett, som påpeker at: «*Leverandører av KI-modeller for allmenne formål skal utarbeide en policy for etterlevelse av EU-regelverk om opphavsrett og nærstående rettigheter.*»[12] I høringsbrevet ber departementet uttrykkelig om innspill på «*Terminologi (legaldefinisjoner) brukt i den uoffisielle oversettelsen av KI-forordningen*», hvilket kan tyde på flere rent språklige utfordringer.

4. Finnes det egentlig noen «unionsrett» om opphavsrett?

AI Act presiserer ikke hva som utgjør «unionsretten om opphavsrett og nærstående rettigheter», og flere har påpekt at det strengt tatt ikke eksisterer noen omforent «europeisk opphavsrett».[13] Et tolkningsalternativ er å legge til grunn at alle EU-staters samlede lovgivning fra 27 land (pluss tre EØS-stater?) skal respekteres. En annen tilnærming er å ta utgangspunkt i EUs rettsakter som direkte gjelder opphavsrett. Det finnes imidlertid ikke et eget, samlet «opphavsrettsdirektiv», og det er ulike forståelser av hvilke forpliktelser som pålegges av ulike EU-direktiver. Det er med andre ord uklart hvilke rettigheter som skal respekteres, og det er ikke tydeliggjort om også nasjonale reguleringer knyttet til opphavsrett skal tas med i betraktning.[14]

I fortalepunkt 105 fremgår at:

> *«Ved direktiv (EU) 2019/790 ble det innført unntak og avgrensinger som tillater eksemplarframstillinger av og uttrekk fra verk eller andre arbeider for tekst- og datautvinningsformål på visse vilkår. I henhold til disse reglene kan rettighetshaverne velge å forbeholde seg rettighetene til sine verk eller andre vernede arbeider for å hindre tekst- og datautvinning, med mindre denne utvinningen gjøres med henblikk på vitenskapelig forskning. Dersom retten til unntak er blitt uttrykkelig forbeholdt på hensiktsmessig måte, må leverandører av KI-modeller for allmenne formål innhente tillatelse fra rettighetshaverne dersom de ønsker å utføre tekst- og datautvinning fra slike verk.»*

Videre påpeker fortalepunkt 106 at for overholdelse av rettigheter «*bør leverandører av KI-modeller for allmenne formål innføre en framgangsmåte for å overholde unionsretten om opphavsrett og nærstående rettigheter, særlig for å identifisere og etterleve rettighetshaveres forbeholdelse av rettigheter i samsvar med artikkel 4 nr. 3 i direktiv (EU) 2019/790.*»

Code of Practice viser til rettigheter *som er «provided for in directives addressed to Member States and that for present purposes Directive 2001/29/EC, Directive (EU) 2019/790 and Directive 2004/48/EC are the most relevant»,* jf. fortalen punkt (c)(i).

Ut fra rimelighetsgrunner antar vi at det er meningen at det er EU-retten som skal etterleves, og at særlige nasjonale bestemmelser vanskelig kan følges opp – og det gir liten mening med en forordning som skal ha en harmonisert regulering av markedsaktiviteter. Det må derfor forsøksvis utledes hva som følger av de aktuelle direktivene som inneholder bestemmelser om opphavsrett, særlig med henblikk på EU-domstolens praksis.

5. Hva slags innhold må policyen ha?

5.1 Innledende om innholdet

5.1.1 Generelt om policy-kravet

Kjernen i policy-kravet, er å utarbeide en policy, holde seg oppdatert og implementere en slik policy for overholdelse av opphavsrett mv. – og dette anses for å være et tiltak i seg selv etter Code of Practice.

AI Act inneholder imidlertid ingen formkrav eller krav til materielt innhold i en slik policy, så lenge den er egnet til å oppnå sitt formål («å overholde unionsretten om opphavsrett»). Av hensyn til notoritet (f. eks. i forbindelse med tilsyn) bør det kunne legges til grunn at policyens innhold i det minste bør være nedfelt skriftlig. *Code of Practice* oppfordrer

9 Alexander Peukert, *Copyright in the Artificial Intelligence Act - A Primer*, mars 2024, s. 18-19.
10 Quintais 2025 s. 19.
11 Peukert 2024 s. 18-19.
12 Høringsnotatet s. 26.
13 F.eks. Peukert 2024 s. 15.
14 Se redegjørelsen i Peukert 2024 s. 15 og 16.

videre aktørene til å offentliggjøre og holde oppdatert et sammendrag av sin opphavsrettspolicy, uten at dette fremstår som noe obligatorisk krav.[15]

Under vil vi særlig ta utgangspunkt i hva *Code of Practice* uttrykker om innholdet i, og etterlevelsen av, en slik policy.

5.1.2 Hva anses som «den nyeste teknologien»?

I artikkel 53 nr. 1 bokstav c heter det at polycien skal sørge for at man identifiserer og etterlever opt-outs «*ved hjelp av den nyeste teknologien*» (*«through state-of-the-art technologies»* i den engelske forordningsteksten).

Dette virker umiddelbart som et meget strengt og ubetinget krav om stadig å anskaffe og benytte den siste og beste teknologien på området. Overordnet følger det dog av Code of Practice at: «*The commitments in this Chapter that require proportionate measures should be commensurate and proportionate to the size of providers, taking due account of the interests of SMEs, including startups*».[16] Selv om proporsjonalitet ikke eksplisitt er nevnt i forbindelse med kravet om bruk av «den nyeste teknologien» taler gode grunner for at det må innfortolkes en viss proporsjonalitetsavveining også her.

Uttrykket brukes imidlertid i flere EU-rettsakter og betegner normalt den beste teknologien på markedet, sett i lys av den teknologiske utviklingen, i den forstand at den mest mulig effektivt oppnår formålet med bruken av teknologien.[17] Det er neppe noe krav om å benytte den absolutt nyeste eller eksperimentelle teknologien som er mer på forsøksstadiet, og langt unna å være «hyllevare». I juridisk teori er det antatt at følgende tilnærming fra annet EU-regelverk innebærer at «den nyeste teknologien» i AI Act:[18]

> *«should be understood as a developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experience and which is accepted as good practice in technology.»*

Samtidig vil det være begrensninger, ved at den «nyeste» teknologien «*does not necessarily imply the latest scientific research still in an experimental stage or with insufficient technological maturity*».

5.2 Innhente og reprodusere bare lovlig tilgjengelig materiale fra Internett

KI-modeller for allmenne formål må sikre at web-scraping (tekst- og datautvinning via såkalte «webcrawlere») begrenses til materiale som er lovlig tilgjengelig. At opphavsrettslig vernet materiale er lovlig tilgjengelig er et vilkår for at tekst og datautvinning skal kunne skje uten forutegående samtykke, iht. DSM-direktivet.[19] Hva som skal til for at noe er «lovlig tilgjengelig» kan by på vesentlig tvil, men vil ikke behandles i det videre her.[20]

Tiltaket innebærer for *det første* særlig å motvirke omgåelse av tekniske tiltak (f.eks. betalingsmurer) som begrenser tilgang, jf. art. 6(3) i direktiv (EU) 2001/29 («Infosoc-direktivet»). *For det annet* er det særlig viktig at leverandøren sørger for å filtrere bort nettsteder som vedvarende og kommersielt krenker opphavsrett, slik disse er identifisert av domstoler eller myndigheter i EU/EØS (typisk nettsider som tilbyr ulovlig strømming eller nedlasting av TV-serier, filmer og sportsarrangementer). En dynamisk EU-liste over slike nettsteder skal være tilgjengelig for å lette etterlevelsen.

5.3 Identifisere og etterleve rettighetsreservasjoner ved innhenting av data

I tiltak 1.3 fastsettes prosedyrer for å respektere forbehold (opt-outs) mot tekst- og datamining etter DSM-direktivet art. 4 nr. 3. Leverandørene må anvende nettroboter («web-crawlers») som leser og følger den såkalte Robots Exclusion Protocol (robots.txt), og må i tillegg identifisere og etterleve andre maskinlesbare standarder for å uttrykke forbehold (opt out) – for eksempel metadata – som er allment akseptert av rettighetshavere og teknisk gjennomførbare.

Tiltaket presiserer at rettighetshaverne står fritt til å gi sitt forbehold (opt out) på enhver «appropriate manner», og pålegger leverandørene å offentliggjøre informasjon om sine web-crawlers, herunder hvordan de identifiserer og respekterer forbehold, samt å tilby automatisk varsling av rettighetshavere når slik informasjon oppdateres.

---

15 Code of Practice, Measure 1.1, punkt (2)

16 Code of Practice, Recitals, punkt (d).

17 Se blant annet Sandra Schmitz-Berndt, *Conceptualising the Legal Notion of 'State of the Art' in the Context of IT Security*. Fra den 16. IFIP International Summer School on Privacy and Identity Management (Privacy and Identity), august 2021, Luxembourg, sidene 25-32.

18 Henvisning til *Annexes to the Commission Implementing Decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence* i David M. Schneeberger, Walter Hötzendorfer & Christof Tschohl, «Article 8; Compliance with the Requirements». I: Ceyhun Necati Pehlivan, Nikolaus Forg, Peggy Valcke, *The EU Artificial Intelligence (AI) Act : A Commentary*, 2024, s. 227.

19 Jf. DSM-direktivets artikkel 3 nr. 1 («lawful access») og 4 nr. 1 («lawfully accessible»)

20 Spørsmålet er behandlet godt i punkt 3.2 i «*Mens vi venter på noe godt*» av Antonsen og Oddbjørnsen: *https://lod.lovdata.no/article/2023/12/Mens%20vi%20venter%20p%C3%A5%20noe%20godt*

5.4 Risikoreduserende tiltak ved integrering i KI-systemer

Code of Practice anbefaler også tiltak for å redusere risikoen for at nedstrøms KI-systemer (der allmenngyldig KI-modell er integrert) genererer utdata som kan krenke rettigheter til verk eller annet materiale. To tiltak nevnes konkret:[21]

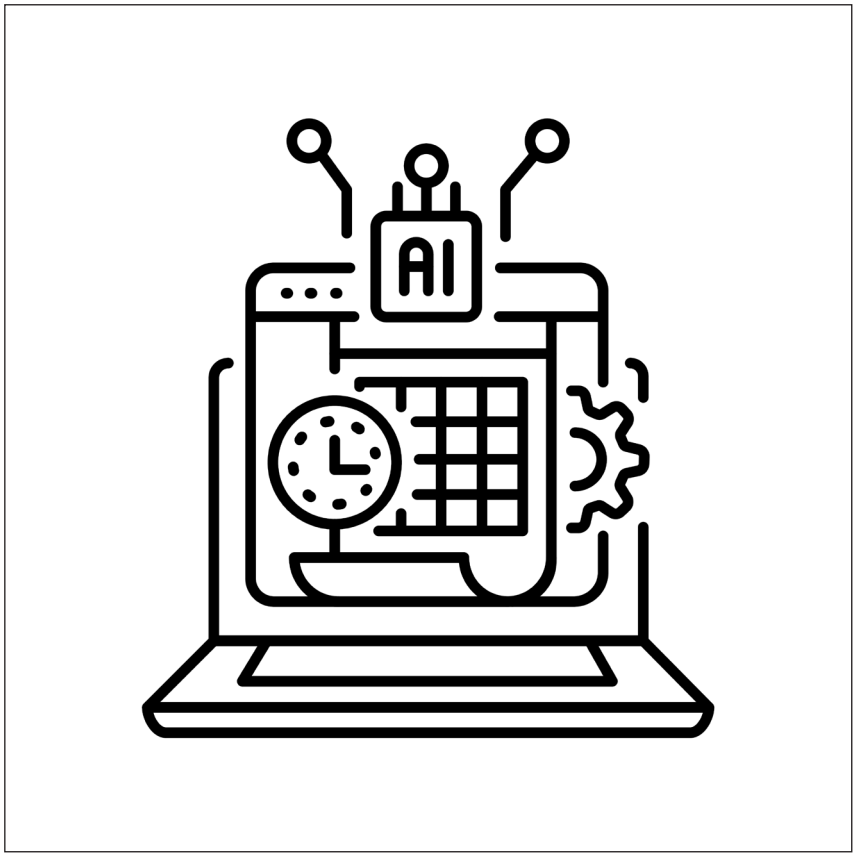
For det første; implementere passende og forholdsmessige tekniske sikkerhetstiltak for å forhindre at modellene deres genererer utdata som reproduserer vernet treningsdata. Slike sikkerhetsmekanismer benyttes i utstrakt grad av de største aktørene i dag og kommer f.eks. til syne hvis du ber ChatGPT generere et bilde av en velkjent superhelt-tegneseriefigur, men får til svar at «*This image generation request did not follow our content policy*». Det er imidlertid ingen åpenhet rundt hvordan slike tiltak fungerer teknisk, og det finnes mange eksempler på at de nokså enkelt kan omgås.

For det annet; forby opphavsrettsstridig bruk av en modell, og innta forbudet i sine retningslinjer for akseptabel bruk, vilkår og betingelser eller andre tilsvarende dokumenter. Dersom det leveres KI-modeller utgitt under frie og åpne kildekode-lisenser, skal leverandøren varsle brukere om forbudet mot opphavsrettsstridig bruk av modellen i dokumentasjonen som følger med modellen, uten at det berører lisensens frie og åpne kildekode-karakter.

Anbefalingene gjelder uavhengig av om en leverandør integrerer modellen i sine egne KI-systemer eller om modellen leveres til en annen virksomhet som ledd i et kommersielt forretningsforhold.[22]

5.5 Utpeke et kontaktpunkt og muliggjøre innlevering av klager

Ifølge *Code of Practice* bør det også utpekes et kontaktpunkt for elektronisk kommunikasjon for berørte rettighetshavere. Det må derfor etableres en mekanisme som gjør det mulig for berørte rettighetshavere (og deres autoriserte representanter, for eksempel kollektive forvaltningsorganisasjoner) å sende inn klager vedrørende manglende overholdelse av sine leverandørforpliktelser.



Illustrasjon: Colourbox.com

> Tiltakene som er anbefalt av Code of Practice påvirker for øvrig ikke tiltakene, rettsmidlene og sanksjonene som er tilgjengelige for å håndheve opphavsrett og beslektede rettigheter i henhold til ulike rettsregler.

Det bør videre gis lett tilgjengelig informasjon om ordningen. Trolig vil informasjon på nettsider være tilstrekkelig.

Leverandører må behandle klager på en samvittighetsfull og upartisk måte innen rimelig tid. Code of Practice åpner for unntak fra en omstendelig prosess hvis en klage er åpenbart grunnløs eller leverandøren allerede har svart på en identisk klage fra samme rettighetshaver.

Tiltakene som er anbefalt av Code of Practice påvirker for øvrig ikke tiltakene, rettsmidlene og sanksjonene som er tilgjengelige for å håndheve opphavsrett og beslektede rettigheter i henhold til ulike rettsregler.[23]

Ove A. Vanebo, assosiert partner og advokat i CMS Kluge Advokatfirma.

Mikkel Lassen Ellingsen, advokat spesialisert innenfor immaterialrett, teknologi og medie- og markedsføringsrett.

21 Code of Practice s. 6
22 Code of Practice s. 6
23 Code of Practice s. 6.

NIS2:
Personlig ansvar for ledelsen og ansatte

Del 3 i artikkelserien om cybersikkerhet og NIS2

Av Kristian Foss og Mira Levánd Bergsland

I denne tredje og siste artikkelen i vår serie om Network and Information System-direktivet («**NIS2**»), vil vi fokusere på hvilket personlig ansvar ledelsen og ansatte kan pådra seg dersom virksomheten de er involvert i ikke etterlever direktivet. NIS2 er enda ikke implementert i norsk rett, men minimums-direktivet danner likevel et gulv og byr på visse overraskelser.

Den største overraskelsen er kanskje NIS2s klare anvisning på at ansvaret for overtredelse av direktivets sikkerhetskrav skal være *personlig*. Overraskelse nummer to er retten tilsynsmyndighetene skal gis til å *fjerne ledelsen* midlertidig om andre av de tallrike sanksjonsmulighetene ikke virker godt nok. Retten til å nekte *virksomheten* å drive bør også nevnes i denne sammenhengen. I tillegg kommer det nå sedvanlige overtredelsesgebyret, på opptil minst 2 % av årsomsetningen.

> Den største overraskelsen er kanskje NIS2s klare anvisning på at ansvaret for overtredelse av direktivets sikkerhetskrav skal være *personlig*.

Bakgrunnen for denne uvanlige reguleringen er, ikke overraskende, økningen i cybertrusler og sårbarheten i et snart totalt oppkoblet samfunn. Slik verdenssituasjonen har utviklet seg, med fundamental usikkerhet også sikkerhetspolitisk

Kristian Foss

Mira Levánd Bergsland

– Russland, Ukraina, USA og Kina er stikkord – blir sikkerhet i digital infrastruktur nesten et eksistensialistisk spørsmål for et moderne samfunn.

Det personlige ansvaret NIS2 introduserer er imidlertid ikke alene om å pålegge enkeltpersoner et mulig økonomisk ansvar. Det vi i norsk rett omtaler som *styreansvaret*, men som i realiteten omfatter mange flere personer enn dem i styret, virker parallelt og i samvirke med NIS2. De norske ansvarsreglene er derfor nødvendig å behandle når det personlige ansvaret i NIS2 skal forklares.

Vi begynner med å redegjøre for ansvarsreglene og noen utvalgte sanksjoner i NIS2 (pkt. 1), før det såkalte styreansvaret etter aksjeloven (asl.) § 17-1 behandles (pkt. 2). Til slutt sier vi noen ord om årssakssammenheng (pkt. 3) og forholdet mellom NIS2 og styreansvaret i Norge (pkt. 4).

1. Ansvaret etter nis2

I dette punktet gir vi en oversikt over hvilke personer som kan bli ansvarlige, hvem som kan kreve erstatning, på hvilket grunnlag og for hvilke tap.

1.1 Hvilken personkrets kan bli personlig ansvarlige?

NIS2 art. 20 (1) leser:

> *«Member States shall ensure that the* ***management bodies*** *of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and* ***can be held liable*** *for infringements by the entities of that Article.*
>
> *The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of* ***public servants*** *and elected or appointed* ***officials****.»* [våre uthevinger]

1.1.1 Ledelsens ansvar – «management bodies»

Norge skal med andre ord sørge for at såkalte «management bodies» kan holdes ansvarlige for overtredelse av artikkel 21. Artikkel 21 gjelder mer eller mindre konkrete krav til sikkerhet, som omtalt i del 2 av vår artikkelserie: *NIS2: Hvilke konkrete sikkerhetskrav gjelder?*

Begrepet «management bodies» er ikke definert i NIS2. Rent språklig kan begrepet oversettes til «ledelsesorganer», noe som også brukes i den danske versjonen av NIS2. Begrepet gir imidlertid ikke mer veiledning ut over å åpne for at i det minste styrer og kanskje også daglige ledere kan bli holdt ansvarlige.

Ytterligere veiledning kan finnes i forarbeidene til lov om digital operasjonell motstandsdyktighet i finanssektoren (DORA), som trådte i kraft 1. juli i år. Med henvisning til DORA (forordningen), art. 3 (30) med referanser uttaler departementet:

> *«Departementet viste i høringsnotatet bl.a. til at foretakene etter forordningen artikkel 5 nr. 1 skal ha et overordnet rammeverk for IKT-risikostyring, og at rammeverket etter nr. 2 skal fastsettes, godkjennes og overvåkes av foretakets ledelsesorgan («management body» på engelsk), jf. også omtale i punkt 2.4.2.2. Ledelsesorganet er definert i forordningen artikkel 3 nr. 30 ved henvisninger til annet regelverk, hovedsakelig slik at det vises til* **organet som har ansvaret for å utarbeide foretakets strategi og overordnede mål og overvåke ledelsens beslutninger**. *Departementet bemerket at dette organet i norsk kontekst vil være styret.»* [våre uthevinger]
>
> (Prop. 54 LS (2024–2025) pkt. 2.5.4.1)

I pkt. 2.4.2.2 uttaler departementet:

> *«Enkelte plikter som pålegges «ledelsesorganet» etter DORA-forordningen er imidlertid av en slik art at de etter norsk rett vil falle inn under det som vanligvis er daglig leders plikter. Den nærmere grensedragningen mellom styret og daglig leder omtales i punkt 2.5.4.3. Her fremgår det at departementet mener at det ved eventuell uklarhet om hvilket selskapsorgan som skal anses som ansvarlig etter DORA-regelverket, påhviler styret i norske foretak å avklare ansvarsfordelingen mellom styret og daglig leder.»* [våre uthevinger]

Teksten i DORA-forordningen art. 3 (30), som proposisjonen viser til, lyder:

> *«or the equivalent persons who* ***effectively run the entity*** *or* ***have key functions*** *in accordance with relevant Union or national law;»* [våre uthevelser]

Det sentrale synes dermed å være hvilke personer som reelt sett utøver kontroll over virksomheten eller funksjonen, selv om det skulle være andre enn styret og daglig leder. Siden formålet med slike regelverk er å ansvarliggjøre de personene som kan besørge etterlevelse, fremstår en slik pragmatisk tilnærming som formålstjenlig.

> Det sentrale synes dermed å være hvilke personer som reelt sett utøver kontroll over virksomheten eller funksjonen.

Da de overordnede formålene med DORA og NIS2 i stor grad overlapper, er det gode grunner for å forstå «management bodies» på samme måte også i NIS2. En liten nyanseforskjell er imidlertid at NIS2 benytter «management bodies» i flertall, noe som kan forstås som at kretsen av mulige ansvarlige organer skal utvides i forhold til DORA. Uansett kan andre enn styret og daglig leder blir ansvarlige, noe for eksempel sikkerhets, IT-ansvarlige og andre som har «C» som første bokstav i engelsk stillingstittel (CEO, CFO, CTO, CISO, osv.) bør merke seg.

Som antydet i proposisjonen pkt. 2.4.2.2, sitert over, kan fastsatte ansvarsforhold bli avgjørende. Av den grunn bør styrer og daglige ledere sørge for å formalisere ansvarsfordelingen nedover i organisasjonen, slik at de selv ikke risikerer å bli sittende med et personlig ansvar for en oppgave de i praksis ikke befatter seg med.

1.1.2 Hva betyr spesialreguleringen for «essensielle» enheter?

NIS2 angir også kretsen av mulige ansvarlige ett annet sted, nemlig i art. 32 (6). Bestemmelsen leser:

> *«Member States shall ensure that any natural person responsible for or acting as a* ***legal representative*** *of an* ***essential entity*** *on the basis of the power to* ***represent*** *it, the authority to* ***take decisions*** *on its behalf* or *the authority to* ***exercise control*** *of it has the power to ensure its compliance with this Directive. Member States shall ensure that it is possible to* ***hold such natural persons liable for breach*** *of their duties to ensure compliance with this Directive.»* [våre uthevinger]

Bestemmelsen gjelder altså bare «essensielle» enheter, men er klar på at fysiske personer skal kunne holdes ansvarlige (se del 1 i artikkelserien *NIS2: Hvilke virksomheter og leveranser vil omfattes av fremtidens krav til cybersikkerhet infrastruktur?*. Bestemmelsen er todelt: Den første delen pålegger landene å sørge for at personer som:

a. er juridiske representanter for en essensiell enhet;
b. har myndighet til å fatte beslutninger på enhetens vegne; eller
c. kan utøve kontroll over enheten

har myndighet til å etterleve direktivet. Myndighet skal følge ansvar.

Den andre delen av art. 32 (6) sier at slike personer skal kunne holdes personlig ansvarlige for

brudd på deres plikter til å sørge for etterlevelse. Ansvar skal følge myndighet. Mekanikken bringer oss tilbake til betydningen av ansvarliggjøring i virksomheten.

Dersom en daglig leder (CEO) ikke har sørget for at for eksempel IT-sjefen (CTO) har myndighet til å etterleve NIS2, vil hun selv, som neste, bemyndigede person være den med myndighet til å etterleve. En slik bemyndiget person skal kunne holdes ansvarlig, som angitt i del to, selv om hun ikke i praksis har (direkte) befatning med det aktuelle området. Strukturen innebærer et brutalt incentiv for å formalisere ansvarsforholdene i virksomheten, noe som også er en del av formålet med NIS2.

Hvor langt ned i organisasjonen kan man tenke seg at et slikt ansvar går? La oss tenke oss at IT-sjefen tydelig (og skriftlig) har gitt *nettverksansvarlig* i oppgave å sørge for at datanettverket etterlever lover og regler. Videre at nettverksansvarlig får myndighet til å fatte beslutninger knyttet til nettverkssikkerhet (se b over), med en viss økonomisk handlefrihet. Så kompromitteres nettverket, og det blir klart at nettverket ikke etterlever kravene NIS2 stiller. Dersom nettverksansvarlig ved å bruke sin myndighet kunne unngått bruddet, vil hun i utgangspunktet kunne bli personlig ansvarlig.

> Hvor langt ned i organisasjonen kan man tenke seg at et slikt ansvar går?

1.1.3 Kan offentlige tjenestepersoner blir personlig ansvarlige?

Mye av den infrastrukturen som NIS2 skal bidra til at blir sikker, besørges av det offentlige. Hvilket personlige ansvar offentlige tjenestepersoner har blir dermed av stor interesse.

Den danske versjonen av art. 20 (1) leser:

> *«Medlemsstaterne sikrer, at de væsentlige og vigtige enheders ledelsesorganer godkender de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet med henblik på at overholde artikel 21, fører tilsyn med dens gennemførelse og kan gøres ansvarlige for enhedernes overtrædelser af forpligtelserne i nævnte artikel.*
>
> *Anvendelsen af dette stykke* ***berører ikke national ret*** *for så vidt angår de ansvarsregler, der gælder for* ***offentlige institutioner****, samt ansvaret for* ***embedsmænd*** *og personer valgt eller udnævnt til* ***offentlige hverv****.»* [våre uthevinger]

Utgangspunktet må være at også offentlige tjenestepersoner kan bli holdt ansvarlig ved brudd på NIS2, da første avsnitt i første ledd ikke gjør unntak for offentlige tjenestepersoner. Men av annet avsnitt følger at særlige ansvarsregler for offentlige tjenestepersoner i nasjonal rett ikke skal berøres. Direktivet fremhever særlig embedsmenn og valgte og utnevnte personer. Hvorvidt dette betyr at alminnelige ansatte er mer eksponert for ansvar, bør klargjøres i den norske implementasjonen.

Av særlig interesse er regler som fritar offentlig tjenestepersoner for personlig ansvar eller letter ansvaret. Den mest nærliggende reglen er arbeidsgiveransvaret, som er knesatt i skadeerstatningsloven (skl.) § 2-1. Bestemmelsen sier i korthet at arbeidsgiver er ansvarlig for skade forvoldt forsettlig eller uaktsomt «under arbeidstakerens utføring av arbeid eller verv for arbeidsgiveren». Går arbeidstakeren utenfor det som «er rimelig å regne med etter arten av virksomhet eller saksområde», bortfaller vernet. Arbeidsgiver kan gå til regress mot arbeidstaker «for så vidt det finnes rimelig» utfra situasjonen (skl. § 2-3).

Arbeidsgiveransvaret betyr dermed ikke et generelt ansvarsfritak for handlingen eller unnlatelsen, men at den skadelidte kan holde seg til arbeidsgiveren. I praksis vil nok det store flertallet av saker medføre at den offentlige ansatte ikke personlig blir ansvarlig, siden tapet eller skaden som søkes erstattet normalt vil være knyttet til utføringen av arbeid.

Samtidig finnes det regler som ansvarliggjør offentlig ansatte, som for eksempel lov om interkommunale foretak, allmennaksjeloven og som vi kommer til, aksjelovene.

Hvor grensen for personlig ansvar for offentlige ansatte skal trekkes bør klargjøres ved implementasjonen av NIS2 i norsk rett. Det ville være uheldig for incentivene til å levere sikre tjenester i henhold til kravene i NIS2 dersom offentlig ansatte i praksis ikke risikerte personlig ansvar. En slik forskjellsbehandling i forhold til privat ansatte vil også fremstå som vilkårlig og urettferdig.

1.2 Forholdet mellom essensielle og viktige enheter

Som det fremgår over finnes det i NIS2 to grunnlag for personlig ansvar. Hva blir da forholdet mellom spesialbestemmelsen i art. 32 (6) for essensielle enheter og den generelle reglen i art. 20 (1)? Omfatter art. 32 (6) flere personer?

Rent umiddelbart fremstår art. 20 (1) å omfatte mer seniorpersoner, jf. «management bodies», altså en noe snever personkrets. En snevrere personkrets rimer godt med at art. 20 (1) også gjelder *viktige* enheter, og ikke bare essensielle som art. 32 (6). Forståelsen understøttes av DORAs definisjon av «management body», selv om forskjellen da kanskje blir mindre åpenbar. Selv personer som bekler «nøkkelfunksjoner» i henhold til nasjonal (eller EØS-rett) vil være en snevrere krets enn dem omfattet av art. 32 (6).

Et beslektet spørsmål er hva betydningen av at personer i *viktige* enheter ikke er tillagt et personlig ansvar i art. 33 slik personer i essensielle enheter er det i art. 32. Gitt vår konklusjon over om at «essensi-

elle» enheter har et personlig ansvar som kan gå lenger ned i organisasjonen enn den generelle reglen i art. 20 (1), er en nærliggende slutning at ansvaret for «viktige» enheter bare følger den generelle ansvarsregelen i art. 20 (1).

Vi mener det vil være unaturlig å tolke fraværet av en personlig ansvarsregel i art. 33 slik at brudd på kravene til sikkerhet i viktige virksomheter skulle kunne skje uten personlig ansvar. Også «viktige» enheter kan ha stor betydning for samfunnet. Slike «viktige» enheter kan pålegges overtredelsesgebyr. At gebyret er lavere enn for essensielle enheter, rimer med forskjellen i personkretsen som kan bli holdt personlig ansvarlig.

1.3 Ansvarsgrunnlag

Hverken art. 20 (1) eller 32 (6) angir om ansvar forutsetter uaktsomhet eller om skyld ikke kreves (objektivt ansvar). Fortalen er også taus om ansvarsgrunnlag. Bakgrunnen er trolig at spørsmål om valg av ansvarsgrunnlag anses å være et nasjonalt anliggende. Igjen blir det opp til departementet å foreslå ansvarsgrunnlag. Her vil vi nok se en del ulike regler fra land til land, inkludert å vise til erstatningsansvaret etter aksjelovene som vi kommer til i pkt. 2.

1.4 Hvem kan kreve og hva kan kreves?

NIS2 angir heller ikke *hvem* som kan kreve erstatning eller *hvilke* typer tap som kan kreves erstattet. Tredjepersoner som har lidd et tap bør kunne kreve erstatning. Men hva med virksomheten selv, vil den kunne holde sine egne ledere personlig ansvarlig? Og hva med aksjonærer som lider tap pga. manglende etterlevelse? Skal alle typer tap kunne kreves dekket av de ansvarlige? Vil det personlige ansvaret være et erstatningsansvar? Om ja, vil de som har lidd et tap kunne kreve kompensasjon for driftsforstyrrelser, gjenopprettingskostnader, bøter og andre økonomiske tap? Alle disse spørsmålene bør løses ved den nasjonale implementeringen.

1.5 Sanksjoner mot virksomheter som kan få betydning for det personlige ansvaret

For fullstendighetens skyld, og fordi krav mot en virksomhet kan begrunne et krav mot en fysisk person, tar vi med en kort oversikt over de mest sentrale sanksjonene i NIS2.

a. Overtredelsesgebyret er ett av ganske få reguleringer i NIS2 som skiller mellom essensielle og viktige virksomheter. For essensielle virksomheter skal et gebyr på minst opptil 2 % av årlig omsetning foregående rapporteringsår gjelde eller EUR 10 000 000 (NIS2 art. 34 (4)). Det høyeste beløpet skal legges til grunn. Tilsvarende tall for viktige virksomheter er 1,4 % og EUR 7 000 000 (5).
b. Ledelsen kan fjernes midlertidig etter NIS2 art. 32 (5) b dersom ikke varsel, instruks, pålegg eller anbefalinger som beskrevet i art. 32 (4) har gitt tilstrekkelig virkning.
c. Virksomheten kan stanses midlertidig etter art. 32 (5) a på samme vilkår som ledelsen kan fjernes.
d. Oppnevnelse av en overvåkingsansvarlig i en periode etter art. 32 (4) g.

Særlig de første tre sanksjonene nevnt over vil kunne medføre betydelige økonomiske belastninger for en virksomhet, og utgjør dermed de mest aktuelle grunnlagene for et krav mot de ansvarlige personene. De øvrige syv sanksjonene eller tiltakene listet i art. 32 (4); varsel, instruks, pålegg (opphør ulovlig adferd og etterlevelse), rapportering, anbefalinger og offentliggjøring, vil vanskeligere kunne tenkes å danne grunnlag for et krav.

Katalogen over sanksjoner er noe kortere for viktige virksomheter, regulert i art. 33. Disse slipper unna uten overvåkingsansvarlig, suspensjon av ledelse eller virksomhet og spesialregulering av personlig ansvar, som beskrevet over.

Som neste punkt vil vise, kan disse sanksjonene også få betydning etter det norske erstatningsansvaret nedfelt i aksjelovgivingen.

2 Det personlige Ansvaret etter norsk aksjelovgivning

For ikke å sprenge rammene for denne artikkelen begrenser vi oss til å behandle ansvaret etter den norske aksjeloven. Vi nevner likevel at annen lovgiving, for eksempel allmennaksjeloven og lov om interkommunale foretak, i stor utstrekning har likelydende regulering. Straffansvar kan også tenkes, enten gjennom bestemmelser i aksjeloven eller i straffeloven, men heller ikke dette vil behandles.

Det personlige ansvaret i norsk rett er ofte omtalt som *styreansvaret*. Begrepet styreansvar indikerer at det kun er personer med styreverv som vil kunne holdes personlig ansvarlig for tap. Slik vi vil vise under, er dette misvisende. «Styreansvaret» er i realiteten et regulært erstatningsansvar som kan strekke seg langt ned i organisasjonen.

2.1 Krav til styret og ledelsen

Før vi dykker dypere inn i det personlige ansvaret for styret og ledelsen er det hensiktsmessig å kort si noe om hvilke krav bakgrunnsretten stiller til de nevnte ved deres utøvelse av de aktuelle rollene og vervene.

Aksjeloven (asl.) inneholder ingen uttømmende krav til hvordan styret og ledelsen skal utføre sine oppgaver og hva oppgavene er. En grunnleggende forutsetning er imidlertid at styret og ledelsen plikter å utøve sine oppgaver i henhold til lov og vedtekter på en forsvarlig måte.

Styret og ledelsen har i henhold til aksjeloven et overordnet forvaltnings- og tilsynsansvar, jf. asl.

§§ 6-12 - 6-14. Styret og ledelsen skal videre ivareta aksjeeiernes vinningsformål, jf. asl. §§ 2-2 (2), jf. 8-4 a, i tillegg til at styret har et særskilt ansvar for å sikre forsvarlig egenkapital og likviditet i selskapet, jf. asl. §§ 3-4 og 3-5.

I tillegg til dette må styremedlemmer ivareta interessene til kreditorer, kunder, ansatte, markedet og samfunnet som helhet. Denne balansegangen påvirker også forventningene som kan stilles til styret . Dette er understreket i rettspraksis, blant annet i Rt. 1993 s. 1399, og i lovforarbeidene, som Prop. 135L (2018-2019) s. 94-95. Styremedlemmer har også taushetsplikt og må avstå fra å utnytte forretningsmuligheter som kan komme i konflikt med selskapets interesser.

Ut over kravene som følger av dette må styret og ledelsens plikter normalt utledes av oppdraget (oppdragsavtalen) eller den underliggende ansettelsesavtalen. Kravene vil måtte avpasses ut fra størrelsen på virksomheten og risikoen i markedet virksomheten driver.

Gjennom disse pliktene er tanken at aksjeloven sikrer at styret opptrer med forsvarlighet og integritet, og at det balanserer ulike hensyn i tråd med selskapets formål og samfunnets forventninger.

2.2 Hvem kan bli ansvarlig?

Det såkalte styreansvaret er regulert av asl. § 17-1, som fastsetter at daglig leder, styremedlemmer, medlemmer av bedriftsforsamlingen, aksjeeiere og andre («*den som*») kan holdes erstatningsansvarlige for skade de har forårsaket forsettlig eller uaktsomt. Ansvaret er individuelt. Dermed kan ett styremedlem bli ansvarlig, mens andre går fri.

Personkretsen som kan gjøre krav om erstatning gjeldende er vid; både selskapet, en aksjeeier og «andre» kan kreve sitt tap erstattet. Selve erstatningsansvaret er slik ordlyden viser, heller ikke begrenset til styret alene, men kan pålegges «den som», altså medvirkeren. Medvirkeransvaret kan omfatte enhver som har bidratt til skaden, for eksempel regulære ansatte, samfunnsorganisasjoner eller interessegrupper, mv., jf. Aarbakke m.fl., Aksjeloven kommentarutgave, § 7-1 note 2.5. Dette gjør ansvar etter aksjeloven § 17-1 aktuelt for roller som for eksempel CFO, COO, CISO og CTO samt mer ordinære ansatte.

I *LB-2023-22165* ble en prosjektleder holdt ansvarlig etter asl. § 17-1. Retten konkluderte med at han hadde hatt en så sentral rolle i et havarert oppussingsprosjekt at han sammen med daglig leder og styreleder ble ilagt erstatningsansvar overfor byggherren, med hjemmel i bestemmelsens medvirkeransvar. I *THOS-2023-16539* (Nordlo), som riktignok ikke gjaldt styreansvaret, finner man uttalelser som går i retning av at det oppstilles et ansvar for ledelsen der underleverandører ikke oppfyller de forpliktelser som er pålagt dem i henhold til kontrakt, mv.

2.3 Ansvarsgrunnlag og andre vilkår for erstatningsansvar

Erstatningsansvar etter asl. § 17-1 forutsetter at de alminnelige vilkårene for erstatning er oppfylt. Herunder må det foreligge en skade eller et tap, ansvarsgrunnlag og årsakssammenheng. Kravet om årsakssammenheng viser til betingelseslæren. Altså må skaden eller tapet ha blitt påført i egenskap av utøvelse av vervet som styremedlem, daglig leder, osv. Se også pkt. 3.

Medvirkeransvaret er spesielt i den forstand at det forutsetter at det foreligger ansvarsgrunnlag for «hovedmannen» etter første ledd, men likevel slik at medvirkeransvaret ikke er betinget av at hovedmannen har opptrådt forsettlig eller uaktsomt – det er tilstrekkelig at hovedmannen har opptrådt rettsstridig, jf. Ot.prp. nr. 55 (2005-2006) s. 1686. Medvirker må kunne bebreides for å ha medvirket til hovedmannens rettsstridige handling, uten at medvirker selv må ha brutt en norm.

2.4 Når aktualiseres typisk styreansvaret?

Det følger av norsk rettspraksis at det er en presumsjon (antagelse) for uaktsomhet ved pliktbrudd, jf- *HR-2016-1440-A* (Håheller-dommen). Slike pliktbrudd kan oppstå ved brudd på lovpålagte forpliktelser, plikter fastsatt i vedtekter, etablerte prinsipper og avtaler. Ved introduksjon av NIS2, DORA og andre sikkerhetsregler vil volumet av slike forpliktelser øke voldsomt. Presumsjonsmekanismen og det økte regelomfanget understreker viktigheten av å utvise aktsomhet på alle områder, men særlig hva angår cybersikkerhet. Utviklingen gjør at forventningene til personer i de ulike stillingene blir svært viktig å avklare i forkant av at oppdraget påtas eller stillingen besettes.

> Det følger av norsk rettspraksis at det er en presumsjon (antagelse) for uaktsomhet ved pliktbrudd.

Det er viktig å merke seg at manglende kvalifikasjoner ikke medfører ansvarsfrihet. Dette betyr at hvis man først har akseptert et styreverv eller en stilling, så har man samtidig bekreftet at man er kvalifisert til det aktuelle vervet eller stillingen.

I saker om erstatningsansvar etter asl. § 17-1 er det ofte brudd på handleplikten som anføres som ansvarsgrunnlag. Handleplikten innebærer at styret må ta nødvendige grep for å unngå eller begrense tap når for eksempel selskapets egenkapital eller likviditet er uforsvarlig (dårlig).

Cyberangrep kan tilsvarende få alvorlige økonomiske konsekvenser for en virksomhet, og kan i sin ytterste konsekvens lede til at hand-

leplikten i asl. § 3-4 og § 3-5 utløses. Nedetid i systemene kan påvirke inntjeningen og omsetningen betydelig, mens betaling av løsepenger kan føre til umiddelbare belastninger på selskapets kontantbeholdning. Selv mindre angrep kan få så store økonomiske følger at de påvirker selskapets egenkapital og likviditet i en grad som utløser styrets handleplikt. Overtredelsesgebyr etter NIS2, kan gi tilsvarende virkning.

Når handleplikten inntrer, må styret vurdere handlingsrommet, identifisere mulige alternativer og iverksette tiltak for å rette på situasjonen. Dette kan inkludere å forhandle med trusselaktørene, betale løsepenger eller leie inn bistand til total nyetablering av IT-systemene. I ytterste konsekvens kan et tiltak være å foreslå selskapet oppløst (avviklet) eller melde oppbud. Se mer om styrets handlingsrom under i pkt. 2.5.

Dersom styret og ledelsen forholder seg passiv eller handler uforsvarlig, og derigjennom påfører for eksempel en aksjonær et tap, kan veien til erstatningsansvar være kort. Dette understreker viktigheten av at styret har en klar strategi og kompetanse til å håndtere krisesituasjoner som cyberangrep, samtidig som det oppfyller sine lovpålagte plikter.

2.5 Hvilket handlingsrom foreligger?

Som nevnt over i pkt. 2.4 er det en presumsjon for uaktsomhet ved pliktbrudd, jf. HR-2016-1440-A (Håheller).

Organiseringen av en virksomhet i et aksjeselskap innebærer imidlertid en ansvarsbegrensning. Begrensningen gjør at det kreves noe spesielt for at styret skal kunne holdes personlig ansvarlig for egne feildisposisjoner, jf. Rt. 1991 s. 119 (Normount). Herunder ligger det innenfor styrets å pådra selskapet rimelig risiko, jf. *HR-2022-2484-A* (Spiro). I samme avgjørelse viser Høyesterett til at det er rom for å ta feil; terskelen for å i ettertid holde styret ansvarlig for forretningsmessige feilvurderinger er høy.

Illustrasjon: Colourbox.com

Det sies gjerne at styret har et visst handlingsrom selv om handleplikten er utløst. Prinsippet har blitt bekreftet i en rekke rettsavgjørelser, for eksempel *HR-2017-2375-A* (Ulvesund) og *LB-2023-130472-2* (Norske Skog). I denne rettspraksisen heter det at ledelsen har et visst strategisk handlingsrom, og det avgjørende for om man kan drive videre er om det er et realistisk håp om å redde selskapet, at ledelsen arbeidet aktivt og lojalt med dette for øyet, og eventuelt kastet kortene innen rimelig tid dersom man ser at redningsforsøket mislykkes.

Selv om den aktuelle rettspraksisen som her er gjengitt gjelder spesifikt for styret er det grunn til å tro at ledelsen generelt vil underlegges samme vurdering.

Vi står derfor overfor en situasjon hvor styret og ledelse har et ikke ubetydelig handlingsrom hva angår forretningsmessige beslutninger, samtidig som Høyesterett har strammet inn kravet til å etterleve konkrete plikter som følger av lov og andre normer. Dette legger press på styret og ledelsen, og bekrefter viktigheten av å ha klare ansvarsinndelinger og rutiner på plass.

2.6 Ansvarsfrihet

Ledelsen har slik vi har vist over et omfattende ansvar for å sikre at selskapet drives i tråd med lov, vedtekter og forsvarlige forretningspraksis. Selv om ansvaret er strengt, er det flere situasjoner hvor ansvarsfrihet kan tenkes. Aksjeloven § 17-2 gir anvisning på lemping, altså reduksjon, av erstatningsansvaret etter asl. § 17-1. Bestemmelsen i § 17-2 henviser til skadeserstatningsloven § 5-2 hvor det heter at erstatningsansvaret kan lempes når retten «*under hensyn til skadens størrelse, den ansvarliges økonomiske bæreevne, foreliggende forsikringer og forsikringsmuligheter, skyldforhold og forholdene ellers*» *finner at ansvaret virker «urimelig tyngende»* for den ansvarlige.

Manglende innsikt og/eller faktisk involvering i selskapets virksomhet og beslutninger, eller manglende tilstedeværelse i styremøter eller beslutningsprosesser kan også lede til ansvarsfrihet. Ren passivitet eller ubegrunnet fravær kan derimot være uaktsomt i seg selv og derfor ikke nødvendigvis ansvarsbefriende.

Det kanskje viktigste «forsvaret» mot ansvar for styremedlemmer eller personer i ledergrupper er å sørge for at vurderinger og eventuelle dissenser dokumenteres. Dokumentasjon av dissenser kan være en effektiv måte for enkeltpersoner å beskytte seg mot ansvar dersom for eksempel styret tar beslutninger som et medlem mener er uforsvarlige. Dissensen kan bidra til å tydeliggjøre at medlemmet har utvist aktsomhet, selv om flertallet har valgt en annen retning. Det samme gjelder dersom man som ordinær ansatt har gjort ledelsen oppmerksom på et kritikkverdig forhold, men opplever at anbefalingen om å bøte på situasjonen ikke blir tatt til etterretning. I et slikt tilfelle er det avgjørende å etablere skriftlige spor som viser at man faktisk har varslet om det kritiske forholdet, slik at ansvaret havner hos personen som reelt sett tok beslutningen.

2.7 Forsikring

Forsikringer spiller en viktig rolle i å redusere personlig risiko. Styreansvarsforsikring gir styret beskyttelse mot økonomiske krav som følge av erstatningskrav. Her bør selskapet være observant på at styreforsikringer ikke nødvendigvis beskytter andre personer enn styremedlemmene og daglig leder. I tillegg kan en god cyberforsikring være avgjørende for å dekke de betydelige kostnadene av cyberangrep. En kriminalitetsforsikring kan avlaste risiko utro tjenere representerer. Ansatte i selskapet vil være dekket av selskapets ordinære ansvarsforsikring. Bruk en anerkjent forsikringsmegler for konkrete råd.

3. Årsakssammenheng

Ansvar etter både NIS2 og asl. § 17-1 forutsetter at handlingen eller unnlatelsen har ledet til konsekvensen, et tap eller en skade. Jo mer sammensatte årsaksrekker, jo mer krevende vil det være å fastslå tilstrekkelig sammenheng. Ville en for eksempel en investering i et sikkerhetssystem til 150 000 kroner medført at et datainnbrudd ville blitt avverget? Om ja, var det uaktsomt å la være å bruke pengene, da man uansett ikke er garantert full sikkerhet og virksomheten hadde behov for pengene til andre viktige formål?

I prinsippet vil ikke en slik vurdering under NIS2 være vesentlig annerledes vurderingen av årsakssammenheng i andre komplekse saksforhold, inkludert ved vurderingen etter asl. § 17-1.

4. Skjerper NIS2 ansvaret i forhold til ASl. § 17-1?

Siden vi enda ikke vet hva som blir ansvarsgrunnlaget i NIS2, hvem som kan kreve hvem for hva, er det for tidlig å si om NIS2 isolert sett skjerper ansvaret. Innføringen av nye plikter, må vi imidlertid kunne anta at vil medføre at en person lettere kan bli kjent ansvarlig under det tradisjonelle styreansvaret i norsk rett.

5. Avslutning

Styrets, ledelsens og ansattes ansvar er en kompleks og dynamisk del av norsk selskapsrett. Med skjerpede krav til aktsomhet og økt fokus på risikostyring fra domstolenes side, men også som følge av nye plikter og økt angrepsrisiko, må styremedlemmer og ledelse være godt informert om sine plikter og ansvar. Rettspraksis viser at domstolene i stor grad respekterer styrets vurderinger, men at klare feilvurderinger kan føre til ansvar. Derfor er det avgjørende å ha en proaktiv tilnærming til styring og risikohåndtering.

Kristian Foss, advokat, Bull & Co advokatfirma.

Advokat Mira Levánd Bergsland er partner i Advokatfirmaet Bull AS, og er kjent for sin spisskompetanse innenfor konkurs- og insolvensrett. Hun har omfattende erfaring med konkurs- og rekonstruksjonsbehandling som bostyrer, restrukturering av virksomheter, finansiering og pant samt M&A transaksjoner, i tillegg til at hun jevnlig jobber med ansvarsspørsmål for styret og ledelsen i norske bedrifter.

Pelham II: Betydningen av «stil» for forståelsen av pastisjunntaket[1]

Av Didrik Arnesen

1. Pastisjunntakets aktualitet

Det overordnede formålet med den EU-rettslige reguleringen av opphavsretten er å skape balanse mellom grunnleggende rettigheter. På den ene siden står rettighetshavers rett til immateriell eiendom etter EU-Charteret artikkel 17 nr. 2; på den andre siden står brukernes ytringsfrihet og kunstneriske frihet etter EU-Charteret artikkel 11 og 13. For å ivareta denne balansen har EU-lovgiver gjort unntak fra rettighetshaverens enerett til eksemplarfremstilling og tilgjengeliggjøring av åndsverk eller annen nærstående prestasjon.[2] En av unntaksreglene følger av opphavsrettsdirektivet artikkel 5(3)(k) og digitalmarkedsdirektivet3 artikkel 17(7)(b), som gir rett til å bruke opphavsrettslig beskyttede verk til pastisj, i tillegg til parodi og karikatur.

Digitalmarkedsdirektivet – som ble vedtatt av EU i 2019 – pålegger medlemslandene å innføre unntaksregelen fullt ut, i motsetning til det eldre opphavsrettsdirektivet som gjorde innføringen av unntaksregelen valgfri.[4] Unntaksregelens nye obligatoriske karakter er nok en grunn til at pastisjbegrepets rettslige innhold i nyere tid er viet mer oppmerksomhet.

Didrik Arnesen

Begrepet «pastisj» brukes sjelden i dagligtale, og ordets meningsinnhold har historisk sett vært inkonsekvent og har blitt forstått ulikt mellom land.[5] «Pastisj» kan kort defineres som en imitasjon av stilen til for eksempel et verk, en kunstner, en epoke eller en sjanger.[6] Det er imidlertid uklart hvordan denne definisjonen skal forstås i en opphavsrettslig kontekst. Grunnen til dette er at en «stil» ikke nødvendigvis er omfattet av opphavsretten, ettersom begrepet kan sikte til de bakenforliggende ideene heller enn det konkrete uttrykket.[7] Ved en slik forståelse sitter man igjen med en unntaksregel uten praktisk betydning, ettersom man uansett befinner seg utenfor opphavsrettens beskyttelsessfære.

> Unntaksregelens nye obligatoriske karakter er nok en grunn til at pastisjbegrepets rettslige innhold i nyere tid er viet mer oppmerksomhet.

Istedenfor å avvise «pastisj» som et meningsløst tilskudd til unntaksbestemmelsen, mener for eksempel European Copyright Society[8] at det vide begrepet satt i en opphavsrettslig kontekst kan være grunnlaget for en fleksibel unntaksregel. Etter deres syn bør pastisjregelen tolkes som en sekkebestemmelse som tillater enhver transformativ bruk av elementer fra eksisterende verk.[9] Andre har fremhevet EU-Charteret

1 Forholdet til norsk rett vil ikke bli problematisert i denne artikkelen, men kan leses om i Arnesen, Didrik (2025) *Den opphavsrettslige statusen til "pastisj" – Hva er den rettslige betydningen av pastisjbegrepet i EU- og EØS-retten, og hvordan forholder norsk rett seg til denne forståelsen? (heretter Arnesen (2025)).*

2 Disse rettighetene følger av Rådsdirektiv 2001/29/EF (heretter opphavsrettsdirektivet) artikkel 2 og 3.

3 Directive (EU) 2019/790.

4 Det kan imidlertid diskuteres om manglende innføring av unntaksregelen vil være i strid med EU-Charteret artikkel 13, se Opinion of Advocate General Emiliou delivered on 17 June 2025 (heretter *Pelham II-uttalelsen) avsn. 96-111 og Arnesen (2025) s. 9.*

5 Se *Pelham II-uttalelsen avsnitt 49.*

6 Se *Pelham II-uttalelsen avsn. 50 og Arnesen (2025) s. 11-12 med videre henvisninger.*

7 Det er et grunnleggende opphavsrettslig prinsipp at ideer ikke gis vern, se for eksempel Rognstad, Ole Andreas (2019) *Opphavsrett s. 91 og Linkis, Jacob (2017) Dansk ophavsrets fleksibilitet – En retsdogmatisk analyse af ophavsretslovens fortolkningsmæssige grænser s. 169.*

8 En organisasjon bestående av akademikere innenfor opphavsrett fra ulike land i Europa.

9 Se European Copyright Society (2024) *Opinion of the European Copyright Society on CG and YN v Pelham GmbH and Others, Case C-590/23 (Pelham II).*

artikkel 13 som en grunn til at nettopp en slik fleksibel regel er nødvendig.[10]

En endelig avklaring av pastisjbegrepets EU-rettslige betydning forventes å komme etter EU-domstolens behandling av sak C-590/23 (*Pelham II*). Saken oppsto etter at produsenten Moses Pelham samplet et to-sekunders lydklipp fra Kraftwerks elektro- og industrilåt *Metall auf Metall* uten å innhente tillatelse fra rettighetshaverne og brukte denne i loop som del av rytmen til hip-hop-låten *Nur Mir*. Saken har allerede resultert i en prejudisiell avgjørelse fra EU-domstolen.[11]
I 2021 ble bruk av åndsverk og nærstående prestasjoner til pastisj tillatt etter den tyske åndsverksloven,[12] og Pelham sin side argumenterer for at samplingen må anses som en lovlig pastisj fra og med lovendringens ikrafttredelsestidspunkt.[13]

I forbindelse med den kommende saken for EU-domstolen avga Generaladvokat Emiliou sin uttalelse i *Pelham II* i juni. Dersom EU-domstolen følger hans anbefaling, vil ikke pastisjunntaket være en fleksibel sekkebestemmelse. Generaladvokaten ga uttrykk for at det EU-rettslige pastisjbegrepet bør forstås som en kunstnerisk frembringelse som "(i) evokes an existing work, by adopting its distinctive 'aestetic language' while (ii) being noticeably different from the source imitated, and (iii) is intended to be recognised as an imitation."[14] Uttalelsen er inntil videre et naturlig utgangspunkt for den EU-rettslige forståelsen av "pastisj", og enkelte sider ved hans syn vil bli nærmere behandlet i det følgende.

10 Se *Pelham II-uttalelsen avsnitt 5*.
11 Se sak C-476/17 Pelham GmbH and Others v Ralf Hütter and Florian Schneider-Esleben (*Pelham I*).
12 Se *Pelham II-uttalelsen avsn. 42*.
13 For en grundigere innføring i sakens faktum, se *Pelham II-uttalelsen avsn. 1 og 9-18*.
14 Se *Pelham II-uttalelsen avsn. 133*.

2. Ikke en sekkebestemmelse

Generaladvokaten er ikke enig i at unntaksregelen blir meningsløs ved at den avgrenses til å gjelde imitasjoner av et annet verks stil. Han mener videre at pastisjunntaket ikke kan være en sekkebestemmelse, ettersom en slik tolkning ville gjort de andre opplistede unntakene overflødige.[15] Videre ville pastisjunntaket i praksis blitt en fribruksregel som strider imot det EU-rettslige systemet som legger opp til at rettighetsbeskyttet materiale kun kan benyttes i konkret angitte tilfeller.[16] I stedet tar Generaladvokaten aktivt i bruk stilbegrepet til å avgrense både hva som kan lånes fra verk og hvordan det skal kunne brukes i den nye frembringelsen.

3. Bare stilistiske elementer kan lånes

Generaladvokaten uttaler at pastisjunntaket skal gi adgang til å låne konkrete verkselementer som oppfyller verkshøydekravet, så lenge det som lånes er «stilistisk».[17]

> Pastisjunntaket skal gi adgang til å låne konkrete verkselementer som oppfyller verkshøydekravet, så lenge det som lånes er «stilistisk».

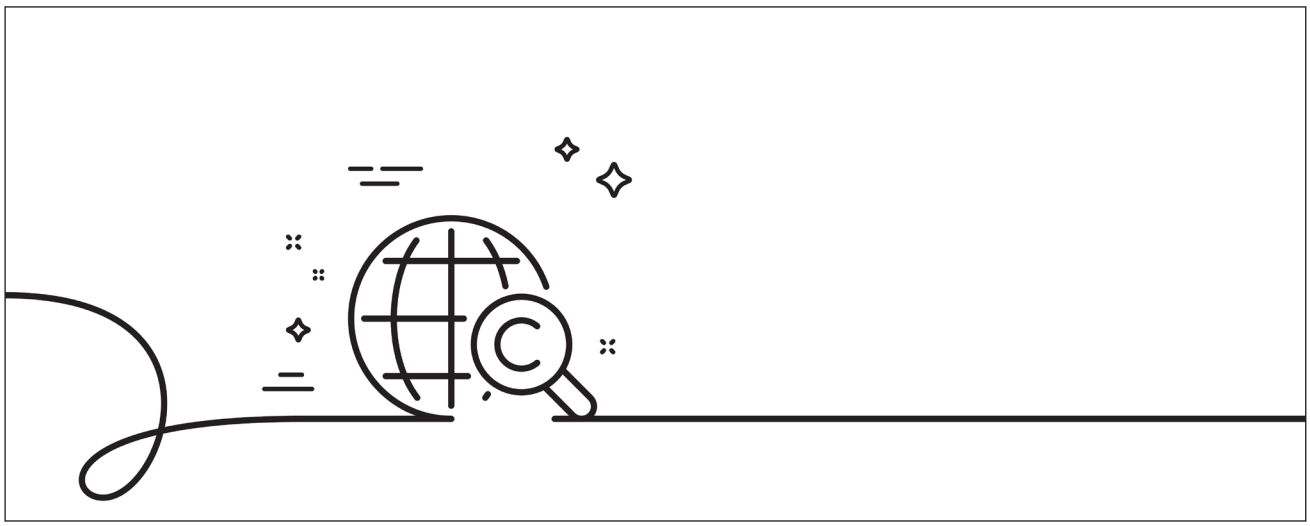
Generaladvokaten oppstiller ikke konkrete kriterier for vurderingen av om et verkselement som lånes er stilistisk. Man kan for eksempel argumentere for at alle enkeltelementer i et verk bidrar til å skape stilen til verket, og at alle elementene derfor er stilistiske. En slik tolkning vil innebære at brukeren fritt kan velge hvilke verkselementer han vil låne, så lenge de øvrige vilkårene er oppfylt. En annen mulig tolkning – som tilsynelatende er mer i samsvar med Generaladvokatens forståelse – er at brukeren bare kan låne de elementene ved verket som representerer eksempelvis sjangeren verket naturlig kan plasseres i, eller kunstnerens stil basert på tidligere verk. Et aktuelt eksempel kan være bruk kunstig intelligens til å lage bilder i Studio Ghibli-stil. Her vil stilen bli definert ut ifra en vurdering av hvilke visuelle trekk som går igjen i filmene. Generaladvokaten mener at en slik unntaksregel også gir brukeren adgang til å sample lydopptak for å lage en pastisj av den underliggende sjangeren.

15 Se *Pelham II-uttalelsen avsn. 69*.
16 Se *Pelham II-uttalelsen avsn. 71*.
17 Se *Pelham II-uttalelsen avsn. 66*.

4. Et krav om at bruken er i samme stil

Videre mener Generaladvokaten at det må kreves at den nye frembringelsen er i samme stil som originalverket for å være omfattet av pastisjunntaket. Ved en slik tolkning får ikke pastisjunntaket anvendelse i Pelham-saken, ettersom *Nur Mir* tilhører en annen sjanger enn *Metall auf Metall*. Hadde samplingen blitt brukt til å lage en annen elektro- og industrilåt, hadde man imidlertid kunne vært innenfor pastisjunntakets anvendelsesområde slik Generaladvokaten definerer det.

Man kan innvende at kravet om at sjangeren til det imiterende verket er sammenfallende med originalverkets sjanger ikke bør vurderes strengt. En grunn til dette er at unntaksregelen også krever at den nye frembringelsen er merkbart forskjellig fra originalverket. Selv om en frembringelse som imiterer et verk kan være merkbart forskjellig fra et verk i samme sjanger, er det nok liten tvil om at forskjellene er enda større dersom den nye frembringelsen ikke er strengt bundet av sjangertrekkene. Mange kunstneriske ytringer som låner fra tidligere verk blander stiler for å bryte med originalverket. Muligens bør det finnes en annen adgang til slik fri bruk av verk enn den som følger av paro-



Illustrasjon: Colourbox.com

diregelen for humoristiske imitasjoner.

Det kan også nevnes at Generaladvokatens avgrensning ikke nødvendigvis er ideell, sett hen til de bakenforliggende hensynene til unntaksregelen. Det er ikke gitt at opphaveren ønsker at en imitasjon skal ligge tett opp til originalverket, samtidig som en bruker trolig ønsker å ha et større handlingsrom.

5. For liten frihet?

Selv om Generaladvokaten bruker stilbegrepet til å konstruere en vesentlig snevrere regel enn den tidligere foreslåtte sekkebestemmelsen er han enig i at hans tolkningsresultat fører til en ubalanse mellom rettighetshavernes og allmennhetens interesser. Denne bekymringen knytter seg riktignok ikke til utnyttelsen av verksdeler som i seg selv har verkshøyde, men snarere til bruk som kun berører de nærstående rettighetene. For eksempel mener Generaladvokaten at produsenters enerett til å råde over lydopptaket blir for omfattende ettersom den gjelder enhver gjenkjennelig bruk av opptaket. Selv om han mener at dette utstrakte produsentvernet ikke er tilstrekkelig begrunnet i investeringshensynet, gir direktivene ikke adgang til en innsnevring.[18]

Generaladvokaten deler også synet til blant andre European Copyright Society om at det nåværende EU-rettslige regelverket kan stå i veien for kunstnerisk utvikling, for eksempel innen musikk. Han peker på at en fribruksregel kan bidra til å løse dette problemet. Etter hans syn krever en slik regel likevel en lovendring, og at den ikke kan innfortolkes i pastisjunntaket.[19]

Didrik Arnesen, advokatfullmektig, arbeider i Advokatfirmaet Wiersholms avdeling for teknologi, media, telekom og immaterialrett.

18 Se *Pelham II-uttalelsen avsn. 112-125.*

19 Se *Pelham II-uttalelsen avsn. 130-132.*

Lovgivning i et digitalt samfunn – Om å bruke lover for å fremme og temme algoritmene

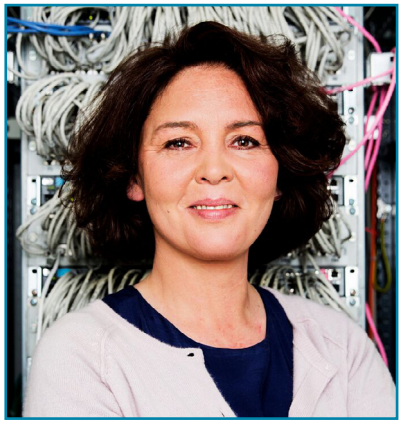
Av Hanne Marie Motzfeldt, ph.d. jur.

Professor, Dr. Jur. Dag Wiese Schartums værk, *Lovgivning i et digitalt samfunn – Om å bruke lover for å fremme og temme algoritmene*, er udgivet i 2025 som en del af CompLex-serien fra Norwegian Research Center for Computers and Law, Universitetet i Oslo. Gennem bogens 311 sider adresserer professor Schartum på erfaren og kompetent vis en af vor tids mest presserende udfordringer: Hvordan forskellige aktører i lovgivningsprocesserne kan og bør forholde sig til den digitale udvikling.

Forfatterens ambition er at øge læserens forståelse for samspillet mellem lovgivning og de digitale løsninger, der anvendes i nutidens samfund (informations- og datasystemer). Formålet er at styrke den demokratiske styring af det digitale samfunds udvikling ved at udbrede viden om og indsigt i dette samspil.

Heraf affødes en opdeling i to overordnede tematikker, der går igennem bogen som en – i øvrigt befriende klar og tydelig – rød tråd. Den ene tematik er, hvordan lovgivning kan anvendes til på konstruktiv og afbalanceret vis at sætte rammer for teknologier for derved at understøtte politisk acceptabel anvendelse af informations- og datasystemer (tæmme algoritmerne). Den anden tematik er, hvordan lovgivning kan udformes til let at implementeres ved hjælp af informations- og datasystemer, herunder automatisk retsanvendelse eller digital beslutningsstøtte (fremme algoritmerne).

Den velstrukturerede fremstilling indledes med **kapitel 1**, der kridter banen op. Kapitlet, der bl.a. indeholder et meget læseværdigt afsnit



Hanne Marie Motzfeldt

om simpel brug af teknologi over for den integrererede udvikling af teknologi, organisation og arbejdsgange, efterfølges af 9 øvrige kapitler. Disse 9 kapitler er systematiseret i 4 hoveddele, der hver især belyser forskellige aspekter af forholdet mellem lovgivning og digitalisering.

Del 1, der giver læseren generelle perspektiver på forholdet mellem lovgivning og digitalisering, samler kapitlerne 2–4. **Kapitel 2** om lovstaten og det digitale samfund indledes med en diskussion af, hvordan retsstaten i modsætning til lovstaten indebærer visse krav til lovgivningens indhold og til, hvordan myndighed udøves. Forfatteren præsenterer i umiddelbar forlængelse heraf bl.a. grundtanken om politik over teknologi og drøfter den hastige teknologiudvikling versus de langsomme demokratiske lovgivningsprocesser. Ved hjælp af næsten finurlig leg med sproget og brug af nutidens parole om ikke at komme for sent til AI-toget, gennemføres en vellykket vurdering af behovet for tidlig (udprøvende) lovregulering. Kapitel 2 introducerer også, hvordan lovgivning kan fungere som en kravspecifikation for informations- og datasystemer, og drøfter en række forhold, herunder hvordan digitalisering kan ændre arbejdsfordelinger, magtforhold og føre til måske vel rigid adfærdsregulering. **Kapitel 3** om digitaliserings- og automatiseringsvenlig lovgivning kaster bl.a. et blik på EU's, norske og danske politikker og programmer om digitaliseringsklar lovgivning for derefter at introducere en række grundlæggende tilgange, begreber og sondringer. Det er i den forbindelse en lettelse, at en retsvidenskabelig forsker med Schartums tyngde og uomtvistelige anerkendelse slår fast, at fravær af retlige rammer ikke i sig selv er digitaliseringsvenligt. I stedet er kapitlets – og bogens – udgangspunkt, at sådan regulering bør skabe en forudsigelig retsstilling. Del 1 afsluttes med det praktisk orienterede **kapitel 4** om modeller, metoder og værktøjer for at udarbejde digitaliseringsvenlig lovgivning. I kapitlet tages en række forskellige lovudviklingsmodeller, -metoder og digitale værktøjer op, ligesom der dykkes ned i forholdet mellem lov- og systemudvikling, behovet for indsigt og kompetencer samt samarbejde mellem politikere, jurister og teknologer.

De efterfølgende kapitler 5–6 er placeret i bogens **del 2** og omhandler lovgivning som ramme for datasystemer og digitalisering. Det centrale **kapitel 5** om lovgivningsprincipper formulerer og uddyber en række principper, der kan overvejes og afvejes overfor modstridende hensyn, når der udformes lovgiv-

ning inden for det digitale område – naturligvis forudsat, at der består et politisk ønske om harmoni med grundlæggende friheder, rettigheder og balancer i et demokratisk samfund. I overskriftsform er disse grundigt gennemtænkte 19 lovgivningsprincipper: Lovlighed, retfærdighed, forsvarlig sagsoplysning, proaktivitet, åbenhed, dokumentation, indbygning af retsprincipper og regler (via design), forståelighed, forklarlighed, kontradiktion, menneskelig kontrol, selvbestemmelse, medvirken, formålsbegrænsning, rigtighed og ajourføring, dataminimering, tidsbegrænsning (lagringsbegrænsning), forholdsmæssig kontrol samt evaluering og kontrol. Efter kapitel 5 går forfatteren videre til mere lovgivningstekniske temaer i **kapitel 6**, hvor det behandles, hvordan love kan og bør skrives for at regulere informations- og datasystemer. Kapitlets reflekterede drøftelser af reguleringsgrader og betydningen af lovgivers teknologiske indsigt suppleres bl.a. af en kærkommen klarlæggelse af, hvad der ligger i betegnelsen teknologineutral lovgivning. I fremstillingen anvendes denne klarlæggelse til en nyttig drøftelse af vanskelighederne ved at kombinere teknologineutralitet og sproglig klarhed. Kapitlet uddyber samtidig en række strategier for både at understøtte (fremme) og styre (tæmme) digitalisering, herunder regulering af AI.

Bogens **del 3** om lovgivning som indhold består af kapitel 7–9. **Kapitel 7** om automatiseringsvenlig lovgivning indleder med en detaljeret gennemgang af, hvordan lovtekster kan udformes til at lette automatiseret retsanvendelse. Under betegnelsen algoritmisk tilgang til lovgivning, behandles vigtige emner som valg af strukturelt koncept (fra fragmentarisk til algoritmisk lovgivning), håndtering af skønsbestemmelser, automatiseringsvenlige begreber og informationer, behovet for relevante kompetencer under det lovforberedende arbejde, samt spørgsmål om AI-venlig lovgivning. Herfra går Schartum videre til at præsentere en retspolitisk tilgang til automatiseret retsanvendelse i **kapitel 8**. Kapitlet præsenterer og drøfter en række udvalgte hensyn, der kan tale for og imod, at en given lovregulering udformes med henblik på automatisering, herunder omkostningseffektivitet, styringseffektivitet, demokratiserende effekter samt skønsanvendelse i forhold til forudberegnelighed og oplevelse af retfærdighed. Der afrundes med en fornuftig opsamling, hvor der peges på behovet for på kvalificeret vis at modvirke digitaliseringens skyggesider; centralisering af magt, øget risici for systemiske fejl og fraværet af retssystemets vekselvirkning mellem induktion og deduktion. Del 3 afsluttes med **kapitel 9,** der går tættere på behovet og mulighederne for at lovregulere automatiseret retsanvendelse. Forfatteren får her slået fast, at en aktiv national lovgivningspolitik er en forudsætning for at give indspil til EU-reguleringen, hvorefter han behandler en række forbundne spørgsmål, herunder om hjemmel for automatisering og datadeling, de forskellige aspekter af åbenhed, dokumentation, mulighed for menneskelig kontrol og kontakt, begrundelse for afgørelser samt klagemuligheder.

> Bogen er et væsentligt – om ikke ligefrem enestående – bidrag til, at retsstaten forbliver robust og relevant i den digitale tidsalder.

I **del 4** om systemudvikling som lovudvikling viser Schartum, hvordan systemudvikling kan anvendes til at etablere en konstruktiv feedback-mekanisme, der kan bidrage til forbedret lovkvalitet. Under den fængende betegnelse regelvask behandles bl.a. betydningen af klarsprog og tydeliggørelse af procedurer, mens forfatteren forklarer, hvordan systemudvikling kan bidrage til at afdække uklarheder og inkonsekvenser i lovtekster.

Om fremstillingen kan det overordnet siges, at forfatterens ambition lykkes, idet hans omfattende viden og erfaring har muliggjort et unikt perspektiv, der forener juridisk teori med praktiske indsigter fra systemudvikling og lovgivningsprocesser. Lovgivning i et digitalt samfunn er således ikke blot en teoretisk øvelse. Bogen er en praktisk guide fyldt med konkrete problembeskrivelser og handlingsorienterede anbefalinger. Navnlig den afbalancerede og ikke-polemiske præsentation af de 19 lovgivningsprincipper kan fremhæves som tydeligt hvilende på en dyb indsigt i digitaliseringens realiteter og på et solidt overblik over eksisterende regulering. Idet Schartum samtidig insisterer på en proaktiv tilgang, hvor lovgivning anvendes som et redskab til aktivt at forme og styre den digitale udvikling, er resultatet både visionært og virkelighedsnært.

Fremstillingen er relevant for praktikere, der arbejder med digitalisering, for forskere inden for retsinformatik og teknologi, samt for studerende, der ønsker at forstå det komplekse og dynamiske felt, hvor jura og digitalisering mødes. Aktører inden for lovforberedende arbejde bør dog være de centrale adressater. I en tid præget af højt tempo, hurtigt skiftende agendaer og tendenser til svækket fordybelse er det denne anmelders ønske, at Lovgivning i et digitalt samfunn betragtes som pligtlæsning for dem, der deltager i og påvirker lovgivningsprocesserne både i Norden og i EU. Baggrunden for dette ønske er, at bogen er et væsentligt – om ikke ligefrem enestående – bidrag til, at retsstaten forbliver robust og relevant i den digitale tidsalder.

Professor i forvaltningsret og digitalisering, ph.d. jur. Hanne Marie Motzfeldt, Juridisk Fakultet, Københavns Universitet.

Skadeståndsansvar vid personuppgiftsbehandling

– En undersökning av skadeståndsansvaret enligt dataskyddsförordningen

Författare: Sandberg Fredrik
Titel: Skadeståndsansvar vid personuppgiftsbehandling – En undersökning av skadeståndsansvaret enligt dataskyddsförordningen
Utgivningsår: 2025
Omfång: 513 sid.
Förlag: Jure
ISBN: 9789172239647
Typ av verk: Akademisk avhandling
Serie: Stockholm Centre for Commercial Law nr. 46

Boken behandlar skadeståndsansvaret och rätten till ersättning enligt EU:s dataskyddsförordning (GDPR). Undersökningen innefattar en utförlig analys av förordningens skadeståndsregler och EU-domstolens praxis med avseende på skadebegrepp, ansvarsförutsättningar, orsakssamband, ersättning och situationer med flera skadevållare. En central fråga i boken är i vilken utsträckning och hur svensk skadeståndsrätt kan tillämpas som komplement till förordningens regler. I avhandlingen uppmärksammas också det nära sambandet mellan skadeståndsreglerna och personuppgiftsansvarets omfattning och innebörd. Med utgångspunkt i komparativ skadeståndsrätt behandlar boken även hur skadeståndsansvaret enligt dataskyddsförordningen förhåller sig till de olika skadeståndsrättsliga traditionerna i medlemsstaterna.

Författaren Fredrik Sandberg är verksam vid Stockholm Centre for Commercial Law, Juridiska fakulteten, Stockholms universitet. Boken är hans doktorsavhandling.

Omtalen er hentet fra: https://www.jure.se/ns/default.asp?url=visatitel.asp?tuid=30260

CompLex 2/25

Forvaltningsorganers adgang til å behandle særlige kategorier av personopplysninger for å hindre algoritmisk diskriminering

Forfatter: Aravindan Balasubramaniam
Oslo: Oslo: Universitetet i Oslo, Juridisk fakultet, Senter for rettsinformatikk 2025, 2/2025. ISSN 2703-8777 Complex (online)

Forfatteren undersøker forvaltningsorganers adgang til å behandle særlige kategorier av personopplysninger for å hindre skjevheter (bias) i KI-systemer. Det hele gjøres gjennom en analyse av likestillings- og diskrimineringsloven, personvernforordningen og KI-forordningen. Fremstillingen er særlig relevant for forvaltningsjurister og -informatikere.

Les hele utgivelsen på CompLex2/25 (pdf)

Omtalen er hentet fra: https://www.jus.uio.no/ifp/forskning/publikasjoner/complex/2025/complex-2-25.html

Delphi

Rebecka Undén

Söktjänsdatabaser under tillsyn

Den svenska integritetsskyddsmyndigheten (”IMY”) inledde i april 2025 tillsyn mot två söktjänster med utgivningsbevis som publicerar uppgifter om lagöverträdelser. Det gäller Legal Newsdesk Sweden AB med hemsidan Lexbase.se samt Fuplex AB med hemsidan krimfup.se. I juni 2025 utvidgade IMY tillsynen genom att inleda granskningar av ytterligare två söktjänster med utgivningsbevis; Upplysning Checknode AB med söktjänsten Upplysning.se och Nusvar AB med söktjänsten Mrkoll.se. Dessa söktjänster tillhandahåller bland annat uppgifter om privatpersoners adresser och personnummer. Tidigare har inte IMY ansett sig behörig att granska databaser med utgivningsbevis, men förra året förklarade sig IMY behörig att inleda tillsyn mot sådana söktjänster mot bakgrund av rättsutvecklingen i såväl europeisk som svensk praxis.

IMY har tagit emot en stor mängd klagomål mot Upplysning.se och Mrkoll.se från registrerade som har begärt att få sina uppgifter borttagna. Söktjänsterna har dock inte upphört med publiceringen av uppgifterna när så begärts. Tillsynen fokuserar på om söktjänsterna agerar i strid med artikel 17.1.c) och 21 i GDPR genom att inte radera personuppgifter när den registrerade begär det.

IMY:s tillsynsskrivelser skickades kort efter att frågan om förhållandet mellan databaser med utgivningsbevis och GDPR ställdes på sin spets i svensk domstol. Högsta domstolen meddelade i februari 2025 beslut i två mål som rörde utlämnande av brottmålsdomar till en nyhetsbyrå och ett bakgrundskontrollsföretag. Besluten slår fast att EU:s dataskyddsförordning, GDPR, kan få betydelse för om det råder sekretess för personuppgifter i brottmålsdomar även på det grundlagsskyddade området.

Kritiserade urvalsmetoder hos Försäkringskassan föremål för tillsyn

IMY har även inlett en granskning av Försäkringskassan för att utreda myndighetens arbete med riskbaserade urval för riktade kontroller mot enskilda. En granskning utförd av organisationen Lighthouse Reports visade att Försäkringskassans AI-metoder för riktade kontroller har missgynnat bland annat kvinnor som ansökt om tillfällig föräldrapenning, så kallad vabersättning (”vård av sjukt barn”). Granskningen ska undersöka om och i så fall hur Försäkringskassan behandlar personuppgifter i samband med riskbaserade urval för riktade kontroller mot enskilda. Tillsynen är ännu i ett tidigt stadium.

Sanktionsavgift för alkoholtester

Ytterligare en nyhet från IMY är att Aktiebolaget Storstockholms Lokaltrafik (”SL”) och Waxholms Ångfartygs AB (även kallat ”Vaxholmsbolaget”), kommunala bolag inom samma koncern, har tilldelats en sanktionsavgift om 75 000 kronor. IMY mottog klagomål från arbetstagare som genomfört alkoholtester inom ramen för sina anställningar och kom fram till att det inte hade varit nödvändigt att samla in och lagra uppgifter från testerna i sådan stor omfattning som SL och Vaxholmsbolaget hade gjort. SL genomförde i genomsnitt två utandningsprov per arbetspass under tio månaders tid. Varje resultat, positivt som negativ, registrerades och lagrades. IMY framhöll att resultatet hade kunnat uppnås med mindre ingripande åtgärder, genom att använda alkolås och att genomföra utredning vid behov – det vill säga, först när ett alkolås förhindrat ett fordons framförande. IMY påminde också om att arbetsgivare som överväger att införa alkoholtester behöver tänka på att resultat från alkoholtester kan indikera att den anställde har ett alkoholmissbruk, vilket utgör en hälsouppgift och därmed är särskild skyddsvärd enligt GDPR.

Rebecka Undén arbetar som Associate på Advokatfirman Delphi.

Gorrissen Federspiel

Tue Goldschmieding

Nyt om persondataret i Danmark

Digitaliseringsstyrelsen modtog alvorlig kritik fra Datatilsynet for mangelfulde sikkerhedsforanstaltninger

Det danske datatilsyn (»Datatilsynet«) har den 24. juni 2025 truffet afgørelse i en sag med journalnummer 2023-442-0197. Sagen vedrørte, om den danske Digitaliseringsstyrelse (»Digitaliseringsstyrelsen«) havde truffet passende tekniske og organisatoriske foranstaltninger inden implementeringen af Næste generations Digital Post (»NgDP«) og systemopdateringen den 23. august 2023.

Datatilsynets afgørelse udsprang af, at Digitaliseringsstyrelsen tidligere havde anmeldt fire tilfælde af brud på persondatasikkerheden til Datatilsynet, som alle udsprang af fejl opstået under overgangen til NgDP. Herudover havde Digitaliseringsstyrelsen offentliggjort driftsopdateringer den 29. august 2023 og den 31. august 2023 på digitaliser.dk, som viste, at der var opstået uhensigtsmæssige ændringer af tilmeldingsstatus for nogle borgere og virksomheder som følge af en ny udgivelse i Digital Post-løsningen den 23. august 2023. Herefter indledte Datatilsynet af egen drift en sag mod Digitaliseringsstyrelsen.

Datatilsynet fandt, at sagen gav anledning til at udtale alvorlig kritik af Digitaliseringsstyrelsen, eftersom de ikke havde behandlet personoplysninger i overensstemmelse med artikel 32, stk. 1 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«). Efter denne bestemmelse skulle den dataansvarlige ved behandlingen af personoplysninger træffe passende tekniske og organisatoriske foranstaltninger for at opretholde et forsvarligt sikkerhedsniveau.

Datatilsynet lagde ved sin afgørelse vægt på, at NgDP var kommunikationskanalen mellem myndigheder, borgere og virksomheder, hvor der blev behandlet mange personoplysninger, ligesom modtagelse og afsendelse af meddelelser kunne medføre retsvirkninger. Af den årsag kunne fejl samt utilstrækkelige sikkerhedsforanstaltninger medføre alvorlige konsekvenser for de registrerede og deres rettigheder.

Læs afgørelsen fra Datatilsynet her: Digitaliseringsstyrelsen får alvorlig kritik for mangelfulde sikkerhedsforanstaltninger

Datatilsynet igangsætter tilsyn om retten til sletning

Det danske datatilsyn (»Datatilsynet«) offentliggjorde den 25. april 2025, at de igangsatte en række tilsyn med private dataansvarlige for at efterprøve, om reglerne vedrørende sletning af personoplysninger blev efterlevet i virksomheder, der tilbød onlinekasino. Tilsynene var en del af Det Europæiske Databeskyttelsesråds (»EDPB«) årlige koordinerede undersøgelse.

Baggrunden for, at tilsynene primært beskæftigede sig med sletning af personoplysninger i virksomheder inden for onlinekasino, var, at behandlingen af personoplysninger medførte en betydelig risiko for de registreredes rettigheder og frihedsrettigheder. Derudover var der en stigende tendens i benyttelsen af onlinekasino.

Tilsynene havde til formål at tegne et billede af virksomhedernes efterlevelse af reglerne om sletning af personoplysninger samt potentielle udfordringer i den forbindelse.

Læs Datatilsynets pressemeddelelse her: Datatilsynet igangsætter tilsyn om retten til sletning

Datatilsynet godkender ansigtsgenkendelse til fodboldlandskampe i Parken

Det danske datatilsyn (»Datatilsynet«) offentliggjorde den 28. april 2025, at Datatilsynet meddelte F.C. København og Dansk Boldspil-Union tilladelse til behandling af biometrisk data efter den danske databeskyttelseslov, jf. lovbekendtgørelse nr. 289 af 8. marts 2024 (»databeskyttelsesloven«) § 7, stk. 4 hvorefter følsomme oplysninger kan behandles, når dette er nødvendigt af hensyn til væsentlige samfundsinteresser, ved at anvende automatisk ansigtsgenkendelse i forbindelse med afholdelse af herrefodboldslandskampe i Parken.

Der gælder et forbud mod behandlingen af biometrisk data i GDPR artikel 9, stk. 1. Efter databeskyttelseslovens § 7, stk. 4 skal Datatilsynet meddele tilladelse til behandlingen af biometrisk data, når behandlingen sker af andre end offentlige myndigheder.

I december 2024 fik F.C. København tilladelse til at gøre brug af automatisk ansigtsgenkendelse. Tilladelsen gjaldt dog kun klubbens kampe og ikke øvrige arrangementer.

Som noget nyt fik også Dansk Boldspil-Union tilladelse til at anvende ansigtsgenkendelse. Tilladelsen til Dansk Boldspil-Union blev givet, da de i fællesskab med F.C. København var dataansvarlige for håndteringen af personoplysninger, når fodboldlandskampe foregik i Parken. Tilladelsen blev givet under forudsætning af, at F.C. København og Dansk Boldspil-Union forud for behandlingen skulle foretage en konsekvensanalyse.

Formålet med tilladelsen var at håndhæve regler om klubkarantæner og generelle karantæner som følge af fodboldkampe.

Læs Datatilsynets pressemeddelelse her: Datatilsynet godkender ansigtsgenkendelse til fodboldlandskampe i Parken

Datatilsynet og Digitaliseringsstyrelsen udgiver en fælles vejledning

Det danske datatilsyn (»Datatilsynet«) og den danske Digitaliseringsstyrelse (»Digitaliseringsstyrelsen«) offentliggjorde den 15. maj 2025, at de i fællesskab har lavet vejledningen »Brug af cookies og lignende teknologier« og et tillæg tiltænkt organisationer, der gør brug af cookies eller lignende teknologier.

Udarbejdelsen af vejledningen skete med henblik på at hjælpe disse organisationer med at overholde gældende lovgivning vedrørende cookies og databeskyttelse. I mange tilfælde finder den danske bekendtgørelse nr. 1148 af 9. december 2011 (»Bekendtgørelse om krav til information og samtykke ved lagring af eller adgang til oplysninger i slutbrugeres terminaludstyr«) og databeskyttelsesreglerne anvendelse sideløbende. Vejledningen skulle derfor hjælpe organisationerne med at sondre mellem reglerne og danne en ensartet forståelse, som muliggjorde en smidig implementering af en lovlig samtykkeløsning.

For at opfylde formålet, indeholder vejledningen blandt andet en gennemgang af de vigtigste regler i Bekendtgørelse om krav til information og samtykke ved lagring af eller adgang til oplysninger i slutbrugeres terminaludstyr og GDPR, praktiske råd, eksempler, samt en gennemgang af potentielle vanskeligheder.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/maj/datatilsynet-og-digitaliseringsstyrelsen-udgiver-en-faelles-vejledning

Læs Datatilsynets vejledning her: https://www.datatilsynet.dk/Media/638829899950476628/F%C3%A6llesvejledning%20med%20DIGST%20-%20Cookie%20og%20lignende%20teknologier.pdf

Opdatering af vejledning om håndtering af brud

Det danske datatilsyn (»Datatilsynet«) offentliggjorde den 20. maj 2025, at vejledningen om håndtering af brud på persondatasikkerheden var blevet opdateret.

I sommeren 2024 udvidede Datatilsynet den første del af vejledningen, hvor de i den forbindelse tilføjede eksempler på tilfælde med brud på persondatasikkerheden.

Den resterende del opdaterede Datatilsynet for nyligt. Det drejede sig om afsnit vedrørende anmeldelse til Datatilsynet samt om underretning af de(n) registrerede. Den nye opdatering dækkede både over indhold, layout, eksempler og henvisninger.

Læs Datatilsynets pressemeddelelse her: Opdatering af vejledning om håndtering af brud

Læs Datatilsynets vejledning her: Håndtering af brud på persondatasikkerheden.pdf

Fælles erklæring fra de nordiske datatilsyns møde i Thorshavn

Det danske datatilsyn (»Datatilsynet«) offentliggjorde den 26. maj 2025 detaljer fra det årlige nordiske møde i Thorshavn mellem datatilsynene i de nordiske lande, hvor det danske og færøske datatilsyn var værter.

Mødets primære formål var erfaringsudveksling og koordinering på tværs af de nordiske lande. Fokus var på brugen af kunstig intelligens i retshåndhævelse samt effektiviseringen af sagsbehandling, It-sikkerhed og håndtering af sikkerhedsbrud. Der blev også diskuteret behovet for klare mandater og ressourcer til at håndtere komplekse databeskyttelsesspørgsmål og deling af erfaringer om behandlingen af børn og unges personoplysninger.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/internationalt/internationalt-nyt/2025/maj/nordiske-datatilsyn-vedtager-faelles-erklaering-om-kunstig-intelligens-og-it-sikkerhed

Nye foranstaltninger skal styrke sikkerheden i it-systemer hos Datatilsynet

Det danske datatilsyn (»Datatilsynet«) offentliggjorde den 28. maj 2025, at de tilføjede to nye foranstaltninger med henblik på forebyggelse af brud på sikkerhed i tilfælde af hacking.

Udvidelsen af foranstaltninger udsprang af en stigning i antallet af sikkerhedsbrud forårsaget af hacking. En sikkerhedskonsulent hos Datatilsynet bemærkede, at mange af de sikkerhedsbrud, som Datatilsynet modtog, kunne have været undgået, hvis de netop tilføjede foranstaltninger var blevet fulgt. På den baggrund tilføjede Datatilsynet foranstaltningerne »Sikkerhedsmæssig styring og vedligeholdelse af software« og »Netværkssegmentering« til deres foranstaltningskatalog.

»Sikkerhedsmæssig styring og vedligeholdelse af software« er en forebyggende foranstaltning, der skal beskytte imod ondsindet brug af software ved dels at vedligeholde softwaren sikkerhedsmæssigt samt isolere softwaren i størst muligt omfang.

»Netværkssegmentering« opdeler et netværk i flere isolerede segmenter og begrænser i højere grad kommunikation med andre dele af netværkets segmenter. På den måde mindskes risikoen for, at et sikkerhedsbrud i et segment påvirker et andet segment med følsomt og beskyttelsesværdigt data.

Læs pressemeddelelsen fra Datatilsynet her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/maj/nye-foranstaltninger-skal-styrke-sikkerheden-i-it-systemer

Læs om foranstaltningen »Sikkerhedsmæssig« styring og vedligehold af software her: Sikkerhedsmæssig styring og vedligehold af software

Læs om foranstaltningen »Netværkssegmentering« her: Netværkssegmentering

Illustrasjon: Colourbox.com

Udvidet DPO-side med praksisnær viden

Det danske datatilsyn (»Datatilsynet«) offentliggjorde den 17. juni 2025 en opdatering vedrørende deres side om databeskyttelsesrådgivere (»DPO'er«), som både var tiltænkt nye DPO'er og DPO'er med erfaring.

Den nye opdatering gav et overblik over DPO'ens rolle og opgaver. Formålet med opdateringen af DPO-siden var at gøre information, inspiration og støtte mere tilgængeligt for DPO'er i deres daglige arbejde.

Som noget nyt gav DPO-siden adgang til videopodcast, hvor DPO'er delte erfaringer og indsigt, FAQ, som gav svar på de mest almindelige spørgsmål, gode råd samt vejledninger og links.

Læs pressemeddelelsen fra Datatilsynet her: Udvidet DPO-side med praksisnær viden

Datatilsynet og Digitaliseringsstyrelsen har udvalgt to AI-projekter til anden runde af den regulatoriske sandkasse

Det danske datatilsyn (»Datatilsynet«) offentliggjorde den 18. juni 2025 hvilke to AI-projekter, som Datatilsynet og den danske Digitaliseringsstyrelse (»Digitaliseringsstyrelsen«) havde udvalgt til andet forløb af den regulatoriske sandkasse.

Af meddelelsen fremgår, at der i alt var 18 ansøgninger. Blandt disse ansøgninger blev Børns Vilkår og BrainCapture udvalgt.

Projektet hos Børns Vilkår gik ud på at udvikle en barnesimulator, som kunne anvendes til at øve svære samtaler med børn og en coachboat, som gav feedback på en sådan samtale med barnesimulatoren.

Projektet hos BrainCapture gik ud på at fremstille en AI-løsning, der kunne fortolke EEG-målinger og klassificere disse i normale og abnormale målinger. Dette ville give patienter mulighed for en hurtigere og mere smidig diagnosticering af neurologiske lidelser.

Datatilsynet og Digitaliseringsstyrelsen lagde ved sit valg af projekter særligt vægt på, at den viden, som opstod i samarbejde med den udvalgte virksomhed eller myndighed, skulle resultere i mest mulig værdi for andre aktører og samfundet.

Læs pressemeddelelsen fra Datatilsynet her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/jun/to-ai-projekter-udvalgt-til-anden-runde-af-den-regulatoriske-sandkasse

Datatilsynet har offentliggjort deres årsberetning for 2024

Det danske datatilsyn (»Datatilsynet«) offentliggjorde den 26. juni 2025 deres årsberetning for 2024. Årsberetningen belyste centrale indsatser fra Datatilsynet som fandt sted i året.

Årsberetningen præsenterede Datatilsynets arbejde inden for områderne Rådgivning og vejledning, Høring over lovforslag, Tilsyn, Anmeldelser af brud på persondatasikkerheden, Tilladelser, Internationalt arbejde og Om Datatilsynet. I årsberetningen fremgik blandt andet Datatilsynets nye vejledninger og opdateret praksis fra 2024, Datatilsynets særlige fokus på tilsyn med brugen af kunstig intelligens, samt Datatilsynets generelle fokus på rådgivning og understøttelse af borgere og dataansvarlige.

Læs pressemeddelelsen fra Datatilsynet her: Datatilsynets årsberetning 2024 er offentliggjort

Læs årsberetningen fra Datatilsynet her: Datatilsynets årsberetning 2024.pdf

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

Gorrissen Federspiel

Tue Goldschmieding

Patenttvist om fremstilling og distribution af biosimilære lægemidler medførte ikke, at forbud eller påbud kunne nedlægges.

Østre Landsret afsagde den 10. april 2025 kendelse i en kæresag BS-38675/2024-OLR vedrørende Janssen Biotech, Inc's (»Janssen«) påstand om forbud og påbud mod Samsung Bioepis NL B.V. (»Samsung«) og AGC Biologics A/S (»AGC«).

Sagen angik, om Samsung's og AGC's fremstilling og distribution af en biosimilær udgave af det biologiske lægemiddel »ustekinumab« indebar en krænkelse af Janssens patent DK/EP 3 883 606 og brugsmodel DK 2023 00038. Ifølge Janssen forelå der en direkte patentkrænkelse i strid med den danske patentlovs § 3, stk. 1, nr. 1, jf. lovbekendtgørelse nr. 90 af 29. januar 2019 (»patentloven«), om patentindehaverens eneret til den pågældende opfindelse, idet patentet var et såkaldt anvendelsesbegrænset produktkrav, jf. Den Europæiske Patentkonventions artikel 54, stk. 5, der svarer til patentlovens § 2, stk. 5.

Samsung og AGC bestred krænkelserne og gjorde gældende, at patentet var ugyldigt grundet manglende opfindelseshøjde, jf. patentlovens § 2, som kræver, at en opfindelse er ny og væsentlig forskellig fra det allerede kendte. De anførte desuden, at Janssen ikke havde sandsynliggjort et øjeblikkeligt behov for et forbud eller påbud.

Sagen var tidligere blevet behandlet ved Sø- og Handelsretten under sagsnummeret BS-10043/2024-SHR, trykt i U.2024.4786, hvor Janssen ikke fik medhold, da retten ikke fandt behovet for indgriben tilstrækkeligt sandsynliggjort.

I ankesagen fandt Østre Landsret, at Janssens dokumentation ikke berettigede et hastende forbud eller påbud, og at påstandene var for ubestemte og potentielt for vidtgående. Landsretten stadfæstede derfor, at der ikke kunne meddeles midlertidigt forbud eller påbud, og Janssen blev pålagt at betale 3.000.000 kr. i sagsomkostninger.

Kendelsen blev kæret til Højesteret, og Procesbevillingsnævnet gav den 27. juni 2025 tilladelse til, at sagen kunne ankes til Højesteret.

Læs kendelsen fra Østre Landsret her: Ø.L.K. 10. april 2025 i kære 10. afd. BS-38675/2024-OLR Ø.L.K. 10. april 2025 i kære 10. afd. BS-38675/2024-OLR | Karnov Group

Sø- og Handelsretten godkender retten til ordmærket »Comeback« ved ibrugtagning

Sø- og Handelsretten afsagde den 25. april 2025 dom i sag BS-2099/2025-SHR mellem Comeback Camp ApS (»Comeback«) og Komeback ApS ("Komeback") om en påstået krænkelse af Comebacks rettigheder efter den danske varemærkelov, jf. lovbekendtgørelse nr. 88 af 29. januar 2019 (»varemærkeloven«) og den danske markedsføringslov jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«).

Comeback havde siden 2010 benyttet ordet »Comeback« i sociale og rådgivende aktiviteter for unge. Komeback, der blev registreret i 2024, anvendte betegnelsen »Komeback« til en social virksomhed med støtte til unge.

Comeback gjorde gældende, at Komebacks næsten identiske navn medførte en forvekslingsrisiko i strid med § 22 i markedsføringsloven, hvorefter erhvervsdrivende ikke må benytte kendetegn på en måde, der er egnet til at fremkalde forveksling med andre, og at Komeback derved krænkede Comebacks etablerede varemærke.

Retten fandt, at »Comeback« havde det fornødne særpræg som varemærke efter § 1 a, § 2, § 3, stk. 3 og § 13 i varemærkeloven for brug i Nice-klasse 25 (beklædning m.v.), og at der var stiftet varemærket ved ibrugtagning, jf. varemærkelovens § 3, stk. 1, nr. 3. Ved at anvende et navn med samme betydning samt visuel og fonetisk lighed krænkede Komeback disse rettigheder. Retten nedlagde forbud, jf. § 413 i den danske retsplejelov, jf. lovbekendtgørelse nr. 1160 af 5. november 2024, mod Komebacks fortsatte brug af »Komeback«, og pålagde Komeback at betale 120.750 kr. i sagsomkostninger.

Læs dommen fra Sø- og Handelsretten her: Domsoversigt BS-2099/2025-SHR

Rettighedsoverdragelse af design til vinreoler ved tvangsauktion var ugyldig

Sø- og Handelsretten afsagde den 29. april 2025 dom i en sag mellem W&B A/S (»W&B«) og Moldow Furniture Design Unipessoal LDA (»Moldow Design«) der vedrørte en tvist om gyldigheden af overdragelsen af designrettighederne til vinreoler. Sagen blev behandlet under sagsnummer Sag BS-39795/2023-SHR.

W&B gjorde gældende, at de ved en tvangsauktion den 22. november

2022 blev ejer af ni designrettigheder registreret hos EUIPO, som oprindeligt havde tilhørt Christian Moldow. Designrettighederne blev solgt til direktøren for W&B for 5.000 kr. ved en tvangsauktion, som blev forestået af W&B's egen advokat på advokatens kontor i København. Auktionen blev gennemført på baggrund af et udlæg i rettighederne foretaget af fogedretten på Frederiksberg. Moldow Design bestred, at W&B havde erhvervet ejendomsretten til designrettighederne og rejste indsigelser mod det udlæg, der var foretaget af fogedretten på Frederiksberg, samt den afholdte tvangsauktion.

Retten fandt, at tvangsauktionen ikke blev korrekt gennemført, da W&B's advokat ikke var godkendt til at forestå auktionen, og den blev afholdt uden for den relevante retskreds. Retten fastslog herefter, at W&B ikke kunne håndhæve de designrettigheder, der blev erhvervet gennem tvangsauktionen, og forbød W&B at producere, markedsføre, og sælge de omhandlede produkter.

Moldow Design kunne derimod som registreret indehaver påtale andres erhvervsmæssige brug af designene, og retten fandt, at W&B's markedsføring af reolprodukterne var i strid med god markedsføringsskik jf. § 3 i den danske lov om markedsføring jf. lovbekendtgørelse nr. 1420 af 2. december 2024.

Læs Sø- og Handelsrettens afgørelse her: Dom__BS-39795-2023-SHR.pdf

Erstatning for salgs-forbud baseret på patentrettigheder der viste sig ikke at bestå

Den 12. maj 2025 afsagde Sø- og Handelsretten dom i en sag om erstatning for tab forårsaget af et midlertidigt forbud mod salg og markedsføring af lægemidlet Copemyl 40 mg/ml. Sagsøger i sagen var Mylan AB, og de sagsøgte var Teva Pharmaceutical Industries Ltd. og TEVA DENMARK A/S (»Teva«). Sagen blev afsagt under sagsnummer BS-44706/2021-SHR.

Det midlertidige forbud blev nedlagt den 15. marts 2019 og forhindrede Mylan AB i at sælge og markedsføre Copemyl 40 mg/ml, som anvendes til behandling af patienter med attakvis multipel sklerose. Teva markedsførte et tilsvarende lægemiddel, Copaxone 40 mg/ml, som også indeholdt det aktive stof glatirameracetat (GA) mod multipel sklerose. Forbuddet var i kraft fra 25. marts 2019 og frem til 23. august 2021, hvor Sø- og Handelsretten ophævede det.

Det midlertidige forbud mod Mylan AB var baseret på patenterne DK/EP 2 949 335, DK/EP 2 630 962 og DK/EP 3 199 172, som viste sig ikke at bestå. De tre patenter blev, i perioden september 2020 til februar 2024, kendt ugyldige af Den Europæiske Patentmyndighed (»Technical Board of Appeal«). Patenterne blev ugyldiggjort med virkning ex tunc, jf. § 80 og § 55 a i den danske patentlov, jf. lovbekendtgørelse nr. 90 af 29. januar 2019.

Da patentrettighederne aldrig havde bestået, og derfor aldrig retsmæssigt havde kunnet danne grundlaget for forbuddet, forelå der et objektivt ansvarsgrundlag for Teva, jf. den danske retsplejelov, jf. lovbekendtgørelse nr. 1160 af 5. november 2024 § 428, stk. 1.

Sø- og Handelsretten udtalte at Teva skulle betale 29.976.930,90 kr. i erstatning til Mylan AB.

Læs dommen fra Sø- og Handelsretten her: Dom_BS-44706-2021-SHR.pdf

Udbyder af uddannelser havde ikke handlet ulovligt eller i strid med forlig om ikke at udbyde en masteruddannelse

Sø- og Handelsretten afsagde den 14. maj 2025 kendelse i sag BS-3959/2025-SHR mellem Copenhagen Coaching Center ApS (»CC«) og Dialogakademiet ApS (»DA«). Sagen var en midlertidig forbuds- og påbudssag, der navnlig angik, hvorvidt DA ved at udbyde en masteruddannelse havde handlet i strid med god markedsføringsskik, jf. § 3 i den danske lov om markedsføring jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«) og § 4 i den danske lov om forretningshemmeligheder, jf. lov nr. 309 af 25. april 2018 (»lov om forretningshemmeligheder«) om uretmæssig erhvervelse og brug af forretningshemmeligheder, eller et forlig indgået med CC.

Parterne havde indgået et forlig, hvor det blev aftalt, at DA ville undlade at udbyde og markedsføre en masteruddannelse, samt undlade at udbyde en masteruddannelse, der var identisk med CC's uddannelse »Master of Business Coaching«.

I forhold til markedsføringsloven og lov om forretningshemmeligheder fandt retten, at det ikke var muligt at fastlægge CC's koncept med den fornødne bestemthed. Det var derfor ikke sandsynliggjort, at CC havde rettigheder efter markedsføringsloven eller lov om forretningshemmeligheder, hvorfor betingelserne for nedlæggelse af forbud og påbud ikke var opfyldt. Retten fandt yderligere, at det ikke var sandsynliggjort, at DA havde udbudt og markedsført en masteruddannelse i strid med forliget med CC. CC's påstande blev afvist på baggrund af manglende klarhed og præcision, og DA blev derfor frifundet.

Læs Sø- og Handelsrettens kendelse her: Kendelse_-_BS-3959-2025-SHR.pdf

Konkurrent til Soundboks forbydes i Danmark

Sø- og Handelsretten afsagde den 28. maj 2025 kendelse i sagen mellem Soundboks ApS (»Soundboks«) og Sharp Consumer Electronics Poland Sp. z.o.o. (»Sharp«). Sagen blev behandlet under sagsnummer BS-18546/2024-SHR.

Soundboks, der producerer festhøjtalere, sagsøgte Sharp med påstand om, at Sharps højtalere ved navn »Sumobox« og »Sumobox Pro« krænkede Soundboks' rettig-

heder i henhold til den danske ophavsretslov jf. lovbekendtgørelse nr. 1093 af 20. august 2023, den danske lov om markedsføring jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«) og den danske varemærkelov jf. lovbekendtgørelse nr. 88 af 29. januar 2019.

Retten afviste ophavsretlig beskyttelse af Soundboks' højtalere, idet der ikke var tilstrækkeligt grundlag for at fastslå, at højtalerne udgjorde et værk af brugskunst.

Retten vurderede dog, at Soundboks' højttalere nød markedsføringsretlig beskyttelse mod produktefterligning efter markedsføringslovens § 3, stk. 1, om god markedsføringsskik. Retten fandt, at Sumobox fremstod som en nærgående efterligning af Soundboks, henset til lighederne i dimensioner, silhuet og farve. Retten fandt, at Sumobox lignede Soundboks i en sådan grad, at det medførte en utilbørlig udnyttelse af det velkendte varemærke, Soundboks' særpræg og renommé. Retten vurderede derfor, at Sharp ved markedsføringen af Sumobox havde overtrådt god markedsføringsskik ved utilbørlig snyltning på Soundboks' markedsposition, jf. markedsføringslovens § 3, stk. 1.

Soundboks blev tilkendt erstatning og vederlag for markedsforstyrrelse på 100.000 kr. Retten nedlagde overfor Sharp forbud mod at eksportere, markedsføre og sælge Sumobox i Danmark. Sharp blev ligeledes forbudt at anvende Sumobox som varemærke for højtalere i Danmark, og modtog påbud om at tilbagekalde alt fysisk markedsføringsmateriale i Danmark.

Læs Sø- og Handelsrettens afgørelse her: Dom_BS-18546-2024-SHR.pdf

»Quick Shoes« krænkede designrettighederne til fire af Skechers EU-designs

Sø- og Handelsretten afsagde den 24. juni 2025 dom i sagen BS-43094/2024-SHR, hvor CV Padel & Sport ApS og A, som solgte og markedsførte skoene Quick Shoes, blev anklaget for at krænke designrettighederne til Skechers U.S.A Inc. og Skechers U.S.A Inc. II's (»Skechers«) EU-designs og for at overtræde den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«).

Retten vurderede først, om Quick Shoes krænkede Skechers' gyldige EU-designs nr. 1-10. Skechers' designrettigheder beskytter ethvert design, der ikke giver den informerede bruger et andet helhedsindtryk, jf. artikel 10 i Rådets forordning (EF) nr. 6/2002 af 12. december 2001 om EF-design. Retten fandt, at Quick Shoes krænkede Skechers' EU-design nr. 1, 4, 5 og 6, idet designene fremstod ens og derfor ikke gav den informerede bruger et andet helhedsindtryk.

Herefter vurderede retten, om Quick Shoes udgjorde en nærgående efterligning af Skechers' Slip-Ins sko i henhold til markedsføringslovens § 3 om god markedsføringsskik og § 4 om god erhvervsskik. Retten fandt, at mønsteret på hælkappen udgjorde en væsentlig forskel mellem de to sko, og efter en helhedsvurdering konkluderede retten, at der ikke var tale om en nærgående efterligning.

Retten fulgte sagsøgers påstand om destruktion og pålagde de sagsøgte at betale 150.000 kr. i vederlag og erstatning for designkrænkelser, jf. § 37 og § 38 i den danske lov om design, jf. lovbekendtgørelse nr. 89 af 29. januar 2019.

Læs dommen fra Østre Landsret her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_-_BS-43094-2024-SHR.pdf

Virksomhed kunne lovligt anvende udsagn om en nærmere specificeret procentsats af genanvendt materiale i deres markedsføring

En virksomhed anmodede den danske forbrugerombudsmand (»Forbrugerombudsmanden«) om at vurdere lovligheden af anvendelsen af udsagnene »Overdel og ydersål: 8 % genanvendt gummi. Foring på indersål og overdel: 100 % genanvendt polyester«. Forbrugerombudsmanden tog stilling til sagen og traf afgørelse den 2. april 2025 under sagsnummeret 25/03389.

Forbrugerombudsmanden vurderede, at ordet »genanvendt« kun kunne bruges, når der var tale om post-forbruger affald.

Forbrugerombudsmanden udtalte, at udsagnene ikke ville være vildledende, hvis virksomheden kunne dokumentere dem, og såfremt de fordele, som udsagnene beskrev, ikke var sædvanlige for tilsvarende produkter. Endvidere blev det understreget, at markedsføring ikke måtte give et vildledende indtryk af, hvor stor en del af produktet der var genanvendt. Forbrugerombudsmanden lagde vægt på, at udsagnene var konkrete og benyttede specifikke procentsatser. Virksomheden kunne således anvende udsagnene uden at overtræde vildledningsforbuddet i den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 § 5 om vildledende handlinger og § 6 om vildledende udeladelser.

Forbrugerombudsmanden anbefalede, at det var produktets samlede procentsats af genanvendt materiale, der burde fremgå af markedsføringen.

Læs Forbrugerombudsmandens afgørelse her: En virksomhed kunne lovligt anvende udsagn om en nærmere specificeret procentsats af genanvendt materiale i deres markedsføring

Grøn Elforsyning betaler bøde på 700.000 kroner for ulovligt telefonsalg og vildledning af forbrugere

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 2. april 2025, at Grøn Elforsyning havde accepteret at betale en bøde på 700.000 kr. for brud på vildledningsforbuddet i den

danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«) § 5 om vildledende handlinger og § 6 om vildledende udeladelser. Grøn Elforsyning blev politianmeldt for uanmodet at have kontaktet forbrugere og for vildledende oplysninger under telefonsamtaler, hvilket inkluderede urealistiske løfter om besparelser, som ikke kunne garanteres uden kendskab til forbrugerens nuværende el-aftale.

Forbrugerombudsmanden vurderede, at Grøn Elforsyning, ved at kontakte forbrugerne uden samtykke, handlede i strid med § 4, stk. 1 i den danske lov om forbrugeraftaler, jf. lov nr. 1457 af 17. december 2013, og leverede urigtige oplysninger under telefonsamtalerne, hvor sælgere præsenterede sig som værende fra »Grøn Energi« eller »Grøn El« i stedet for Grøn Elforsyning. På den baggrund vurderede Forbrugerombudsmanden at Grøn Elforsyning havde handlet i strid med vildledningsforbuddet i markedsføringslovens § 5 og § 6 sammenholdt med § 8, der fokuserer på handelspraksissens evne til at påvirke forbrugerens økonomiske adfærd.

Forbrugerombudsmanden bemærkede endvidere, at aftaler indgået uden samtykke til opringning fra el-selskabet er ugyldige.

Læs Forbrugerombudsmandens pressemeddelelse her: Grøn Elforsyning betaler bøde på 700.000 kroner for ulovligt telefonsalg og vildledning af forbrugerne

Forbrugerombudsmanden politianmelder Ikano Bank for vildledende markedsføring

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) har den 3. april 2025 politianmeldt Ikano Bank.

Politianmeldelsen sker på baggrund af en mulig overtrædelse af den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«) § 5 og § 6, som omhandler vildledningsforbuddet og § 18 vedrørende standardoplysningspligt i forbindelse med markedsføring af lån til forbrugere.

Kunder hos IKEA, som havde et IKEA Shoppingkort, modtog den 1. februar 2023 et kampagnebrev med oplysninger om, at kunderne kunne få deres tilbageværende kredit på deres IKEA Shoppingkort udbetalt til deres NemKonto. Efter Forbrugerombudsmandens opfattelse gav kampagnebrevet forbrugerne anledning til at tro, at der dels var tale om et tilgodehavende, og dels at overførslen til deres konti var helt gratis.

Nye kunder fik desuden tilbud om kreditter på op imod 130.000 kr. Ikano Bank havde i sin markedsføring på IKEAs hjemmeside anført »Ansøg om at få op til 130.000, - i kredit uden renter og gebyrer*. Årlig rente: 0 %. Månedsgebyr: 0, -*« Få steder på hjemmesiden fremgik det med lille skrift, at køb foretaget med IKEA Shoppingkortet efter de første 60 dage ville blive pålagt en variabel rente på 14,5 %, og at lånet kun kunne tilbagebetales med en løsning via iBox, hvis forbrugeren ikke skulle opkræves et betalingsgebyr.

Forbrugerombudsmanden fandt på den baggrund, at forbrugerne i begge tilfælde kunne opfatte ydelsen som vederlagsfri, selv om kreditten medførte omkostninger. Forbrugerombudsmanden fandt, at markedsføringslovens § 5, § 6 og § 18 var tilsidesat, hvorfor Forbrugerombudsmanden indgav en politianmeldelse.

Læs Forbrugerombudsmandens pressemeddelelse her: Forbrugerombudsmanden politianmelder Ikano Bank for vildledende markedsføring

Lovlighed af udsagn til brug for markedsføring af et kombinationsprodukt bestående af 50 % kød og 50% grønt

Den 29. april 2025 udtalte den danske forbrugerombudsmand (»Forbrugerombudsmanden«) sig i en sag vedrørende lovligheden af et udsagn, som en virksomhed brugte til markedsføring af et produkt bestående af 50% kød og 50% grønt. Afgørelsen blev truffet med sagsnummer 25/03203. Virksomheden havde anmodet Forbrugerombudsmanden om en bindende forhåndsbesked, og spørgsmålet i sagen var derfor, om udsagnet »48 % mindre CO_2 end 500 gram af 100 % hakket oksekød fra dansk kalv og malkekvæg« var lovligt i forbindelse med markedsføring.

Virksomheden havde anvendt LCA-modellen til beregningen af CO2-udledningen. I forhåndsbeskeden redegjorde virksomheden for LCA-modellen, herunder at modellen var i overensstemmelse med internationale ISO-standarder, og at uafhængige reviewteams havde godkendt modellen.

Forbrugerombudsmanden fandt, under henvisning til vildledningsbestemmelserne i den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«) § 5 og § 6, og dokumentationskravet i markedsføringslovens § 13, at udsagnet var lovligt.

I den forbindelse lagde Forbrugerombudsmanden til grund, at virksomhedens beregninger af CO2-udledningen for de to produkter var korrekte, ligesom beregningerne af CO2-udledningen for de to produkter både var sammenlignelige og relevante sammenligninger.

Læs Forbrugerombudsmandens afgørelse her: En virksomhed kunne lovligt bruge udsagnet "48 % mindre CO2 end 500 gram af 100 % hakket oksekød fra dansk kalv og malkekvæg" i markedsføringen af et fødevareprodukt

Forbrugerombudsmanden indskærpede vildledningsforbud over for Velkommen

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 7. maj 2025 at

elselskabet Velkommen havde givet vildledende oplysninger om selskabets elpriser. Det fremgik af Velkommens hjemmeside, at forbrugerne fik en elaftale med variabel elpris pr. kWh gennem et abonnement til 1 krone pr. måned. Det var dog ikke oplyst med samme synlighed, at Velkommens pris indeholdt flere tillæg, herunder et spottillæg på 0,04 kr. pr. kWh, et tillæg på 0,15 kr. pr. kWh for grøn kompensation, samt et tillæg for transport og afgifter.

Oplysningerne om tillæggene fremgik ikke tydeligt og var spredt forskellige steder på hjemmesiden. De havde ikke samme synlighed som det fremhævede abonnement til 1 krone. Forbrugerombudsmanden vurderede, at Velkommens oplysninger var egnede til at vildlede forbrugeren og derfor indskærpede Forbrugerombudsmanden vildledningsforbuddet i § 5 i den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«) overfor Velkommen.

Forbrugerombudsmanden fandt desuden, at Velkommen havde tilsidesat sin oplysningspligt, idet selskabet ikke tydeligt på hjemmesiden oplyste den samlede pris eller forklaringen på, hvordan prisen blev udregnet. Hertil havde en klager haft en telefonsamtale med Velkommen, hvor sælgeren ikke nævnte spottillægget eller tillægget for grøn kompensation. De manglende oplysninger om den samlede pris og dens udregning var i strid med § 8, stk. 1, nr. 6 og 7, jf. § 11, stk. 2 i den danske lov om forbrugeraftaler, jf. lov nr. 1457 af 17. december 2023. Forbrugerombudsmanden vurderede endvidere, at tilsidesættelsen af oplysningspligten medførte en manglende overholdelse af markedsføringslovens § 3, stk. 1 om god markedsføringsskik.

Læs Forbrugerombudsmandens pressemeddelelse her: Forbrugerombudsmanden indskærper markedsføringslovens vildledningsforbud over for Velkommen

E-mails med invitationer til en lederkonference var i strid med spamforbuddet

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) modtog 25 klager vedrørende uanmodede e-mails om en lederkonference og traf afgørelse i sagen den 20. maj 2025 under sagsnummeret 24/07461.

Forbrugerombudsmanden vurderede, at de 25 uanmodede e-mails var sendt af et dansk og engelsk selskab i forening. Disse e-mails indeholdt et tilbud om gratis billetter til konferencen for modtageren og en kollega. De to selskaber havde ikke dokumentation for, at de havde indhentet gyldigt markedsføringssamtykke fra klagerne, og Forbrugerombudsmanden fandt derfor, at de havde overtrådt spamforbuddet i § 10, stk. 1 i den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024.

Forbrugerombudsmanden understregede, at spamforbuddet gælder for alle modtagere, herunder henvendelser til generelle postkasser uden personlig modtager samt offentligt tilgængelige mailadresser.

Læs Forbrugerombudsmandens afgørelse her: E-mails med invitationer til en lederkonference var i strid med spamforbuddet

Virksomhed kunne ikke lovligt benytte udsagnet »klimavenlig« baseret på klimakompensation

En virksomhed havde anmodet den danske forbrugerombudsmand (»Forbrugerombudsmanden«) om at tage stilling til virksomhedens klimaudsagn. Forbrugerombudsmanden traf afgørelse den 20. maj 2025 under sagsnummer 25/04484.

Virksomhedens klimaudsagn drejede sig om et klistermærke med udsagnet »klimavenlig salon« til anvendelse i virksomhedens saloner. Klimaklistermærket skulle opsættes i saloner, som gennem træplantning havde fået kompenseret deres forbrug af strøm, varme og varmt vand.

Forbrugerombudsmanden udtalte, at det var en væsentlig oplysning for forbrugeren, om klimafortrinnet ved et produkt skyldes klimakompensation, og at udsagnet på denne baggrund ville være vildledende, hvis det ikke i umiddelbar tilknytning til udsagnet blev oplyst, at klimafordelen skete gennem klimakompensation. Uden oplysning om kompensation, ville forbrugeren fejlagtigt kunne tro, at der var sket en CO_2-reduktion kun ved produktet eller ydelsen.

Da virksomhedens klimaklistermærke ikke oplyste om kompensationen i umiddelbar tilknytning til klimaudsagnet, vurderede Forbrugerombudsmanden at klimaklister-mærket var i strid med vildledningsforbuddet i den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 § 5 og § 6 sammenholdt med § 8 der fokuserer på handelspraksissens evne til at påvirke forbrugerens økonomiske adfærd. Virksomheden kunne derfor ikke lovligt anvende klimaklistermærket i deres markedsføring.

Læs Forbrugerombudsmandens afgørelse her: Virksomhed kunne ikke lovligt benytte udsagnet »klimavenlig« baseret på klimakompensation

Forbrugerombudsmanden har indskærpet regler om vildledende markedsføring over for Falck

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 11. juni 2025 at to udsagn på Falcks hjemmeside havde været vildledende. De to udsagn gav indtryk af at forbrugere kunne få hurtig og billig adgang til psykologhjælp, hvis de led af angst eller depression, hvilket ikke var tilfældet.

Det ene af de to udsagn på hjemmesiden lød: »Du kan få psykologhjælp, hvis du finder dig i en kompliceret følelsesmæssig situation, såsom angst, depression, stress eller sorg.« Dog fremgik det af Falcks egne vilkår, som var at finde

et andet sted på hjemmesiden, at sundhedsabonnementet ikke dækkede, hvis man havde en psykiatrisk diagnose eller havde angst eller depression. Forbrugerombudsmanden vurderede på den baggrund, at udsagnet havde været vildledende over for forbrugeren, da sundhedsabonnementet på psykologhjælp alligevel ikke dækkede angst og depression.

De to udsagn førte til at Forbrugerombudsmanden indskærpede forbuddet i den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 § 5 om forbud mod vildledende markedsføring. Falck fjernede de to udsagn fra deres hjemmeside, og tilbød også at betale abonnementsbetalingerne tilbage til fem kunder, som havde fået afslag på dækning grundet angst eller depression.

Læs Forbrugerombudsmandens pressemeddelelse her: Forbrugerombudsmanden indskærper regler om vildledende markedsføring over for Falck

Tesla betaler bøde for at vildlede om pris og lån ved bilkøb

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) meddelte i en pressemeddelelse af 16. juni 2025, at Tesla Motors Denmark ApS (»Tesla«) har accepteret at betale en bøde på 190.000 kroner for overtrædelse af oplysningspligten ved markedsføring af lån, og for vildledende udeladelser om kontantprisen på deres bilmodeller. Overtrædelserne fandt sted i 2019 og involverede manglende oplysninger om registreringsafgift samt dokument- og leveringsgebyr på Teslas danske hjemmeside. Dette blev af Forbrugerombudsmanden vurderet som en overtrædelse af forbuddet mod vildledende udeladelser i § 6 af den danske markedsføringslov jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«).

Derudover undlod Tesla at give et repræsentativt eksempel på omkostningerne ved lån til finansiering af bilmodellerne, hvilket var i strid med markedsføringslovens krav om kreditoplysninger i § 18. Bødens størrelse afspejler de kriterier, der var gældende på det tidspunkt, da overtrædelserne blev begået. Den nye bødemodel i markedsføringsloven, der blev indført i 2022 og tager udgangspunkt i virksomhedernes omsætning, blev ikke anvendt i denne sag.

Læs Forbrugerombudsmandens pressemeddelelse her: Tesla betaler bøde for at vildlede om pris og lån ved bilkøb

Royal Unibrew betaler bøde på 4 millioner kroner for vildledende klimaudsagn

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 17. juni 2025 at Royal Unibrew A/S (»Royal Unibrew«) havde accepteret at betale en bøde på 4 millioner kr. efter at have været blevet politianmeldt af Forbrugerombudsmanden for vildledende markedsføring.

Royal Unibrew havde anvendt udsagnene »CO_2 klima-neutral« og »Egekilde er CO_2-neutral. Verificeret af COWI« på Egekildedåsers emballage. Udsagnene udgjorde en overtrædelse af vildledningsforbuddet i § 5 og § 6 af den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024, da de vildledte forbrugeren vedrørende Egekildevandets CO_2-neutralitet. CO_2-neutraliteten var delvist opnået gennem klimakompensation, hvilket ikke blev oplyst samtidig med udsagnet om CO_2-neutralitet på emballagen, og derfor var udsagnet egnet til at vildlede forbrugeren om Egekildevandets klimabelastning.

Læs Forbrugerombudsmandens pressemeddelelse her: Royal Unibrew betaler bøde på 4 millioner kroner for vildledende klimaudsagn

To virksomheder politianmeldt for at reklamere for elektroniske cigaretter

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 19. juni 2025 at de havde politianmeldt to virksomheder for at reklamere for elektroniske cigaretter og tilbehør. Politianmeldelsen vedrørte virksomheden »GS Newco ApS« med hjemmesiden »GoSmoke.dk« og virksomheden »Easy To Smoke ApS« med hjemmesiden »Easy-to-smoke.dk«.

Overtrædelserne i politianmeldelserne af de to virksomheder omfattede blandt andet visning af brugeranmeldelser på hjemmesiden, anbefalinger af konkrete produkter, salgsfremmende udsagn, anprisninger, salg af »nybegynder kits«, opfordringer til at tilmelde sig nyhedsbreve samt tilbud om gratis fragt ved køb over 499 kr.

Forbrugerombudsmanden udtalte i den forbindelse, at reklameforbuddet mod at reklamere for elektroniske cigaretter er et absolut forbud. Alle andre oplysninger end neutrale oplysninger om produkt og pris, vil som udgangspunkt være en overtrædelse af reklameforbuddet i § 16 i den danske lov om elektroniske cigaretter, jf. lovbekendtgørelse nr. 1166 af 4. november 2024.

Læs Forbrugerombudsmandens pressemeddelelse her: https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20250619-to-virksomheder-politianmeldt-for-at-reklamere-for-elektroniske-cigaretter-og-tilbehoer

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

Bird & Bird

Wendela Hårdemark

Högsta domstolen om 33 § avtalslagen och digitala avtal – Nätkasinot –

Den 1 juli 2025 meddelade Högsta domstolen dom i mål nr T 607-24 och ett spelbolag dömdes att betala drygt 500 000 euro samt ränta till en spelare. Domen har väckt stor uppmärksamhet eftersom den klargör hur 33 § lag (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område (i det följande avtalslagen) ska tolkas i ljuset av dagens digitala möjligheter att samla in och analysera information respektive ingå avtal.

Processen i underinstanserna

Spelaren hade under perioden 2009 – 2014 spelat på datorsimulerade automatspel online främst enarmade banditer och spelat för nästan 15 miljoner euro. Dessa spel ledde till sammanlagda förluster uppgående till cirka 8 miljoner kronor. I oktober 2014 stängde spelbolaget spelarens konto efter spelarens begäran. Kort därefter sökte spelaren läkarvård och fick i december 2014 diagnosen spelberoende. Spelaren väckte talan vid Patent- och marknadsdomstolen och yrkade att spelbolaget skulle betala 1 000 000 kr i skadestånd för fysiskt och psykiskt lidande samt i nästan 15 miljoner euro jämte ränta i obehörig vinst i strid med bland annat 33 § avtalslagen. Spelbolaget bestred yrkandena.

Spelarens talan ogillades av Patent- och marknadsdomstol i sin helhet. Efter överklagande tog Patent- och marknadsöverdomstolen upp målet till prövning. Vid Patent- och marknadsöverdomstolen begränsade spelaren sitt yrkande om ersättning till i första hand 790 625 euro och i andra hand 527 395 euro. Spelaren justerade även sin talan så att 33 § avtalslagen åberopades som separat grund för spelarens yrkande. Som framgår av 33 § avtalslagen får en rättshandling inte göras gällande om omständigheterna vid dess tillkomst är sådana att det skulle strida mot tro och heder att med vetskap om dem åberopa rättshandlingen och den gentemot vilken rättshandlingen företogs måste antas ha haft sådan vetskap. Bestämmelsen innebär att avtal som tillkommit under ohederliga eller otillbörliga förhållanden kan förklaras ogiltiga och att eventuella prestationer som utförts ska gå åter.

Patent- och marknadsöverdomstolen ansåg att det var tillräckligt att spelbolaget hade haft vetskap om att spelaren haft allvarliga spelproblem för att anses ha varit i ond tro enligt 33 § avtalslagen. Det krävdes följaktligen inte att spelbolaget kände till att spelaren var spelberoende i medicinsk mening. Vidare, då det fanns tydliga tecken på att spelaren påtagligt avvek från vad som kunde anses vara ett sunt spelande ansåg Patent- och marknadsöverdomstolen att spelbolaget haft vetskap om att spelaren haft allvarliga spelproblem. Trots denna kännedom fortsatte spelbolaget att på ett påträngande sätt marknadsföra ett spel som var förenat med en betydande risk för dem som spelar att drabbas av spelberoende gentemot spelaren. Rättshandlingarna ansågs därför vara ogiltiga eftersom det måste anses strida mot tro och heder att göra dem gällande mot spelaren. Domen överklagades av spelbolaget till Högsta domstolen som meddelade prövningstillstånd.

Högsta domstolens bedömning

Frågan i Högsta domstolen var om de rättshandlingar som lett till avtal om spel stred mot tro och heder enligt 33 § avtalslagen. För att besvara denna fråga behövde Högsta domstolen bedöma om omständigheterna vid spelen (rättshandlingarna) var sådana att de skulle anses strida mot tro och heder och om spelbolaget hade haft vetskap om detta.

Högsta domstolen inledde med att konstatera att ett företag som

Illustrasjon: Colourbox.com

användер sig av digitala lösningar för att träffa avtal och hantera kundrelationer utan mänsklig inverkan och som samlar in och bearbetar stora mängder information om och från kunder måste anses ha vetskap om den information som tekniken ger tillgång till och som företaget faktiskt använder. Eftersom spelbolaget ansågs ha haft tillgång till omfattande data om spelarens spelmönster samt använt sig av denna information fann Högsta domstolen att spelbolaget vid tillämpningen av 33 § avtalslagen måste anses ha haft vetskap om spelarens spelbeteende. Därutöver gav utredningen vid handen att spelbolaget känt till att spelaren spelat för anmärkningsvärt stora belopp, spelat påfallande många spel per dag, ägnat mycket tid åt sitt spelande samt visat tydliga tecken på att spelaren tappat kontrollen över sitt spelande. Under dessa förhållanden ansåg Högsta domstolen även att spelbolaget haft vetskap om att spelaren haft allvarliga spelproblem.

Som även Patent- och marknadsöverdomstolen funnit, fann Högsta domstolen att spelbolaget, trots denna vetskap, fortlöpande riktat uppsökande marknadsföring mot spelaren som varit påträngande och rört en av de mest riskfyllda spelformerna i beroendehänseende. Under dessa omständigheter ansåg Högsta domstolen att det stred mot tro och heder att i ond tro göra spelen som spelaren genomfört under viss period gällande. Spelavtalen ansågs således vara ogiltiga med den följden att prestationerna skulle gå åter. Spelaren fick alltså tillbaka 527 395 euro som motsvarade differensen mellan insatta belopp och utbetalda vinster under perioden januari 2012 till oktober 2014.

Rättslig betydelse och framtida tillämpning

I målet var omständigheterna särpräglade. Högsta domstolen redovisar att denna typ av spel var tillåten 2009–2014 och att det då inte fanns några uttryckliga krav på marknadsföring. I dag krävs tillstånd för att bedriva denna typ av tjänst, och det ställs särskilda krav på marknadsföring. Attitydförändringen lyser igenom i Högsta domstolens dom och det blir därför osäkert om och i vilken utsträckning 33 § avtalslagen kan bli tillämplig för att ogiltigförklara andra typer av avtal rörande digitala tjänster.

Avgörandet antyder en utveckling mot ett mer långtgående ansvar för företag som samlar in och bearbetar kunddata. Dessa företag kommer i praktiken att anses ha vetskap om den information som deras system tillhandahåller och förväntas sannolikt agera på de slutsatser som rimligen kan dras av den, även vid automatiserad kundkontakt. I takt med att AI och avancerade analysmetoder integreras i kommersiella tjänster kan detta ansvar komma att skärpas ytterligare. Avgörandet ger emellertid inte något generellt svar på vilka krav som ställs på ett företag för att vetskap om att en rättshandling strider mot tro och heder ska anses föreligga, vilket ändå i slutändan talar för att domen kan få en mer begränsad framtida tillämpning.

Domen finns att läsa här. *https://rattspraxis.etjanst.domstol.se/54bb162c-5180-4514-8c73-ed02a8274595*

Wendela Hårdemark är advokat och delägare på Bird & Bird, där hon även leder Stockholmskontorets IP-grupp. Hon är expert inom immaterialrätt och har mångårig erfarenhet av tvister på detta område i allmän domstol, UPC, skiljeförfaranden och medling. Wendela har ett särskilt fokus på patent-, varumärkes-, upphovs- och marknadsrätt samt företagshemligheter.


Wikström & PARTNERS

Anton Karlsson och Karin Tilly

EU-kommissionen har introducerat en frivillig AI-uppförandekod för AI-modeller

EU-kommissionen har tagit fram en AI-uppförandekod, *"General-Purpose AI Code of Practice"*,[1] i samband med att AI-förordningens[2] regler om nya[3] så kallade AI-modeller för allmänna ändamål började tillämpas från och med den 2 augusti 2025. Uppförandekoden innehåller tre delar som berör transparens, upphovsrätt samt skydd och säkerhet, varav sistnämnda del endast är tillämplig för leverantörer av AI-modeller för allmänna ändamål med systemrisk, vilket för närvarande endast omfattar ett begränsat antal aktörer.

Illustrasjon: Colourbox.com

Det är frivilligt för leverantörer av AI-modeller att ansluta sig till uppförandekoden för att visa att de efterlever kraven i AI-förordningen, vilket enligt kommissionen kan leda till minskad administrativ belastning samt öka den rättsliga säkerheten för leverantörerna. Nyssnämnda kan bland annat säkerställas genom att leverantörer av AI-modeller åtar sig att följa de kompletterande vägledningarna[4] som utfärdats av EU-kommissionen, och som klargör omfattningen av AI-förordningens regler avseende AI-modeller för allmänna ändamål.

Vägledningarna har tagits fram för att visa hur EU-kommissionen tolkar några av AI-förordningens väsentliga begrepp, och tydliggör bland annat när en AI-modell utgör en AI-modell för allmänna ändamål, med eller utan systemrisk, samt när en aktör utgör en leverantör som släpper ut AI-modellen på marknaden. Det tas även upp när kraven som omfattar leverantörer av AI-modeller för allmänna ändamål

1 *https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai.*

2 Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmonierade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens), ("AI-förordningen").

3 Leverantörer av AI-modeller för allmänna ändamål som redan släppts ut på marknaden eller tagits i bruk innan den 2 augusti 2025 ska börja efterleva kraven i AI-förordningen från och med den 2 augusti 2027.

4 *https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act.*

aktualiseras, hur undantag för öppen källkod kan tillämpas, samt följderna för leverantörer vid efterlevnad av uppförandekoden och AI-förordningen. En mall[5] har också publicerats som kan fyllas i för att ge allmänheten en transparent överblick avseende den träningsdata som använts för att träna AI-modellen, för att visa varifrån informationen hämtats.

Samtliga nämnda verktyg och dokument syftar till att hjälpa leverantörer av AI-modeller för allmänna ändamål att efterleva kraven i AI-förordningen, samt förtydliga för övriga aktörer i AI-värdekedjan vilka krav som bör ställas på AI-modellerna, och när de själva kan komma att agera som en leverantör. Uppförandekoden kommer sannolikt också få betydelse vid kravställning och upphandling av AI-modeller. Bland leverantörerna som i dagsläget har undertecknat uppförandekoden återfinns exempelvis Microsoft, Google, IBM och OpenAI, medan Meta inte avser att ansluta sig till uppförandekoden enligt Joel Kaplan, Chief Global Affairs Officer[6].

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

5 *https://digital-strategy.ec.europa.eu/en/library/explanatory-notice-and-template-public-summary-training-content-general-purpose-ai-models.*

6 *https://www.linkedin.com/posts/joel-kaplan-63905618_europe-is-heading-down-the-wrong-path-on-activity-7351928745668055042-XuF7/.*

LOVDATA