Lov & Data

40 år

Desember 2024

Nr. 160 4/2024

Innhold

Leder 2
Sara Habberstad

Jubileumsartikler

Trygve Harvold
Da Lov & Data ble til 4

Ahti Saarenpää
En säker digital miljö?. 5

Søren Sandfeld Jakobsen og Laura Hovgaard Rasmussen
Modsætninger i EU's Digital Age:
Balancen mellem Databeskyttelse og Datadeling 9

Daniel Westman
Från nördigt nischområde till mainstream. 14

Olav Torvund
Det ble en verdipapirsentral. Det var et steg mot noe mer 16

Arve Føyen
Statlige IT-anskaffelser og IT-anskaffelseskontrakter i Norge – Utviklingstrekk og erfaringer 20

Johs Hansen Hammer
Arbeider med juridiske ekspertsystemer ved Institutt for rettsinformatikk for 40 år siden 25

Dag Wiese Schartum
Registrerte personers rettigheter i et 50-årsperspektiv . 30

Stein Schjølberg
Artificial Intelligence (AI) and Law 38

Artikler

Jalmari Männistö
CJEU case C-159/23 on copyright protection of computer program's variable content 44

Torben Aronsen Manndal
DPIA og FRIA – Når inntrer plikten til å gjennomføre vurderingene og hvordan samspiller regelsettene? . . 48

Changkyu Choi and Marius Aasan
Data Vaccination: Balancing Data Security and Utility. . 54

Cecilie Island og Melissa Jakobsen Tveit
Når kan behandlingsansvarlige belage seg på 'berettiget interesse' som behandlingsgrunnlag?
Nye retningslinjer fra EDPB 57

JusNytt 60
Halvor Manshaus: Nasjonalstater og hacking

Rettsinformatisk litteratur 69

Nytt om personvern 71

Nytt om immaterialrett. 78

Nytt om IT-kontrakter. 88

Annet nytt. 91

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

Trykk og layout: Aksell AS

Miljøfyrtårn®

Leder

Sara Habberstad

I skapet på mitt hjemmekontor er det lett å legge merke til bunken med tidsskrifter. De ligger midt i skapet, uten voldsom orden. Lov & Data har vært med meg siden jeg oppdaget fagfeltet, og bestemte meg for at Institutt for Rettsinformatikk (nå Senter for rettsinformatikk) var stedet for meg på juridisk fakultet. Tidsskriftets har vært og er et utsnitt av hva som beveger seg i grenselandet mellom IT og jus, sett fra perspektivet til personer som forholder seg til feltet daglig, i akademia og i praktisk arbeid. Idag gir Lov& Data et bilde av feltet på tvers av fire nordiske land. Å få bli del av tidsskriftet fremover er en oppgave jeg ser frem til med glede og ydmykhet.

På 90-tallet var fagfeltet fortsatt først og fremst for spesielt interesserte. I mine første år i arbeidslivet fikk jeg gjerne spørsmål fra andre jurister om hva i all verden det var man jobbet med innenfor dette området. Slik er det ikke lenger. Idag er det trolig langt flere som kan ha glede og nytte av innholdet i tidsskriftet.

Det er ingen tvil om at det store skiftet her var med GDPR i 2018. Personvern ble allemannseie, og interessen for vårt fagfelt økte.

Idag ser vi stor interesse for også nye regler på området. Som med GDPR er det i stor grad EUs regler som har betydning for oss idag. Regler om kunstig intelligens, med AI Act, og regler om informasjonssikkerhet, med NIS2 i spissen, vil påvirke virksomheter og personer fremover. Slik GDPR gjorde det, og fortsatt gjør det.

En utvikling vi ser fra 2018 er forholdet samfunnet har til EUs regler. Da GDPR trådte i kraft var det få som snakket om personopplysningsloven, personuppgiftslagen, Dataskyddslagen eller Databeskyttelsesloven. Det var i de fleste beskrivelser kun GDPR som ble omtalt. Før GDPR var det vel vanske-

lig å forestille seg at «mannen i gata» skulle kjennen navnet på en EU-forordning bedre enn sin egen lokale lov. Idag er dette ikke lenger vanskelig å se for seg. Jeg vil tippe at NIS2 og AI Act vil være langt mer kjent enn sine nasjonale varianter, også når de kommer på plass. Blant våre fire land er det per november 2024 ingen som har ferdigstilt nasjonale lover som implementerer direktivet NIS2, men til tross for dette ser vi mye som skrives om NIS2, og vi ser få som stiller spørsmålstegn ved om NIS2 er relevant.
I en verden der virksomheter og personer er tett knyttet sammen over landegrenser er det tydelig at vi opplever noen regler som relevante uavhengig av implementeringsfarten til nasjonal lovgivning. Det blir interessant å følge utviklingen fremover på disse områdene, ikke minst her i Lov & Data.
I dette nummeret av Lov & Data har vi en meny med rikelig innhold fra områdene vi nettopp har sett på. I tillegg vil du som leser kunne se frem til flere artikler som tar for seg utviklingen de siste 40 år.

Sara Habberstad

Illustrasjon: Colourbox.com

KORREKSJON:
I den trykte jubileumsutgaven var forfatter av «Jubileumsfesten fortsetter på lod.lovdata.no» falt bort. Forfatter er Sara Habberstad.

Da Lov & Data ble til

Av Trygve Harvold

Det var ingen selvfølge at Lovdata skulle utgi et tidsskrift i 1984. Lovdata var litt over 3 år gammel, gikk med underskudd, hadde 6 ansatte som jobbet som gale for å utvide de få databasene stiftelsen kunne tilby og hadde bare hundre brukere som i begynnelsen slett ikke var fornøyd med det informasjonssystemet de ble tilbudt. Men det Lovdata hadde var en Xerox 2700 laserskriver og samarbeidet med Jon Bing.

La meg begynne med laserskriveren. Xerox 2700 var den første laserskriveren som Xerox lanserte på verdensbasis, og Lovdata kjøpte en av de første som ble solgt i Norge. Lovdata gjorde dette fordi en stor del av inntektene kom fra å levere tekst til trykksaker. Lovdata leverte blant annet teksten til Grøndahls særtrykk, og planla selv å utgi *Norges Forskrifter*, som ville bli den første konsoliderte utgaven av alle Norges gjeldende sentrale forskrifter. Hvis Lovdata kunne levere ferdig sats til disse trykksakene, i stedet for bare tekst som trykkeriet selv måtte sette, ville det utgjøre en betydelig besparelse. Men Xerox 2700 var bare en stor maskin med et kommandospråk som ikke var integrert med noe som helst. Lovdata utviklet derfor et sette- og ombrekkingsprogram som oversatte Lovdatas markeringskoder til maskinens kommandospråk, og dermed ble det mulig å lage trykkesats med proporsjonal skrift. Plutselig hadde Lovdata den tekniske muligheten for å produsere og utgi et tidsskrift til en overkommelig pris.

Trygve Harvold

Og så hadde Lovdata som sagt en fantastisk støttespiller i form av Jon Bing. Allerede i første halvdel av 70-årene erfarte Jon og jeg hvor viktig det var å knytte internasjonale forbindelser og utveksle erfaringer. Jon arbeidet alltid aktivt med å etablere og vedlikeholde et enormt internasjonalt nettverk. Senere, etter at Institutt for rettsinformatikk og Lovdata var etablert, følte vi et behov for et rettinformatisk tidsskrift som kunne formidle nyheter fra inn- og utland.

Vi ønsket et uhøytidelig og utradisjonelt tidsskrift, og nå hadde vi plutselig fått muligheten. Jon ble ansvarlig redaktør og Henning Ve redaksjonssekretær. Overfor Lovdatas styre ble tiltaket forsvart med at dette kunne sees på som markedsføring. Det kunne det vel knapt, men styret innså vel også at tidsskriftet kunne fylle en viktig funksjon i rettssamfunn i rask endring. Etter hvert ble det inngått avtaler med de rettsinformatiske foreningene i Norge, Sverige og Danmark, slik at medlemmene fikk tidsskriftet tilsendt som en del av medlemskapet.

> Tidsskriftet klarer fremdeles å formidle nyheter og spre kunnskap om forhold og problemer knyttet til rettsinformatikk på en svært engasjerende måte.
>
> Det er en stor glede å kunne gratulere Lov & Data med 40 år.

Allerede fra 1985 var det mange bidragsytere fra både Sverige og Danmark. Dette var veldig oppmuntrende, og på 90-tallet fikk tidsskriftet egne redaktører for Danmark (1991) og Sverige (1999) og i år altså også for Finland. Omfanget av tidsskriftet er gradvis blitt utvidet og innholdet har endret karakter i takt med den teknologiske utviklingen, men det uhøytidelige preget er heldigvis bevart. Tidsskriftet klarer fremdeles å formidle nyheter og spre kunnskap om forhold og problemer knyttet til rettsinformatikk på en svært engasjerende måte.

Det er en stor glede å kunne gratulere Lov & Data med 40 år.

Trygve Harvold.
Direktør i Lovdata fra 1981 til 2010.

En säker digital miljö?

Av Ahti Saarenpää

I oktober 2024 försvarade doktoranden *Jenna Andersson* sin doktorsavhandling inför publiken vid Vasa universitet på institutionen för affärsrätt. *Andersson* är ekonomie magister. Temat för studien var informationssäkerhet i organisationer.[1] Hon hade avgränsat sitt forskningsämne till att analysera och utveckla god informationssäkerhetspraxis i organisationer. Trots denna begränsning omfattar boken drygt 400 sidor. Det är en längre avhandling än vad som är brukligt i Finland i dag. Jag hade äran och nöjet att vara opponent på den avhandlingen.

Andersson ställde två grundläggande frågor i sin avhandling. Hon frågade:

1. Är det nuvarande regelverket för informationssäkerhet i organisationer bra?
2. Finns det behov av en nationell lag om informationssäkerhet i Finland?

Den sistnämnda frågan påminner om ett viktigt skede i utvecklingen av den finska rättsinformatiken. År 1997 publicerade vi en omfattande rapport om samma fråga vid Institutet för rättsinformatik vid Lapplands universitet. Idén till denna rapport uppstod under förberedelserna inför implementeringen av EU:s personuppgiftsdirektiv. Den personifierades av en fråga till mig från *Miliza Vasiljeff*, regeringsråd vid finansministeriet. Frågan var: ”Ahti,

Ahti Saarenpää

varför stiftar vi bara lagar om dataskydd här? Borde vi inte också överväga behovet av lagstiftning om datasäkerhet?” Jag gick med på det, och med finansiering från finansministeriet inleddes sedan arbetet. Det var ett viktigt ämne.

Svaret var positivt. Det fanns ett verkligt behov av en allmän lag om informationssäkerhet. Det var inte tillräckligt att personuppgiftsdirektivet kortfattat föreskrev behovet av att skydda information. Detta visade de begåvade unga forskarna i sina goda texter.[2]

Trots att många upplysta parter - såsom riksdagens justitieombudsman och dataombudsmannen - stödde idén om en nationell informationssäkerhetslag ledde vårt förslag inte till något genombrott.

Jag har förstått att det fanns tre olika huvudskäl till detta. För det första sågs informationssäkerhet vid den tidpunkten främst som en teknisk fråga. För det andra hade utvecklingen av informationssamhället bara börjat och en mer allmän förståelse för informationssäkerhet höll fortfarande på att ta form. Och för det tredje sågs personuppgiftsdirektivet som en tillräcklig garanti för datasäkerhet. Det fanns således många skäl till det negativa svaret från förvaltningen. Till dessa ska läggas de skilda åsikterna hos två viktiga ministerier - justitieministeriet och finansministeriet.

> Frågan var: ”Ahti, varför stiftar vi bara lagar om dataskydd här? Borde vi inte också överväga behovet av lagstiftning om datasäkerhet?” Jag gick med på det, och med finansiering från finansministeriet inleddes sedan arbetet.

När *Jenna Andersson* nu återigen föreslår en nationell datasäkerhetslag som ett resultat av hennes forskning är situationen en helt annan. Vi lever i ett digitalt nätsamhälle och en digital rättsstat. Detta har också erkänts av Europeiska unionen, som inledningsvis intog en försiktighetsprincip när det gäller informationssäkerhet. Deklarationen från 2022 om rättigheter och principer för ett digitalt samhälle är mycket talande. EU vill främja en säker

1 Andersson, Jenna Organisaation hyvä tietoturvan sääntelyjärjestelmä *https://osuva.uwasa.fi/bitstream/handle/10024/18074/978-952-395-150-1.pdf?sequence=2&isAllowed=y*

2 Saarenpää, Ahti & Pöysti, Tuomas & Sarja, Mikko & Still, Viveca & Balboa Alcoreza, Ruxandra: Tietoturvallisuus ja laki: näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä: tutkimusraportti Valtiovarainministeriö, hallinnon kehittämisosasto, Lapin yliopiston oikeusinformatiikan instituutti. Valtiovarainministeriö, (1997) 679 s.

digital miljö.[3] Det är svårt att föreställa sig en sådan värld utan en stark koppling mellan dataskydd och datasäkerhet. Men framför allt är informationssäkerhet ännu bredare, mycket bredare än bara en nödvändig grundpelare för ett gott dataskydd.

Jenna Anderssons bok handlar också om det nya NIS2-direktivet[4], som fokuserar på cybersäkerhet. Hon påpekar med rätta att det är viktigt att förstå sig på cybersäkerhet för att kunna etablera goda säkerhetsrutiner i organisationer. NIS2 är en lagstiftning som ligger rätt i tiden och som har blivit en bredare ersättning för bristerna i den tidigare, bara några år gamla NIS1. Och cybersäkerhet är naturligtvis en del av den bredare informationssäkerheten.

Jag har själv skrivit många gånger kort om digitala jurister. Min utgångspunkt är att alla goda jurister i dag också är digitala jurister. Den tid då vi undrade över informationsteknikens intåg i advokatlivet är sedan länge förbi. *Peter Seipel* och *Jon Bing* gjorde ett pionjärarbete för att skingra tidigare tvivel. I deras fotspår var det lättare för mig att sprida samma budskap i Finland.

Men vad kan man då förvänta sig av digitala jurister? *Ethan Kash* påpekade redan på 1990-talet att de måste ha en bredare bas än traditionella jurister som är snävt inriktade på enskilda rättsområden.[5] Detta är utan tvekan fallet. Jag har själv nyligen argumenterat för att digitala jurister i dag bör förväntas ha tillräcklig kunskap om framför allt följande frågor:

1. God kunskap om informationssäkerhet
2. Goda kunskaper om skydd av personuppgifter
3. God kunskap om informationsvägar inom e-tjänster och informationshantering
4. God informationskompetens
5. God kunskap om rättsstatsprincipen
6. God kännedom om nätverkssamhällets infrastrukturer
7. God förmåga att identifiera de positiva och negativa effekterna av AI

Med andra ord är både våra metodologiska färdigheter och färdigheterna att vara ”rättsvetare” i vårt sammanhang tvungna att förnyas om och när vi vill vara goda jurister. Att identifiera sådana förändringar och belysa dem har varit och är fortfarande en av grundpelarna i rättsinformatiken. Vi kan verkligen tala om en framåtblickande disciplin.

Jag har tidigare framfört listan ovan i samband medskyddet av personuppgifter. [6] En advokats arbete består ju i mycket stor utsträckning av behandling av personuppgifter. Men i dag anser jag att goda kunskaper om datasäkerhet bör vara den främsta prioriteringen. Det är vad vår digitala miljö kräver.

Men vår personliga förmåga till att möta förändring är ofta notoriskt blygsam. Tillåt mig att här kort belysa två förbryllande uttryck för långsamhet. De gäller för det första den ostadiga utvecklingen av skyddet av personuppgifter i praktiken, och för det andra den bisarra tanken att försöka bortförklara ett stort systemfelmed att det beror på mänskliga misstag. De båda är viktiga på samhällelig nivå.

Inledningsvis utvecklades skyddet av personuppgifter relativt snabbt i formella termer på lagstiftningsnivå under 1970- och 1980-talen, tack vare Tyskland och Sverige. Tiden var mogen för att reglera närmare den tidigare fria användningen av personlig information, vår personliga information. Men vi befinner oss fortfarande i en situation där man försöker göra personuppgifter till varor i olika former. Och vi befinner oss fortfarande i en situation där problem med dataskydd inte ens erkänns. Jag vill uppmärksamma läsarna av denna publikation på ett beslut som fattades för några år sedan av Finlands Advokatförbunds tillsynsnämnd som övervakar advokater.[7]

Det handlade om en situation där advokaterna hade upphört att arbeta på ett gemensamt kontor. Den advokat som senare lämnade byrån fysiskt krävde att den andre advokaten skulle radera hans personuppgifter från byråns dator. Den senare vägrade med motiveringen att han inte hade någon skyldighet att radera uppgifterna. Den advokat som lämnat firman klagade till tillsynsnämnden. Nämnden fann, med stöd av artikel 17 i dataskyddsförordningen, att uppgifterna i fråga skulle ha raderats. Eftersom den advokat som hade begärt raderingen själv hade agerat olämpligt genom att lagra sina personliga personuppgifter på byråns dator, utdömdes emellertid ingen påföljd.

Jag kan inte frigöra mig från tanken att alla tre parter, både de två advokaterna och tillsynsnämden, handlade fel. Det som framför allt glömdes bort var skyddet av personuppgifter som en grundläggande rättighet. Perspektivet var för snävt.

Ett annat förbluffande uttryck för inkompetens är den långvariga

3 Den europeiska förklaringen om digitala rättigheter och principer 15.12.2022.

4 DIREKTIV (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet)

5 Katsh Law in a Digital World (1995) och nyförtiden https://blackwells.co.uk/bookshop/product/Law-in-a-Digital-World-by-M-Ethan-Katsh/9780195359855

6 Saarenpää The Digital Lawyer, Jusletter IT 26. Ferrera 2015.

7 13.11.2020 Seuraamuksen määräämättä jättäminen | 3. jaosto (på finska)

tendensen att förklara dataintrång eller dataläckage som inget annat än mänskliga fel, som ofta framför allt verkar vara systemfel. Med andra ord har datasäkerheten misslyckats eftersom de lagstadgade riskbedömningarna inte har utförts och ett dataläckage eller ett dataintrång därför har möjliggjorts av enkla mänskliga misstag.[8]

Ett annat problem är avsaknaden av riskanalys vid planeringen av informationssystem. I den finska rättsinformatiken har jag lyft fram *informationens väg* som ett grundläggande teoretiskt juridiskt begrepp vid utformningen av informationssystem. Med informationens väg menar jag att man vid utformningen måste ta hänsyn till alla dem som har rätt att få tillgång till informationen i informationssystemet. Och den måste också ta hänsyn till i vilken form informationen tillhandahålls eller i vilken form mottagaren har tillgång till den. I den finska regleringen av skyddet för personuppgifter ingick informationsvägen i all sin enkelhet i genomförandet av personuppgiftsdirektivet. Den nuvarande nationella dataskyddslagen innehåller samma bestämmelse i följande form:

> (29.4) En personbeteckning får inte onödigtvis antecknas i handlingar som skrivs ut eller upprättas på grundval av ett register.

I den digitala miljön är tanken på ett dynamiskt dokument som kan omvandlas till ett dokument som behåller sitt bevisvärde för olika ändamål både naturlig och oumbärlig. Den statiska pappershandlingens tid torde vara förbi. Men vi stöter fortfarande på situationer där olika uppgifter i dokument svärtas ner och beroende på hur effektiv svärtningen är kan uppgifterna fortfarande vara mer eller mindre synliga. Säkerheten bör inte vara beroende av detta.

Jag ska ännu kort återkomma till *Jenna Anderssons* avhandling. En av hennes grundtankar är att skapa god praxis. Detta innebär naturligtvis en uppförandekod i enlighet med dataskyddslagstiftningen. Därmed kommer vi in på ett av de intressanta problemområdena med regelkommunikation. Vi måste med andra ord fråga oss hur vi ska kunna förenkla den stora mängden lagstiftning för att tillgodose yrkesutövarnas behov. Denna förenkling är en nödvändighet när vi kommer till gränszonerna mellan dataskydd och datasäkerhet.

Ett bra exempel är behandlingen av hälsouppgifter i olika former. GDPR har för närvarande 94 artiklar. Inom området hälso- och socialdata kompletteras den i Finland av lagen om behandling av kunduppgifter inom social- och hälsovården, som innehåller 102 paragrafer. Enbart dessa två författning skapar en sådan mängd lagstiftning som är som råmaterial problematisk även för jurister.

Därför är det oundvikligt att vi behöver uppförandekoder och praxis. Man har inte funderat så mycket på hur de ska utformas. Det finns anledning att göra det. Allt kan inte överlåtas till organisationernas dataskyddsombud. Denna ganska nya profession, som blivit ännu viktigare genom dataskyddsförordningen, är redan mycket vaksamt när det gäller att göra personrättsliga saker på rätt sätt.

Och den tvetydighet som fortfarande råder mellan enskildas privaträttsliga rätt till självbestämmande och förvaltningsrättslig behandling av uppgifter om enskilda, även i ljuset av dataskyddsförordningen, gör inte tolkningen mycket enklare. Därför behöver vi oundvikligen uppförandekoder och goda rutiner.

Andersson tar också upp frågan om standarder och certifieringar. Detta är i sig naturligt. Framför allt bör implementeringen av dataskydd inte reduceras till ett sagolikt hantverk. Men det finns utan tvekan faror i kvaliteten på certifieringen i synnerhet. Som *Lee Bygrave* träffande påpekat, bör inte inbyggd säkerhet (security by design) innebära att man cementerar vissa yrkens särintressen .[9]

Ännu en intressant fråga som *Jenna Andersson* tar upp förtjänar att nämnas just i denna publikation. I sitt arbete ifrågasätter hon om arbetet är en del av rättsinformatiken eller informationsrätten. Den reflektionen är i och för sig naturlig. En avhandlingsförfattare måste ju öppet kunna placera sitt arbete inom rättsvetenskapens område. *Andersson* placerar sin forskning inom informationsrätten. Jag dristar mig till att vara något oense. Det är ingalunda bara på lagstiftningsnivå som man rör sig i hennes arbete. Det finns också teori längs vägen till kunskap. Då kommer vi med nödvändighet att nå upp till rättsinformatikens nivå när det gäller forskningens källdjup. Lyckligtvis är det inte bara fråga om teorilös rättsvetenskap. Vi stöter alltför ofta på en sådan dogmatism i praktiken.

Det har snart gått fyra decennier sedan professor *Asko Lehtonen* som den första i Finland betonade informationsrättens betydelse som en del av undervisningen i och utvecklingen av rättsinformatik. Ämnet hade tidigare varit kontroversiellt. I dag är informationsrätten som en del av rättsinformatiken en ytterst viktig del av rättsinformatikens kärnområde. Detta bör man ha i åtanke när man läser EU:s deklaration om digitala rättigheter och principer för det digitala årtiondet, som redan nämnts ovan. Det är ett slags deklaration av *allmänna läror*. Det är synd att *Jon Bing* inte längre finns kvar för att se och uppleva den.

---

8 Saarenpää, Human Error and Data Security, Jusletter IT 25. Februar 2021

9 Bygrave, Lee A. Data Protection by Design and by Default (October 18, 2021). University of Oslo Faculty of Law Research Paper No. 2021-19, in ssrn.com/abstract=3944535

I Finland håller vi på att genomföra en omfattande reform av den nationella lagstiftningen om dataskydd.[10] I detta sammanhang kommer vi förhoppningsvis att kunna göra oss av med den gamla, beklagliga administrativa och statliga bördan i de nuvarande nationella lagarna. Resultatet av denna börda har senast varit att den offentliga sektorn inte är föremål för de administrativa sanktionsavgifterna enligt dataskyddsförordningen. Men detta borde inte ha hänt. Medan dataskyddsförordningen representerar den rättsstatliga idén om dataskydd har det nationella handlingsutrymmet delvis använts för att uppnå föråldrade administrativa statliga mål. Och även i det reformarbete som planeras nu syns myndigheternas perspektiv vara centralt.

> Lyckligtvis har rättsinformatiken inte alls bara varit ett intresse för en generation. I dagens värld måste alla goda jurister vara digitala jurister i en digital miljö.

Som jag hoppas att jag lyckats påvisa ovan, kan en enda bra avhandling i dag öppna upp ett belysande perspektiv på utvecklingen av den digitala miljön och rättsinformatiken. När jag fick möjlighet att delta i det första riktiga nordiska mötet om rättsinformatik i Oslo 1985 var jag redan väl medveten om den viktiga väg som *Peter Seipel* och *Jon Bing* redan då var inne på. Lyckligtvis har rättsinformatiken inte alls bara varit ett intresse för en generation. I dagens värld måste alla goda jurister vara digitala jurister i en digital miljö.

Ahti Saarenpää är professor emeritus i privaträtt och hedersordförande för institutet för rättsinformatik vid Lapplands universitet, docent i personlighetsrätt vid Helsingfors universitet, f.d. ordförande för datasekretessnämnden samt medlem av Finlands vetenskapsakademi

10 Tietosuojalainsäädännön kokonaisuudistus: Koordinaatioryhmän väliraportti *http://urn.fi/URN:ISBN:978-952-400-951-5*

Modsætninger i EU's Digital Age: Balancen mellem Databeskyttelse og Datadeling

Av Søren Sandfeld Jakobsen og co-author Laura Hovgaard Rasmussen

1 Indledning

2024 rinder ud, og vi har nu over seks års erfaring med Databeskyttelsesforordningens glæder og sorger.

Databeskyttelsesforordningen, i daglig tale også kaldet GDPR, har ikke kun fremhævet den betydelige værdi der ligger i persondata, men også hvad adgang til og brug af persondata har af betydning i vores moderne samfund. Vi har, som afledning heraf, lært, at det er afgørende at passe særdeles godt på disse data.

Ved indgangen til 2025 befinder os midt i EU's digitale tidsalder, hvor nye lovgivningsinitiativer konstant dukker op inden for den digitale udvikling, og det kan være en udfordring at holde trit med dem alle.

> Hvordan kan vi balancere disse i udgangspunktet modsatrettede hensyn om databeskyttelse og behov for datadeling, uden at det har negative konsekvenser for både fysiske personer, men også innovationen i EU?

Med de mange teknologiske fremskridt er mulighederne for dataanvendelse næste ubegrænsede og nye koncepter og anvendelser opstår

Søren Sandfeld Jakobsen

Laura Hovgaard Rasmussen

kontinuerligt. Dette medfører dog også nogle hidtil uafklarede problematikker og problemstillinger, som EU og Kommissionen, men også private aktører, står over for – nemlig udfordringer, hvor ønsket om at beskytte fysiske personer og deres privatliv kolliderer med behovet for at udvide adgangen til data og datadeling for at øge vækst og innovation på det europæiske marked - for at sikre Europas konkurrencedygtighed på globalt plan.

EU har udviklet et omfattende sæt af regler med henblik på at beskytte fysiske personer; På den ene side blandt andet EU's Charter om Grundlæggende Rettigheder og GDPR, der sætter individets rettigheder i centrum. På den anden side nye lovgivningstiltag som for eksempel EU's Data Act og European Health Data Space, der tilskynder til bredere datadeling.

Hvordan kan vi balancere disse i udgangspunktet modsatrettede hensyn om databeskyttelse og behov for datadeling, uden at det har negative konsekvenser for både fysiske personer, men også innovationen i EU?

2 Modsætninger i lovgivningen

2.1 Databeskyttelse og retten til privatliv

Beskyttelse af individets rettigheder er en grundsten i EU-retten. I EU-kontekst har dette mundet sig ud i flere reguleringer, der har til formål at stille regler for beskyttelsen af fysiske personer og deres rettigheder.

2.1.1 Den Europæiske Unions Charter om Grundlæggende Rettigheder (»Charteret«)

Den Europæiske Unions Charter om Grundlæggende Rettigheder blev udarbejdet af Det Europæiske Konvent og blev vedtaget den 7. december 2000 af Europa-Parlamentet, Europa-Kommissionen og

Ministerrådet. Med Lissabon-traktaten fik Charteret retskraft på traktatniveau den 1. december 2009. Charteret er EU's pendant til Menneskerettighedskonventionen (EMRK), der er vedtaget af Europarådet i 1950.

Charteret lægger vægt på vigtigheden af menneskets værdighed, som er ukrænkelig, og som skal beskyttes og værnes om.[1] Charteret understreger betydningen af frihed, privatliv og sikkerhed.

Artikel 7 i Charteret fastlægger, at enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation.[2] Artikel 8 i Charteret bestemmer retten til beskyttelse af personoplysninger, og disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf.[3]

2.1.2 Traktaten om Den Europæiske Unions funktionsmåde (»TEUF«)

Traktaten om Den Europæiske Unions funktionsmåde udgør, sammen med EU-traktaten, det primære retsgrundlag for det politiske sammenhold i Den Europæiske Union. Traktaten, der dannede grundlag for EU-samarbejdet, blev oprindeligt underskrevet i Rom i 1957, men er ændret adskillige gange efter, senest i 2007 i Lissabon. Formålet med TEUF er at skabe grundlag for en tæt sammenslutning mellem de europæiske folk.

TEUF artikel 16 fastslår, at enhver har ret til beskyttelse af personoplysninger om vedkommende selv, og at Europa-Parlamentet og Rådet fastsætter regler for beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.[4]

2.1.3 Databeskyttelsesforordningen - GDPR

GDPR blev indført for at styrke og harmonisere databeskyttelse for alle individer i EU, og blev vedtaget i 2016. Forordningen erstatter EU's persondatadirektiv fra 1995.[5] Forordningen fastlægger beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger som en grundlæggende rettighed efter Charterets artikel 8 og TEUF artikel 16.[6] Den skal give enkeltpersoner kontrol over deres personlige data og forpligter organisationer og virksomheder til at beskytte disse data, ved at opstille klare principper for behandling af personoplysninger, herunder at behandlingen skal være lovlig, rimelig og gennemsigtig, og ikke gå ud over hvad der er nødvendigt. Forordningen har til formål at skabe et område med frihed, sikkerhed og retfærdighed samt at fremme økonomisk og social fremgang inden for det indre europæiske marked.[7]

Forordningen fastsætter derudover skrappe regler for sikkerhedsforanstaltninger og videredeling af personoplysninger, og såfremt der er høj risiko for fysiske personers rettigheder, er der endnu strengere krav til behandlingen.

Charteret, TEUF og GDPR er særligt vigtige i en digital tidsalder, hvor data er en ressource, men samtidig også en kilde til potentielle krænkelser af privatliv og fysiske personers rettigheder.

2.2 EU's Digital Decade[8] - Datadeling

EU's digitale tidsalder, eller digitale årti, er EU's vision for at skabe et integreret digitalt samfund og økonomi, og fremme den digitale omstilling. Det har til formål at forbedre dataadgang og datadeling på tværs af EU's indre marked, og sigter mod at udnytte fordelene ved digital teknologi samtidig med, at man beskytter borgernes rettigheder og fremmer innovation. Hensynet bag dette tiltag er den hurtige udvikling inden for især teknologien, som allerede er anerkendt i Charteret[9], i TEUF[10] og i GDPR[11].

I kølvandet heraf, er der vedtaget eller stillet forslag om en bred vifte af forordninger og direktiver, herunder, men ikke begrænset til, EU's Data Act og European Health Data Space.

2.2.1 EU's Data Act

Det digitaliserede samfund producerer et hav af data, ikke kun persondata, men også data om for eksempel brugen af digitale produkter og enheder, som kan være værdifulde for værdiskabelse og innovation. EU's Data Act, også kaldet Dataforordningen, har til formål at fastsæt-

1 Charter 2016/C 202/02 Den Europæiske Unions Charter om grundlæggende rettigheder, artikel 1.
2 Ibid, artikel 7.
3 Ibid, artikel 8.
4 2016/C 202/01 – Konsolideret udgave af traktaten om Den Europæiske Unions funktionsmåde, artikel 16.
5 Direktiv 95/46/EF.
6 EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse), præambelbetragtning nr. 1.
7 Ibid, præambelbetragtning nr. 2.
8 *Decision - 2022/2481 - EN - EUR-Lex*
9 Charter 2016/C 202/02 Den Europæiske Unions Charter om grundlæggende rettigheder, præambel.
10 2016/C 202/01 – Konsolideret udgave af traktaten om Den Europæiske Unions funktionsmåde, bl.a. artikel 4 og 173.
11 EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse), præambelbetragtning nr. 6.

te et harmoniseret regelsæt for deling af data inden for EU's indre marked, og sikre fair adgang til og anvendelse af data indenfor Europa. Data Act skal fremme datadeling, innovation og konkurrenceevne ved at skabe en fælles ramme for dataudveksling, og åbner adgangen for anvendelse og videreanvendelse af data i ubegrænset omgang og dermed fremme en effektiv dataøkonomi. Hindringer for delingen af data udgør nemlig en hæmsko for en optimal datadeling til gavn for samfundet, da usikkerhed omkring deling af data, men også rettigheder og forpligtelser vedrørende data, afskrækker mange dataindehavere for at indgå aftaler om udveksling af data.[12] Med EU Data Act sigtes der altså mod at udnytte data som en ressource for økonomisk vækst og teknologisk udvikling.

Dataforordningen tilskynder til datadeling ved at kræve, at dataindehavere (dette vil i praksis ofte være produktudviklere) forsyner brugerne med data genereret af produktet og deler disse data med tredjeparter på brugerens anmodning. Brugere af forbundne produkter og relaterede tjenester har dermed ret til at få adgang til og anvende de data, der genereres ved brugen, og kan dele dem med tredjeparter.[13] Brugerne har ret til at dele data med tredjeparter til både kommercielle og ikke-kommercielle formål, og der er dermed fastsat et grundlag for en retfærdig fordeling af værdien af data.[14]

Data Act trådte i kraft 11. januar 2024 og finder anvendelse fra september 2025.

2.3 European Health Data Space (»EHDS«)

Forslaget til Forordningen om det europæiske sundhedsdataområde, EHDS, har til formål at give fysiske personer i EU større kontrol over deres elektroniske sundhedsdata og sikre en retlig ramme med pålidelige styringsmekanismer og et sikkert databehandlingsmiljø. Især området omkring sundhedsdata er et utroligt vigtig område, men er svært for fysiske personer at navigere i. Medlemsstaterne har implementeret uensartede lovgivninger på området, hvilket hindrer den sekundære anvendelse af digitale sundhedsdata.[15] EHDS har dermed til formål at skabe en fælles ramme for deling og brug af sundhedsdata på tværs af medlemslandene, og at give enkeltpersoner adgang til og kontrol over deres sundhedsdata (primær brug) og muliggøre sikker genbrug af data til forskning, innovation og politisk beslutningstagning (sekundær brug).

For at beskytte de følsomme personoplysninger, som sundhedsdata er, bygger EHDS på GDPR, og indfører sektorspecifikke regler for at sikre både datasikkerhed og privatlivets fred. De fysiske personer bevarer retten til at fravælge datadeling, hvilket afbalancerer individuel autonomi med den bredere offentlige interesse. EHDS tager også fat i covid-19-pandemien og fastslår betydningen af sundhedsdata for udviklingen af politikker som reaktion på sundhedskriser, samt at det er afgørende for menneskers liv og sundhed, at der er adgang til effektiv deling af data, både i forbindelse med behandling her og nu, men også i forhold til forskning på sundhedsområdet, innovation, patientsikkerhed, statistik, og meget mere.[16]

Forslaget til forordningen blev fremlagt i 2022. Forslaget er stadig under behandling.

3 Konflikt mellem databeskyttelse og datadeling

GDPR bygger på en anerkendelse af, at teknologien udvikler sig hurtigt og skaber udfordringer i forhold til beskyttelsen af fysiske personer. Derfor er det i præamblen til GDPR også antaget, at forordningen ikke skal være til hinder for innovation. Der redegøres i GDPR ikke nærmere for, hvordan vi skal imødekomme disse hensyn, men blot at EU skal have en stærk og sammenhængende databeskyttelsesramme.[17] EU's efterfølgende reguleringer, herunder Data Act og EHDS, søger at imødekomme begge hensyn, men er det lykkes?

EU's forskellige reguleringer har gennemgående samme hensyn, men så alligevel ikke; Charteret, TEUF og GDPR fokuserer på at beskytte fysiske personers rettigheder, og sætter individet i fokus, mens Data Act og EHDS fremmer datadeling, hvilket sætter tredjeparter i fokus. Dette skaber en iboende konflikt og en mulig disharmoni mellem regelsættene, da øget datadeling kan kompromittere privatlivets fred.

Selvom Data Act og EHDS fremhæver GDPR som det bærende element for behandling af personoplysninger, stiller GDPR stadigt andre eller strengere krav til dokumentationen og detaljerne for be-

12 EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2023/2854 af 13. december 2023 om harmoniserede regler om fair adgang til og anvendelse af data og om ændring af forordning (EU) 2017/2394 og direktiv (EU) 020/1828 (dataforordningen), præambelbetragtning nr. 1 og 2.

13 Ibid, præambelbetragtning nr. 5 og 6.

14 https://digital-strategy.ec.europa.eu/da/policies/data-act

15 Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om det europæiske sundhedsdataområde (COM(2022)) 197 final, baggrund for forslaget.

16 Ibid.

17 EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse), præambelbetragtning nr. 6, 7 og 159.

handlingen end Data Act og EHDS gør. Disse uoverensstemmelser gør det svært for både fysiske personer og juridiske personer at navigere rundt i de forskellige rettigheder og forpligtelser. Samtidig hermed er implementeringen og fortolkningen af databeskyttelsesforordningen i EU-medlemslandene ligeledes forskelligartede, og der er en betydelig juridisk usikkerhed for alle omfattet af forordningerne og regelsættene, og det er svært at navigere i.[18] Hvad der gælder i ét medlemsland, gælder ikke nødvendigvis i et andet på grund af det nationale råderum fastsat i GDPR.

Dertil udvider Data Act anvendelsesområdet til også at omfatte non-personal data (ikke-personoplysninger), og giver adgangsrettigheder til alle brugere, ikke kun datasubjekterne – Dette kan give anledning til tvivl om hjemlen for databehandlingen under GDPR artikel 6, også i forbindelse med videregivelse til tredjeparter.[19] Det udvidede anvendelsesområde stiller samtidig store krav til, hvordan data klassificeres i behandlingen – om det reelt er personoplysninger eller ikke personoplysninger, og det er vigtigt for dataindehaveren at klassificere oplysningerne korrekt.

4 Anonymisering som løsning?

4.1 Anonymisering: En løsning, der ikke holder?

Er personoplysninger gjort anonyme, altså på en sådan måde, at det ikke længere er muligt at identificere en fysisk person ud fra oplysningerne, gælder beskyttelsen under GDPR ikke.[20] Data Act og EHDS angiver ligeledes, at personoplysninger som udgangspunkt skal anonymiseres, medmindre de anonyme data ikke er tilstrækkeligt til at opfylde det formål, de skal anvendes til.[21]

Det virker umiddelbart som en lige til løsning på problemet – Hvis vi ikke længere kan identificere den fysiske person bag dataene, er der ikke et beskyttelseshensyn at tage, og dataene kan frit flyde på EU's indre marked til ubegrænset anvendelse til innovation og forskning med videre.

Men problemerne opstår, når det ikke helt er muligt at anonymisere data – eksempelvis når data kan »de-anonymiseres«, fordi rådataene fortsat bliver opbevaret.

Den tidligere Artikel 29-gruppe (nu erstattet af Det Europæiske Databeskyttelsesråd (»EDPB«)) udstedte i 2014 retningslinjer og teknikker for anonymisering, men mange af teknikkerne er forældede. Set i forhold til den hurtigt udviklende teknologi medfører anonymisering altså tekniske udfordringer, som der ikke helt er taget stilling til på nuværende tidspunkt.

Et vigtig konfliktpunkt, som også adresseres i EHDS, er, når der efter anonymisering af personoplysninger er en tilbageværende risiko for de-anonymisering; Når der, på trods af brugen af avancerede anonymiseringsteknikker, stadig er en restrisiko for genidentifikation af den fysiske person, for eksempel i tilfælde af sjældne sygdomme, der kun rammer et meget snævert antal personer. Her vil der være tale om en afgrænset personkreds, og det kan være muligt at genidentificere en person bag dataene.[22]

Et andet konfliktpunkt er, når en tredjepart eller en bruger under for eksempel EDHS modtager anonymiseret data, men der stadig ét sted i datakæden findes en krypteringsnøgle, der reelt gør det muligt at de-anonymisere dataene – rådataene findes altså stadig. EHDS åbner også mulighed for, at ansøgere kan anmode om de de-anonymiserede data,[23] og i disse tilfælde, vil der netop ikke være tale om, at dataene reelt er anonymiseret, som defineret i GDPR præambelbetragtning nr. 26. Denne adgang til brug af ikke-anonymiserede data, som lovligt kan behandles ved for eksempel at have tilstrækkelige sikkerhedsforanstaltninger på plads, ville medføre at man undgår at miste den analytiske værdi af dataene til forskningsformål, hvilket jo netop er det som EHDS søger at imødegå, men selv med tilstrækkelige sikkerhedsforanstaltninger er der en stor risiko for den registrerede i kraft af de meget følsomme oplysninger, som sundhedsdata er.[24]

4.2 Syntetiske datasæt: En alternativ løsning?

Syntetiske datasæt genereres til at efterligne reelle data, men uden at indeholde personlige oplysninger – altså en simulation af mønstre fra virkelige data. Syntetiske datasæt kan bruges til blandt andet at træne

18 Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om det europæiske sundhedsdataområde (COM(2022)) 197 final, baggrund for forslaget.

19 Clocker, Dr. Felix, 2023, »Disharmony between Data Act and GDPR«, CMS Law-NowTM.

20 EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse), præambelbetragtning nr. 26.

21 Se f.eks. Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om det europæiske sundhedsdataområde (COM(2022)) 197 final, præambelbetragtning nr. 49.

22 Ibid, præambelbetragtning nr. 64.

23 Ibid, præambelbetragtning nr. 49.

24 European Commission: Directorate-General for Research and Innovation, European Group on Ethics in Science and New Technologies, Biller-Andorno, N., Céu Patrão Neves, M., Laukyte, M. et al., *Opinion on democracy in the digital age*, Publications Office of the European Union, 2023, *https://data.europa.eu/doi/10.2777/078780*

AI-modeller, de kan bruges til forskning og de kan anvendes til udvikling af nye produkter og koncepter, uden at kompromittere privatlivet. Dog kan syntetiske datasæt, i og med at de ikke er virkelige data, variere i nøjagtighed og anvendelighed.

Da der ikke i realiteten anvendes personoplysninger om fysiske personer, kan man argumentere for, at syntetiske datasæt er anonyme data uden den iboende risiko for de-anonymisering. På den anden side kan man også modargumentere med, at syntetiske datasæt, hvis det bevarer egenskaber fra det oprindelige datasæt, vil have en sammenkædningsmulighed den oprindelige data, og dermed kan det være muligt at udlede en fysisk person. Ifølge den, om muligt forældede, vejledning fra Artikel 29-gruppen,[25] skal det være helt umuligt nogensinde at kunne knytte data tilbage til en person, før end data er anonym i ordets forstand.[26]

4.3 AI og anonymisering?

I takt med den teknologiske udvikling, er AI-systemer også blevet mere udbredt, mere effektive og mere anvendte. Dette stiller spørgsmålet, om det vil være muligt at få et AI-system til effektivt at anonymisere data på den dataansvarlige og dataindehaverens vegne. Ved at indføre persondata i et AI-system specifikt udviklet til at anonymisere, og slette inputtet, vil persondataene i AI-systemets black box blive gjort anonymt, og der vil ikke sidde en dataansvarlig/dataindehaver tilbage med en krypteringsnøgle, da persondataene i praksis vil forsvinde i systemets black box.

Med AI vil der være risiko for, at et andet AI-system kan krydskombinere data og derigennem re-identificere personoplysningerne,[27] og der vil i dette tilfælde ikke være tale om en effektiv anonymisering, selvom der ikke findes en krypteringsnøgle til re-identifikationen.

5 Konklusion: Kan balancen skabes?

EU står over for en fundamental udfordring: Hvordan sikrer vi, at innovation og økonomisk vækst ikke underminerer EU-borgernes privatliv og databeskyttelse? En af løsningerne til dette er anonymisering af data, da der hermed ikke vil opstå risiko for krænkelse af borgernes rettigheder, samtidig med at der så kan ske fri anvendelse af den anonymiserede data på det indre europæiske marked, til gavn for forskning, udvikling og innovation. Men er dette en reel mulig løsning på nuværende tidspunkt?

En anden løsning er at gøre brug af syntetiske datasæt, og dermed skabe »anonym« data, men selv med syntetiske datasæt kan man risikere, at der vil opstå situationer, hvor det er muligt at udlede en fysisk person bag, såfremt den syntetiske data bevarer egenskaber fra det oprindelige datasæt.

Dette er blot nogle af de udfordringer vi står overfor i EU's digitale tidsalder, og vi må kontant være i udvikling for at følge med og for at finde balancen til hensynene – også på lovgivningens side.

Søren Sandfeld Jakobsen
Professor, ph.d., advokat
ssj.law@cbs.dk
CBS LAW
Copenhagen Business School

Co-Author:
Laura Hovgaard Rasmussen
Advokatfuldmægtig, Gorrissen Federspiel
lara@gorrissenfederspiel.com

25 *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_da.pdf*

26 López, César Augusto Fontanillo, and Abdullah Elbi, 2022, »On Synthetic Data: A Brief Introduction for Data Protection Law Dummies.« European Law Blog, September.

27 Buckley, Gerard and Caulfield, Tristan and Becker, Ingolf, How might the GDPR evolve? A question of politics, pace and punishment (May 16, 2024). Accepted in Computer Law & Security Review: *http://dx.doi.org/10.2139/ssrn.4830619*

Från nördigt nischområde till mainstream

Av Daniel Westman

Inledning

När Lov & Data grundades 1984 var rättsinformatiken ett relativt nytt juridiskt ämne. Inspirerad av professor Peter Seipel fick jag själv upp ögonen för ämnet knappt tio år senare under mina studier vid Stockholms universitet. När Sverige kom med i Lov & Data-familjen 1999 blev jag svensk redaktör och fick tillfälle att samarbeta med tidskriftens huvudredaktör professor Jon Bing.

Det känns som att tiden sedan dess har flugit iväg, men sett i backspegeln är det lätt att se hur intensiv den tekniska, samhälleliga och rättsliga utvecklingen har varit. Lov & Datas jubileum ger mig anledning att stanna upp och reflektera över den it-relaterade juridikens utveckling och områdets karaktär idag. Även om det finns mycket att säga blir framställningen här kortfattad och fokuserad på några utvalda poänger.

Dåtid

Även om juridiken kopplad till samhällets datorisering hade analyserats ända sedan 1960-talet var rättsinformatiken och it-rätten i början av 1990-talet fortfarande nischområden med hög nördfaktor.

Vissa specialregler inriktade på digitala tillämpningar fanns på plats i svensk rätt, t.ex. hade bestämmelserna om allmänna handlingars offentlighet i 2 kap. tryckfrihetsförordningen anpassats till ”upptagningar för automatisk databehandling”, datalagen (1973:289) reglerade förutsättningarna för att inrätta datoriserade personregister

Daniel Westman

och upphovsrättslagens skydd för litterära verk hade uttryckligen gjorts tillämpligt på datorprogram.

Men det är ingen överdrift att påstå att lagstiftaren i huvudsak fortfarande hade en ”hands-off” inställning till uttrycklig reglering av digitala företeelser och inte minst var skeptisk till en direkt reglering av nya tekniska företeelser. Ledordet var – ofta utan att begreppet tydligt definierades – teknikneutral lagstiftning.

Fokus riktades därmed i stor utsträckning mot tillämpningen av generellt utformade rättsregler på nya digitala företeelser. En central metodologisk utmaning, som uppmärksammades i den rättsinformatiska forskningen och utbildningen, var behovet av att förstå tekniken och vilka egenskaper hos denna som var rättsligt relevanta vid tillämpningen av en viss rättsregel. Professor Mads Bryde Andersen har talat om utmaningarna i termer av ett beskrivningsproblem.

Det it-rättsliga perspektivet utgår från att det finns ett värde i att samlat studera hur rättsregler inom olika traditionella rättsområden påverkar användningen och utformningen av den digitala tekniken. Det tvärjuridiska perspektiv utesluter givetvis inte att digitala frågor också studeras inom de traditionella rättsområdena, något som också har kommit att ske i betydande utsträckning. Under 1990-talet fanns det emellertid också personer, bl.a. den amerikanska domaren Frank Easterbrook, som helt ifrågasatte värdet av en rättslig disciplin som utgick från den digitala miljön som studieobjekt.

Inom den tidiga rättsinformatiken var studieobjektet inte bara den materiella juridikens tillämpning på digitala företeelser, utan intresset riktades också mot hur jurister kunde använda tekniken för att lösa uppgifter. Exempelvis analyserades hur juridiskt godtagbara lösningar kunde ”byggas in” in i produkter och infrastrukturer. Det var ett perspektiv som många jurister vid denna tidpunkt uppfattade som svårtillgängligt, men som nu framstår som mer naturligt och till och med utgör ett uttryckligt rättsligt krav i vissa sammanhang (jfr exempelvis dataskyddsförordningens krav på inbyggt dataskydd och dataskydd som standard).

Nutid

Idag genomsyrar den digitala tekniken hela samhället. Under de senaste trettio åren har vi sett många nya tekniker introduceras och flera av dessa har kommit att spela en viktig roll. För närvarande kretsar mycket kring maskininlärning och anknytande datahantering. Rättsliga frågor

rörande användning och insamling av den data, liksom frågor som rör denna nya form av automatisering står i fokus.

I takt med samhällets genomgripande digitalisering har attityden till ny rättslig reglering av digitala företeelser kommit att omprövas i grunden. Från EU-lagstiftaren är det bokstavligen ”proppen ur”. I en inledande rättslig våg – som fortfarande pågår – har det handlat om att uppdatera och it-anpassa generella regelverk såsom dataskyddslagstiftningen, upphovsrätten och produktansvarsregleringen.

I en andra våg har vi sett helt nya typer av regelverk som är direkt inriktade på digitala företeelser (viss teknik, plattformar, grindvakter, infrastrukturer etc.). Förordningen om digitala tjänster (Digital Services Act) och AI-förordningen (AI Act) utgör exempel på denna typ av regleringsansats. Ofta är de nya regelverken omfattande och detaljerade samtidigt som de innehåller nya mekanismer för tillsyn och utdömande av kraftfulla sanktioner.

De nya lagstiftningsinsatserna har resulterat i ett omfattande och komplext it-rättsligt regelverk. I praktiken aktualiseras inte sällan lagstiftning i flera lager. AI-förordningen gäller t.ex. utöver generella regler om t.ex. dataskydd. Dagens it-jurister måste därför såväl kunna tillämpa generella regelverk – vissa uttryckligen anpassade till den digitala miljön, andra inte – som ha kunskap om den nya teknikspecifika regleringen. Till detta kan läggas ett behov av att kunna tillämpa relevanta sektorspecifika regler, t.ex. inom finansiell sektor och hälsosektorn, vilka med tiden fått en allt tydligare koppling till digitala företeelser.

På ett plan kan det framstå som naturligt att digitala företeelser – mot bakgrund av den genomgripande digitaliseringen av samhället – behandlas som andra produkter och tjänster i regleringshänseende. Samtidigt är regleringen av information, data och digital teknik förknippad med särskilda intressen. Ofta aktualiseras exempelvis en eller flera grundläggande rättigheter, något som ställer särskilda krav på såväl lagstiftaren som rättstillämparen.

Enligt min mening innebär de senaste årens rättsliga utveckling på många sätt en renässans för it-rättens och rättsinformatikens perspektiv och grundläggande poänger. Det är uppenbart att jurister måste ha åtminstone en grundläggande förmåga att anlägga ett tvärjuridiskt perspektiv på den allt mer kompakta regleringsmiljön. När det nu talas om behovet av ”data governance” enligt ett flertal regelverk är det exempelvis en tydlig påminnelse om detta behov. Samtidigt blir det allt oftare tydligt att juridiken måste ”byggas in” i tekniken och att detta arbete ställer särskilda krav på kompetens och funktionsöverskridande arbetssätt.

Krav på it-juristen

Kraven på de moderna it-juristerna är höga. Precis som tidigare krävs att de besitter åtminstone grundläggande förståelser av den digitala tekniken och av terminologin på området. Till det kommer nu alltså behovet av att hänga med i den intensiva rättsutvecklingen i form av ny lagstiftning och rättspraxis, inte minst från EU-domstolen.

I allt högre grad krävs och förväntas dessutom nya arbetssätt. Det handlar allt mer om att kunna samarbeta med andra professioner och att kunna arbeta verksamhetsnära, t.ex. med rättslig kravställning och granskning av tekniska lösningar – inte ”endast” med abstrakt juridik.

Denna kravbild kan framstå som övermäktigt, men det finns vägar framåt. Jag vill särskilt framhålla behovet av samarbete inom ett arbetslag med olika kompetenser och profiler. Jag tror personligen att det skulle vara bra om det tydligare etablerades olika juristroller på it-området. Jag brukar lite förenklat tala om att vi både behöver ”jurist-jurister” (med olika verksamhetsinriktning), som kan djupdyka i regelverket, och jurister som är experter just på det teknik- och verksamhetsnära arbetet, men utan att behöva besitta samma djupgående kompetens rörande regelverkets alla delar. Genom att sätta ett tydligt namn på den senare yrkesrollen skulle det vara lättare att skapa en tydlig yrkesidentitet och i förlängningen att rekrytera rätt kompetens. En ökad användning av AI liksom nya utbildningskoncept kan också bidra till att i framtiden hantera de höga kraven som ställs på it-juristerna.

Personligen gillar jag de nya utmaningarna och satsar därför på att hänga med trettio år till inom området. Vi får se hur det går!

Daniel Westman

Det ble en verdipapirsentral. Det var et steg mot noe mer

Av professor dr. juis Olav Torvund

I første nummer av «Lov og Data» skrev jeg en artikkel om «Forslag om en norsk verdipapirsentral». Jeg hadde da arbeidet med en utredning om etablering av en verdipapirsentral i Norge. Det var en utredning preget av sterkt tidspress, da man i det gamle oppgjørssystemet hadde store problemer med å håndtere den eksplosive veksten i verdipapiromsetningen. Man fryktet et totalt sammenbrudd. Det var en spennende utfordring med en særdeles bratt læringskurve for en ung og nyutdannet jurist. Jeg hadde arbeidet med elektroniske betalingstransaksjoner. Men kjente ikke verdipapirmarkedet. Jeg var også temmelig blank når det gjaldt selskapsrett. Vi må bare erkjenne at vi ikke helt forsto hva vi gjorde den gangen.

Det ble en verdipapirsentral. Loven ble vedtatt i juni 1985. Finansnæringen hadde forskuttert at dette ville bli vedtatt, og hadde startet oppbyggingen av en verdipapirsentral. Den kom i drift i 1987. Det ble vedtatt en ny lov om verdipapirregistre i 2002,[1] en lov som i 2019 ble avløst av en ny verdipapirsentrallov.[2] Denne siste og någjeldende loven er basert på EUs direktiv 2017/828 (Aksjonærrettighetsdirektivet). Det som startet i Norden på 1980-tallet er utvidet til hele EU/EØS.

Verdipapirsentralen ble senere overtatt av Oslo børs, som igjen er overtatt av Euronext. Euronext har

Olav Torvund

også overtatt blant annet den danske og den svenske verdipapirsentralen. I de snart 40 årene som har gått, kan vi konstatere at det gikk bra. Det har ikke vært alvorlige problemer verken av driftsmessig, økonomisk eller juridisk art.

Jeg skal ikke dvele ved det som ble foreslått for 40 år siden, men trekke noen hovedlinjer fram mot i dag. For meg ble dette startskuddet til å se på digitalisering av formueretten mer generelt, som jeg har skrevet om i boken *«Formueretten i informasjonssamfunnet»* som ble utgitt i 2022.

De dyptgripende og varige endringer i den rettslige reguleringen kommer når vi gjøre noe annet, eller gjør noe på en kvalitativt annen måte enn vi gjorde det tidligere. Teknologskift som innebærer at vi grunnleggende sett gjør det samme, men med en ny teknologi, kan gi friksjon og overgangsproblemer. Det får ofte mye oppmerksomhet. Men utfordringene er gjerne av forbigående karakter.

Jeg starter med betaling. Det virkelig store skiftet kom da vi gikk over fra fysiske betalingsmidler til kontopenger: innskudd i og likvide kreditter fra banker. Utviklingen av fysiske betalingsmidler fra naturalier til sedler og mynt, lar jeg ligge. Vi betalte ikke lenger ved overlevering av fysiske betalingsmidler i en eller annen form, men ved oppdateringer i informasjonssystemer som representerte fordringer mot banker. Vi fikk det som kalles en *dematerialisering*. Verdiene var ikke lenger representert av fysiske gjenstander i form av dokumenter.

Overgangen gikk ganske langsomt, og kontanter brukes fortsatt – om enn i stadig mindre omfang. Det var først da bankene begynte å markedsføre lønnskonti med sjekker overfor privatpersoner, at bankinnskudd ble tatt i bruk som betalingsmidler fra forbrukere: «Bli sjekkis du også!», som det het i bankenes reklamekampanjer. Eller kanskje brukte bankene De-formen den gangen.

Denne langsomme overgangen illustrerer også at det nye gjerne kommer i tillegg til det gamle, det erstatter det ikke – i alle fall ikke med en gang. I dag er sjekktjenesten avviklet, noe de færreste har merket noe til. Folk hadde sluttet å bruke sjekker før tjenesten ble avviklet.

Etableringen av Verdipapirsentralen representerte et slikt skifte. Fram til dette tidspunktet hadde verdipapirer sirkulert nettopp som papirer. Det var et radikalt og brått skifte, for det ble bestemt ved lov at obligasjoner fra et visst tidspunkt ikke lenger skulle kunne sirkulere som ihendehavergjeldsbrev og aksjebrev ble avviklet i børsnoterte selskaper. Her var det ingen myk og langvarig overgang.

1 Lov om registrering av finansielle instrumenter (verdipapirregisterloven), lov 5. juli 2002 nr 64.

2 Lov om verdipapirsentraler og verdipapiroppgjør mv. (verdipapirsentralloven) lov 15. mars 2019 nr. 6.

En viss forutgående overgang hadde det likevel vært. Flere obligasjonsutstedende kredittforetak hadde etablert sine egne «papirløse» systemer. For aksjer hadde man allerede registre i form av aksjebøker, slik at der ble overgangen mindre brå. Større banker hadde etablert aksjonærservice som håndterte aksjeboken og aksjebrev i børsnoterte selskaper. Aksjebrevene var i stor grad erstattet av aksjesertifikater som kunne representere et større antall aksjer. Når aksjer ble omsatt, ble gamle aksjesertifikater makulert og erstattet av nye.

På 1990-tallet fikk «elektronisk handel» mye oppmerksomhet. Elektronisk handel er et lite egnet begrep for å avgrense virksomheten og for en rettslig kategorisering. All handel i et moderne samfunn er i alle fall for en stor del elektronisk. Det handlet mye om å rydde opp i lovbestemmelser som hindret effektiv bruk av elektronisk kommunikasjon i formuerettslige transaksjoner. Ulike formkrav kunne hindre slik kommunikasjon. Norge er et uformelt land, så vi hadde ikke veldig mange slike krav. Men vi hadde noen. Jeg har valgt å dele formkravene i tre hovedkategorier:[3]

De *primære formkrav* er formkrav som er en forutsetning for disposisjonens gyldighet. I Norge er det enklest å gå ut av formueretten, og peke på formkravene for testament. Men det finnes også slike krav i formueretten, uten at jeg går nærmere inn på disse.

De *sekundære formkrav* er formkrav som ikke er en forutsetning for transaksjonens gyldighet, men er en forutsetning for rettsvirkninger som man ønsker. En avtale om overdragelse av fast eiendom kan hos inngås muntlig. Men vil man tinglyse overdragelsen, kreves et dokument. En kredittavtale krever i utgangspunktet ingen bestemte former. Men skal en fordring være negotiabel, må formkravene for omsetningsgjeldsbrev være oppfylt.

De *tertiære formkravene* er slike som ikke er nødvendig for transaksjonen i seg selv. Men andre regler, eller bare rutiner som er etablert, er basert på at det eksisterer et dokument. Mitt favoritteksempel er da en den gangen ung forsker skulle reise på en konferanse i Stockholm på midten av 1990-talet. SAS hadde nettopp introdusert elektroniske billetter. Siden hun arbeidet med elektronisk handel, syntes hun det kunne være interessant å prøve dette. Innsjekking, sikkerhetskontroll og ombordstigning på Fornebu gikk uten problemer. Da hun skulle reise hjem fra Stockholm gikk også innsjekking og sikkerhetskontroll på Arlanda uten problemer. Men da hun kom til tax-free butikken var det stopp. Vi må ha ditt boardingkort, sa de i kassen. Hun forklarte at hun reiste med elektronisk billett og ikke hadde noe boardingkort. Men det ble ikke godtatt, så hun fikk ikke kjøpt «kvoten» på den turen. Et system som gjør at nordmenn ikke kan handle tax-free vil ikke kunne bli noen suksess, og det gikk ikke lang tid før det var ryddet opp i dette. SAS hadde tenkt på hva som var nødvendig for dem for at folk skulle kunne gjennomføre flyreisen, men tenkte ikke på at andre hadde lagt opp sine rutiner med utgangspunkt i at alle hadde dokumentet boardingkort.

Man kan møte slike tertiære formkrav på andre og i alle fall i et kommersielt perspektiv viktigere områder: Tollbehandling, finansiering, forsikring, regnskapsføring, osv. Det er vanskelig å få oversikt over alle slike formkrav, og mange holder fast ved papiret «for sikkerhets skyld».

De typiske formkrav var krav om skriftlighet og/eller underskrift. I Norge var det stort sett krav om skriftlighet med et underforstått krav om underskrift, mens det typiske i f.eks. England var et krav om «written and signed document». Man kan velge en pragmatisk tilnærming til skriftlighetskravet, slik man gjorde i forarbeidene til finansavtaleloven av 1999. Skriftlighet betyr ikke nødvendigvis et krav om papir eller en annen fysisk databærer, men at det er uttrykt ved skrifttegn.[4] I tillegg kreves gjerne en viss bestandighet og at det skriftlige skal kunne hentes fram senere.

I vår del av verden er de fleste hindringer for å kunne gjennomføre transaksjoner elektronisk ryddet av veien. Men man kan fortsatt møte dette i en del land. At hindringer er ryddet av veien, betyr ikke at alle problemer er løst. Det er ingen rettslige hindre for å legge ut på jordomseiling i en liten båt. Men det betyr ikke at det ikke medfører betydelig risiko å legge ut på en slik tur. Man bør være godt forberedt. Hvilke rettslige utfordringer som møter oss når det ikke lenger er noen rettslige skranker for å bevege seg på ut det «elektroniske havet», er til nå i liten grad behandlet. Her skal jeg tilbake til Verdipapirsentralen. En overgang fra dokumentbaserte til elektroniske transaksjoner er ikke bare et spørsmål om å «sette strøm på papiret». Transaksjonene gjennomføres på en kvalitativt annen måte, som da man for betalingstransaksjoner gikk over fra fysiske betalingsmidler til kontopenger.

Det bygges opp tjenesteinfrastrukturer. Banker er et gammelt eksempel på dette. Nå fikk vi noe tilsvarende for verdipapirmarkedet, og vi ser varianter av dette på mange områder. Et viktig element er at vi får ulike registersystemer. Den gangen kommunikasjonen var langsom ble registersystemer gjerne brukt for transaksjoner som typisk hadde høy verdi og lav transaksjonshyppighet, som fast eiendom. I markeder med større transaksjons-

3 Dette er nærmere drøftet, men langt flere eksempler i min bok «Formueretten i informasjonssamfunnet» s 107–149.

4 Ot.prp.nr.41 (1998–1999) Om lov om finansavtaler og finansoppdrag (finansavtaleloven) s. 24.

hyppighet brukte man gjerne negotiable dokumenter, som kan gå fra hånd til hånd uten at det er nødvendig å sende melding til utsteder eller et sentralt register. I dag går det raskt å sende meldinger og oppdatere registre, mens det å håndtere fysiske dokumenter er langsomt, dyrt og medfører betydelig risiko.

Det er to strategier for å få dokumentene ut av sirkulasjon. Man kan samle dokumentene i et sentralt depot, hvor det føres et register over hvem som eier dokumentene. Dette kalles *immobilisering*. Løsningen er rettslig sett enkel, da man kan beholde de gamle dokumentreglene. I noen verdipapirmarkeder har man valgt dette. Løsningen er kostbar og etter min vurdering lite praktisk. Man trenger registersystemet og i praksis er det dette som betyr noe, og i tillegg det sentrale depotet. Det er et utslag av en juridisk konservatisme og frykt for forandring, slik at papiret fungerer som en «juridisk sutteklut».

Den andre strategien er *dematerialisering*, hvor dokumentene fjernes og rettsvirkningene er knyttet til innførslene i registeret, ikke til dokumentet. Det krever at det etableres nye rettsregler gir registrene de rettsvirkninger man ønsker. Når systemet er etablert, er det enklere og rimeligere enn systemer basert på immobilisering.

Noen vil ha en «digital sutteklut» i form av digitale negotiable dokumenter. I Norge har Høyesteretts ankeutvalg i Rt-2010-604 lagt til grunn at gjeldsbrev kan være digitalt signerte, men at de ikke kan være eksigible. De viste blant annet til en uttalelse fra Justisdepartementets lovavdeling, JD-LOV-2003-3054. Negotiabilitetsspørsmålet ble ikke vurdert. Siden den gang er tvangsfullbyrdelsesloven § 7-2 endret, slik at etter første ledd, bokstav g kan en elektronisk *gjeldserklæring* være tvangsgrunnlag når kreditor er en finansinstitusjon. Man har forlatt kravet at man må bruke gjeldsbrevformen. Men slik krav kan ikke være negotiable.

I Sverige har Högsta Domstolen i NJA 2017 s. 769 konkludert med at et digitalt dokument kan være et omsetningsgjeldsbrev hvis det tilfredsstiller kravene for å være et omsetningsgjeldsbrev, herunder at det skal være et unikt originaldokument. Dette kravet var ikke oppfylt i den aktuelle saken.

I England vedtok man i 2023 en lov om dette, Electronic Trade Documents Act. Uten å gå inn i detaljer, så sier også den at slike dokumenter i prinsippet kan eksistere i digital form, forutsatt at visse grunnleggende krav er oppfylt. De kan stikkordsmessig oppsummeres som i den svenske dommen: Det må være et unikt originaldokument. I rapporten fra Law Commission[5] er man opptatt av «possession» av elektroniske dokumenter. Det blir mye «i prinsippet», og verken den svenske dommen eller den engelske rapporten og loven sier noe om hvordan dette kravet kan oppfylles i praksis. Jeg tror ikke det kan oppfylles, og derfor at konseptet er en illusjon.

Noen registersystemer er informasjonssystemer hvor de registrerte opplysninger ikke har noen selvstendig rettslig betydning, utover å kunne tjene som bevis. Det å kunne fremskaffe bevis på hva som faktisk har skjedd, kan ofte i praksis være tilstrekkelig til å løse en konflikt. Noen systemer er ikke utviklet for å være registreringssystemer, men registrerer opplysninger av andre grunner. Finanskommunikasjossystemet SWIFT oppbevarte data om gjennomførte transaksjoner først og fremst ut fra eget behov, ikke minst til fakturering. Men disse dataene ble etterspurt av partene i transaksjonene, for å kunne avklare hva slags transaksjoner som var gjennomført mellom dem. I noen land er eiendomsregistre også egentlig bare informasjonssystemer, uten den rettslige betydning som tinglysing har hos oss. I noen systemer er registrerte data bestemmende for partenes og også tredjemenns rettigheter og plikter.

Det rettslige rammeverket kan være etablert ved lov, som for tinglysing og verdipapirsentral. Eller det kan være basert på kontrakter. Det finnes noen kontraktsbaserte systemer innen shipping. For å delta i disse må man akseptere «klubbreglene», herunder at det som står i registeret har rettsvirkninger. Et lovgivningsbasert system vil har rettsvirkninger overfor alle, et kontraktsbasert system vil bare ha rettsvirkninger overfor de som er parter i avtalene, i praksis de som er medlemmer i «klubben». Hva slags betydning det som er registrert i et kontraktsbasert system vil ha i en eventuell konkurs, har ikke jeg oversikt over.

Moderne informasjonsteknologi har gjort at transaksjoner kan gjennomføres raskere og billigere enn tidligere, også over store avstander. På overflaten virker det enkelt, men under overflaten er transaksjonene gjerne langt mer kompliserte enn de var tidligere.

For noen transaksjoner vil registreringen hos en tredjepart kun ha en informasjonsfunksjon, med eller uten rettsvirkninger knyttet til registreringen, uten at de på noen måte blir part i transaksjonene. Kartverket, som i dag tar hånd om tinglysingen i Norge, blir ikke part i de transaksjoner som tinglyses. Det er transaksjoner mellom typisk en kjøper og en selger, som tinglysingen registrerer informasjon om. I en betalingstransaksjon skjer det også et oppgjør mellom en betaler og en betalingsmottaker. Men banken registrerer ikke bare hva som skjer. Den er selv part i betalingstransaksjonen. Det går fra en toparttransaksjon til det som tilsynelatende er en trekanttransaksjon, men som i realiteten er tre toparttransaksjoner, en for hver side i trekanten. Det kan også være mer enn tre «kanter» uten at jeg går inn i det. I verdipapirmar-

5 Law Commissions: Electronic trade documents: Report and Bill. Law Com No 405.

kedet er det også en del transaksjoner hvor tredjeparten går inn som part i transaksjonene.[6]

Dagens kommunikasjonsteknologi har muliggjort en globalisering. Vi får en *deterritorialisering* av transaksjonene, slik at partene kan inngå avtaler uavhengig av hvor de måtte befinne seg. Vi skal ikke så langt tilbake i tid før det stort sett bare var profesjonelle aktører som handlet internasjonalt. Nå har vi fått et stort antall internasjonale forbrukertransaksjoner.

Men også om vi holder forbrukertransaksjonene utenfor, ser vi endringer som kan gi betydelige rettslige utfordringer. I internasjonale transaksjoner kan den tredjepartstjenesten man gjør bruk av være i et tredjeland. Vi får en *reterriitorialisering*.Jeg bruker gjerne danske obligasjoner som eksempel. Spoler vi tiden drøyt 40 år tilbake, før danske VP kom i drift, kunne f. eks. en nordmann og en finne som møttes i Stockholm gjennomføre en obligasjonshandel. Man kunne utveksle inhendehaverobligasjoner og kontanter. Antagelig ville avtalen mellom selger og kjøper i utgangspunktet være underlagt svensk rett, men partene kunne ha avtalt at et annet lands rett skulle gjelde. I dag gjennomføres oppgjøret i Danmark og er underlagt dansk rett. Dette kan partene ikke avtale seg bort fra.

I betalingstransaksjoner vil det endelige oppgjøret alltid skje i valutalandet. Et oppgjør i NOK skjer i Norges Bank, mens et oppgjør i USD skjer i Federal Reserve i New York, uavhengig av hvor i verden partene måtte befinne seg. USA har få hemninger mot å gripe inn i transaksjoner mellom tredjeland, slik at det å velge verdens mest brukte valuta til internasjonale betaler, kan medføre en viss politisk risiko.[7]

Globalisering av transaksjoner innebærer at verden må synkroniseres, i alle fall når det gjelder gjennomføring av visse transaksjoner. For 50 år siden, i 1974 lærte finansnæringen hva slags risiko tidsforskjeller kan medføre. Den tyske banken Herstatt bank var meget aktiv, det er fristende å si hyperaktiv i valutamarkedet. Banken hadde hatt store tap og hadde en rekke ganger overskredet grensen for hvor store transaksjoner den kunne foreta. Det var den gangen vanlig at oppgjøret skjedde en gang om dagen, typisk etter at markedet lukket. Banken hadde kjøpt tyske mark som skulle betales i US dollar. Etter at markedet i Frankfurt var lukket og oppgjøret gjennomført slik at banken fikk sine tyske mark, ble banken satt under administrasjon. På grunn av tidsforskjellen gikk det noen timer før oppgjøret i US dollar skulle gjennomføres i New York. Da var Herstatt bank en insolvent bank under administrasjon. Det ble noen rettssaker på begge sider av Atlanteren. Resultatet ble at Herstatt bank, eller dens bo fikk beholde det den hadde mottatt av tyske mark, mens kreditorene som skulle hatt betaling i US dollar ikke fikk noe. Dette satte fart i utviklingen av sanntidssystemer som gjør at handler kan gjøres opp døgnet rundt. Det har også kommet regler for å håndtere slike situasjoner.

For transaksjoner som gjelder store beløp, som det ofte vil være i finansmarkedene, er prinsippet om samtidig utveksling av partenes ytelser viktig. I dokumentbaserte systemer med kontant oppgjør, kunne man levere verdipapirene med en hånd og samtidig ta imot kontanter med den andre. I de elektroniske markedene må flere systemer synkroniseres, slik at overføringene i begge systemer skjer på samme tidspunkt. Jeg har brukt verdipapirmarkedet og valutamarkedet som eksempler. Men det er mange markeder som fungerer på samme måte. Råvaremarkedene er i stor grad finansmarkeder, med tilsvarende oppgjør.

Det bør ikke overraske at globalisering medfører at spørsmål om jurisdiksjon og lovvalg får langt større betydning enn de hadde tidligere. En litt spesiell variant har vi når det gjelder rettigheter i luftfartøy. Etter den norske luftfartsloven skal rettsstiftelser i norske luftfartøy registreres i luftfartøysregisteret. I medhold av Cape Town-konvensjonen[8] er det opprettet et *International Registry of Mobile Assets* i Dublin internasjonale interesser. Hva som er nasjonale interesser i luftfartøy som skal registreres i luftfartøysregistre, og hva som er internasjonale interesser i norskregistrerte luftfartøy hvor i alle fall rettsstiftelser skal registreres i Dublin, er for meg temmelig uklart. Det blir ikke enklere av at det som skal registreres i luftfartøysregisteret er rettsstiftelser i selve luftfartøyet, mens det som skal registreres i Dublin er rettsstiftelser i flyskrog og flymotorer.

De nye tjenesteinfrastrukturene som bygges opp er i liten grad undersøkt. Vi vet lite om hvordan de er bygget opp, og også ofte lite om hva de gjør. De rettslige sidene ved virksomhetene, både når det gjelder selve organiseringen og de tjenester som ytes, er i liten grad undersøkt. Jeg er ganske sikker på at det her vil være grunnlag for flere doktoravhandlinger.

Olav Torvund er professor ved Institutt for privatrett/SERI. Han ble ansatt som vitenskapelig assistent i 1982, og har for det mest vært der siden. I 1984 tok han, sammen med Cecilia Magnusson Sjöberg initiativ til Nordisk årbok i rettsinformatikk. Olav Torvund har særlig arbeidet med elektroniske transaksjoner, samt opphavsrett og ytringsfrihet og har publisert bøker om disse temaene.

6 Igjen viser jeg til mer utførlige drøftelser i min bok «Formueretten i informasjonssamfunnet» s. 332–336.

7 Se nærmer «Formueretten i informasjonssamfunnet» s. 397–403.

8 Cape Town Convention on Internatinoal Interests in mobile Equipment fra 2001.

Statlige IT-anskaffelser og IT-anskaffelseskontrakter i Norge – Utviklingstrekk og erfaringer[1]

Av Arve Føyen

1. Innledning

Denne artikkelen gir en oversikt over utviklingen og erfaringene med statlige IT-anskaffelser og IT-anskaffelseskontrakter i Norge. Den tar for seg historiske utviklingstrekk fra 1970-tallet til i dag, og hvordan standardavtaler har bidratt til å skape forutsigbarhet og balanse i markedet. Videre belyses endringer i terminologi og kontraktstyper, samt viktige milepæler som IBMs markedsdominans og den påfølgende antitrustsaken. Artikkelen diskuterer også utviklingen av Statens standardavtaler (SSA) og utfordringer knyttet til sentralisering versus lokal selvbestemmelse i IT-anskaffelser. Til slutt ser den på fremtidige trender og utfordringer, inkludert innkjøpsstrategier for skytjenester og behovet for nye juridiske rammer i møte med teknologisk utvikling.

2. Bakgrunn

a. Innledning og litt terminologi

Standardavtaler for EDB (elektronisk databehandling) har gjennomgått en betydelig utvikling siden de første norske avtalene ble utformet på 1970-tallet. I en tid preget av teknologisk usikkerhet og begrenset brukerkompetanse, ble standardiserte kontrakter avgjørende for å sikre forutsigbarhet og balanse i forholdet mellom leverandører og kunder. Denne artikkelen gir en oversikt over utviklingen av slike avtaler i Norge, deres historiske bakgrunn, og hvordan de har bidratt til struktur og balanse i et dynamisk marked.

Arve Føyen

Terminologien i IT-bransjen har utviklet seg i betydelig grad fra 1950-tallet til i dag. Utviklingen reflekterer både teknologiske gjennombrudd og samfunnets økende avhengighet av digitale løsninger.

De tidligste maskinene ble kalt *«regnemaskiner»* eller *«datamaskiner»*, og de var ofte enorme maskiner brukt til komplekse beregninger i forskning og militæret.

«Stormaskin», eller *«Mainframe»* beskrev store, kraftige datamaskiner som IBM 704 og UNIVAC. Stormaskiner ble brukt av store organisasjoner til tunge beregningsoppgaver.

«Programvare» eller *«Software»* ble i den tidlige tiden brukt mest om maskinens kontrollprogrammer (operativsystem mv), mens mye av applikasjonsprogrammene fremdeles var maskinvarebasert.

> Terminologien i IT-bransjen har utviklet seg i betydelig grad fra 1950-tallet til i dag. Utviklingen reflekterer både teknologiske gjennombrudd og samfunnets økende avhengighet av digitale løsninger.

På 1970-tallet kom fremvekst av minidatamaskiner og personlige datamaskiner (PCer).

Med lanseringen av IBM-PCen i 1981 ble «PC» et vanlig begrep som beskrev rimelige og små maskiner for privatpersoner og kontorbruk. Ettersom programvaremarkedet vokste, begynte bransjen å selge «programvarepakker» som Microsoft Office, med flere applikasjoner som kunne dekke et bredt spekter av behov.

Uavhengig av størrelse og kapasitet ble samlebetegnelsen «EDB» (Elektronisk Databehandling) mye brukt, og utstyre ble kalt for «EDB-maskiner», «EDB-utstyr» eller «EDB-utrustning». Senere har betegnelsen «IT-utstyr», «PC», Lap-top» og «Programvare» blitt mer vanlig.

b. Avtaletyper

EDB-avtaler omfatter avtaler for anskaffelse, vedlikehold og bruk av

1 Deler av fremstillingen i denne artikkelen er basert på kapittel 1-3 i boken *«Kontrakter for utvikling av programvare»,* Cappelen Damm Akademisk 2006 Red: Føyen, Arve Madsen, Kristine M. Klüwer, Christine

utstyr og programvare, samt levering av tjenester som konsulentbistand og utvikling av spesialtilpasset programvare. Eksempler på slike avtaler inkluderer kjøpsavtaler, lisensieringskontrakter, driftsavtaler, tilpasningsavtaler og kontrakter for teknisk vedlikehold.

Standardavtaler er utarbeidet for gjentatt bruk innen samme type transaksjoner. Det finnes to hovedtyper av standardavtaler. For det første ensidig utformede avtaler, ofte laget av henholdsvis leverandørsiden eller kundesiden. Dernest har vi standardavtaler som er utarbeidet og fremforhandlet av representanter for både kunder og leverandører. Sistnevnte avtaletype søker å balansere partenes interesser, men har vært mindre vanlig i EDB-sektoren, hvor leverandørens standardvilkår lenge dominerte.

c. Utviklingen i anskaffelse av datamaskiner

Datamaskiner fikk gradvis innpass i Norge fra slutten av 1950-tallet. Mange forstod at datamaskiner kunne brukes både til matematiske beregninger, og til administrative funksjoner i offentlig forvaltning og i privat næringsliv.

På 1960- og 1970-tallet var IBM den helt dominerende leverandøren av datamaskiner og tilhørende programvare. Opprinnelig solgte IBM sine stormaskiner som en helhetspakke, hvor både maskinvare og programvare ble levert samlet uten separat betaling for programvaren. Programvare og tjenester ble sett på som en del av verdien til eller egenskapene ved maskinvaren. Kunder som kjøpte IBM-datamaskiner, fikk tilgang til IBMs programvare uten tilleggskostnader («bundling»). På slutten av 1960-tallet begynte imidlertid det amerikanske justisdepartementet å undersøke IBM for mulige antitrust-brudd.

Bundling av maskiner med programvare og tjenester, sammen med IBMs sterke markedsstilling gjorde det svært vanskelig for andre aktører å komme inn på markedet. Mot slutten av 1970-tallet hadde IBM ca 70% markedsandel i markedet for stormaskiner (i USA). Det amerikanske justisdepartementet reiste en omfattende antitrustsak mot IBM i 1969 på grunn av IBMs dominerende posisjon. Saken var en av de lengste og mest kjente antitrustsakene i amerikansk historie og varte i nesten 13 år før den ble avsluttet uten dom i 1982.

Bl a. på grunn av antitrustsaken besluttet IBM å skille maskinvare fra programvare og tjenester. («unbundling»). Fra 1969 begynte de å prise programvare separat, noe som gjorde det mulig for kunder å kjøpe kun programvare eller tjenester uten å være bundet til IBMs maskinvare.

Selv om antitrustsaken ble avsluttet uten dom, hadde den stor betydning for IT-bransjen. Den bidro til å åpne markedet for nye aktører og akselererte utviklingen av en konkurransepreget programvareindustri. I tillegg etablerte den presedens for regulering av teknologiselskaper med stor markedsmakt, noe som har påvirket senere antitrustsaker mot andre store teknologiselskaper som Microsoft på 1990-tallet og Google og Amazon i nyere tid.

3. Anskaffelseskontraktene – Statens standardavtaler for IT-anskaffelser (SSA)

a. Anskaffelser av EDB-maskiner og programvare

På 1970-tallet var det som nevnt leverandørenes egne standardformularer som preget markedet, spesielt i privat sektor. Disse var ofte direkte oversettelser av amerikanske kontrakter, som hverken var tilpasset norsk språk eller lovgivning.

Et problem i denne perioden var mangelen på forståelige kontraktsvilkår og systematikk, noe som førte til hyppige misforståelser og konflikter. Leverandørene (de norske salgsselskapene – datterselskap av de store utenlandske leverandørene) tilbød ofte «side letters» som fravek standardformularene, noe som skapte manglende oversikt og juridisk usikkerhet. I flere tilfelle førte slike side letters til at ledelsen i norske «døtre» ble sparket på grunn av avvik fra selskapets kontrakts-policy.

IBMs dominerende stilling også i det norske markedet medførte at det var IBMs kontraktsvilkår og leveranseavtaler som var nærmest enerådende i det Norske markedet på 1960-tallet, og gjennom store deler av 1970-tallet. Alle de øvrige leverandørene (f. eks. Univac, Honeywell Bull, Burroughs, Control Data og Hewlett Packard) fulgte IBMs eksempel og benyttet liknende kontrakter. Spesifikasjoner for leveranser var basert på maskinens tekniske egenskaper, snarere enn på funksjonelle krav fra kjøpersiden.

Historien om statlige EDB-anskaffelseskontrakter i Norge begynner på 1970-tallet. Dette var en tid preget av rask teknologisk utvikling og et økende behov for effektivisering av offentlige tjenester. I denne perioden var EDB, og EDB-avtaler et relativt nytt felt, og mange av de avtalene som ble inngått var preget av manglende erfaring og forståelse av kundenes funksjonelle behov.

I min spesialfag-avhandling fra 1972–73 til juridisk embetseksamen skrev jeg om «Ansvarsfraskrivelser i edb-kontrakter». Der påpekte jeg at det var betydelige utfordringer knyttet til de kontraktene som ble benyttet i bransjen på grunn av leverandørenes massive ansvarsfraskrivelser. Som konsulent i Statens Rasjonaliseringsdirektorat (forløperen til Digitaliseringsdirektoratet og DFØ) fra 1974 til 1979 fikk jeg i oppdrag å arbeide med videreutvikling av Statens standardavtaler (SSA). Målet var å sikre bedre og mer rettferdige avtalevilkår for staten ved anskaffelse av EDB-utrustning fra dominerende leverandører, og skape mulighet for Norske leverandører til å bli med i konkurransen.

På 1960- 1970- og 1980-tallet var «EDB-avtaler» primært knyttet til

kjøp av hardware og lisenser for programvare. En interessant trend på 1990-tallet var fremveksten av «shrink-wrap»- og «click-wrap»-avtaler, som ofte følger med programvareprodukter. Disse avtalene ble kritisert for å utfordre etablerte prinsipper for avtaleinngåelse, men de ble likevel vanlige i programvaremarkedet.

> Historien om statlige EDB-anskaffelseskontrakter i Norge begynner på 1970-tallet. Dette var en tid preget av rask teknologisk utvikling og et økende behov for effektivisering av offentlige tjenester.

b. IKT- og digitaliseringspolitikk

Fremveksten og utviklingen av en norsk IKT-politikk har siden starten på 1960-tallet vært preget av en konflikt mellom ønsket om sentral styring og kontroll med utviklingen og utnyttelse av statens innkjøpsmakt på den ene siden, og ønsket om lokal selvbestemmelse og tilrettelegging for et fritt fungerende marked med rom for lokale leverandører på den annen side. [2]

Denne utviklingen har i perioder svingt mellom initiativ for sentral styring og samordning på den ene side, og frislipp av kategorien «la de tusen blomster blomstre», med frivillighet og lokal selvstendighet og selvstyre på den andre siden. I nevnte artikkel av Arild Jansen (se fotnote 2), fremgår at:

> *«Konfliktene har omhandlet anskaffelser av datakraft, felles maskinteknisk[e] plattform[er], spørsmål om utvikling og bruk av felles programsystemer, felles dataregistre, samordning og standardisering, rammeavtaler med mer. Den datatekniske utviklingen fra tidlig 50-tall til i dag innebærer så vel teknologiske som organisatoriske og bruksmessige revolusjoner.»*

Artikkelen beskriver på en utmerket måte de konfliktlinjene som eksisterte (og fortsatt eksisterer) knyttet til styring av IKT-politikken og digitaliseringen av det offentlige Norge.

Rådet for Databehandling i Staten («DB-rådet») ble opprettet ved kgl.res. av 23. mars 1961, for å kvalitetssikre IT-anskaffelser. Mandatet ble fornyet ved kgl.res. av 3. mai 1974. I henhold til dette skulle alle større IT-anskaffelser i staten (med verdi over kr. 200 000) forelegges for Rådet til (rådgivende) uttalelse, og det skulle redegjøres for hvordan norskprodusert utstyr er vurdert i anskaffelsen. Rasjonaliseringsdirektoratet var sekretariat for rådet, og direktoratet ga bistand med anbudsinnbydelser, evaluering av tilbud og kontraktsforhandlinger til statsinstitusjoner som ønsket det. Rådet ble nedlagt i 1981, etter fremleggelsen av NOU 1978:48 «Desentralisering og effektivisering av offentlig databehandling»[3] som ble behandlet i St.meld. nr. 12 (1982–83). [4]

c. Statens standardavtaler

Rådet for databehandling i staten så at leverandørenes avtaler var svært ufordelaktige og utilstrekkelige. Det tok derfor initiativet til å lage de første standard avtaleformularene om henholdsvis kjøp og vedlikehold av EDB-utstyr (SSA-K og SSA-V).

De første avtalene ble laget på begynnelsen av 1970-tallet av h.r. adv. Ole Torleif Røed, direktør Svein A. Øvergaard i Administrasjonsdepartementet og Per Scott som ledet arbeidet fra Rasjonaliseringsdirektoratets side.[5] Jeg overtok dette arbeidet som nyansatt jurist i Rasjonaliseringsdirektoratet i 1974, og hadde hovedansvaret frem til 1979.

Senere har arbeidet vært ledet av ansatte i Rasjonaliseringsdirektoratet og dets etterfølgere (Statskonsult, Statskonsult AS, Direktoratet for forvaltning og IKT, Digitaliseringsdirektoratet og fra 1.9.2020 Direktoratet for forvaltning og økonomistyring (DFØ)).

Andre som aktivt har bidratt i revisjoner av avtalene er b. a. Senter for rettsinformatikk (SERI) ved det Juridiske fakultet, Universitetet i Oslo og senere også innleide eksterne advokater. Fra 2015-revisjonen har også IKT-Norge (forening for IKT-leverandører) bidratt aktivt i revisjonsarbeidet, med bistand fra eksterne advokater.

Disse standard avtaleformularene har nå en over 50-år gammel historie og har blitt revidert og tilpasset gjennom årene i takt med utviklingen av teknologi og endringer i markedet.

d. Hensynet bak utviklingen av Statens standardavtaler

De første standardavtalene ble utviklet for å styrke statens forhandlingsposisjon overfor leverandørene. I samarbeid med Industridepartementet ble det lagt til rette for norsk dataindustri, og det ble gjennomført prosjekter for forskning og utvikling (Dette var før innføringen EU's anskaffelsesregler, og det var noe videre rom for tilrettelegging for nasjonale industripolitiske retningslinjer). Dette sammen med krav om at anbudsinnbydelser skulle legge til rette for mulige tilbud fra norske leverandører førte til et betydelig oppsving for norske leverandører – særlig for Norsk Data AS.

Norsk Data hadde på 1970- og 1980-tallet betydelig suksess i det

2 Jansen, Arild Fra Emma til MinSide, side 6 flg. *https://www.jus.uio.no › afin › EMMA2007_AJ,*

3 NOU 1978:48 «Desentralisering og effektivisering av offentlig databehandling».

4 St.meld. nr. 12 (1982–83).

5 https://anskaffelser.no/avtaler-og-regelverk/statens-standardavtaler-ssa/ssa-enes-historie-og-bakgrunn

norske og internasjonale markedet, noe tidligere generalsekretær i IKT-Norge, Per Morten Hoff, påpeker i forordet til boken «Norsk Data – hva gikk galt»[6]. Det fremgår der at:

> *«ND var gjennom mange år en stor økonomisk suksess. ND ble det første norske selskap notert på London Stock Exchange i 1981 og NASDAQ i 1983. «Det er kun Norsk Hydro som i samme periode hadde høyere børsverdi av norske selskaper. ND var i sin storhetstid noe så sjeldent som en norsk høyteknologibedrift som kunne nyte verdensomspennende anerkjennelse.»*

Kombinasjonen av industripolitiske retningslinjer, Rådet for Databehandling i Staten/Rasjonaliseringsdirektoratet og utviklingen av de kundeutformede Statens Standardavtaler var medvirkende til Norsk Datas suksess på 1980-tallet. Norsk Data sine løsninger fikk i Norge særlig stor utbredelse i offentlig forvaltning.

> De første standardavtalene ble utviklet for å styrke statens forhandlingsposisjon overfor leverandørene.

På slutten av 1980-tallet og begynnelsen av 1990-tallet var tiden for såkalte minimaskiner i ferd med å løpe ut, og det samme gjaldt proprietære løsninger. Flere av de internasjonale aktørene baserte seg på varianter av Unix operativsystem, som (med visse modifikasjoner) gjorde det mulig å kjøre den samme applikasjonsprogramvaren på utstyr fra forskjellige leverandører. Det medførte større fleksibilitet for kundene til å kjøpe maskinvare fra forskjellige leverandører, og unngå innelåsingseffekter i forhold til én enkelt leverandør. Personlige datamaskiner tok over, og det ble i bransjen et fokus på horisontal integrasjon basert på standarder.[7]

Med fremveksten av nye teknologier, ble det utviklet flere spesialiserte avtaler, som konsulentavtaler utviklingsavtaler og tilpasningsavtaler, samt driftsavtaler, for å møte de spesifikke kravene i markedet. Programutviklingsavtalen (SSA-U) og tilpasningsavtalen (SSA-T) ble introdusert for å håndtere nye former for programvareutvikling og tilpasning av standardløsninger. Det finnes i dag en rekke forskjellige kontrakts-standarder på anskaffelser.no[8]

e. Endringer i innkjøpsstrategier og anskaffelse av skytjenester

Mot slutten av 1990-tallet og begynnelsen av 2000-tallet ble Forvaltningsnettsamarbeidet (FNS) etablert. Dette var opprinnelig et samarbeid mellom staten ved Arbeids- og administrasjonsdepartementet (AAD) og kommunene ved Kommunenes Sentralforbund. Formålet var å etablere en felles innkjøpsordning på tele- og dataområdet for hele offentlig sektor. Nye rammeavtaler som skulle forenkle prosessen og sørge for at offentlige etater kunne dra nytte av bedre priser og betingelser ble utlyst[9]. Forvaltningsnettavtalene ble lagt inn i Statens Forvaltningstjeneste/Statskjøp i 2000. Sentraliseringen av innkjøpsmakt førte imidlertid til en utfordring med hvordan man skulle balansere hensynet til lokalt næringsliv og fri konkurranse i markedet med behovet for kostnadseffektivitet i offentlige innkjøp. Statskjøp ble nedlagt, og Forvaltningsnettavtalene ble avviklet i april 2002 med begrunnelsen (v/arbeids- og administrasjonsminister Victor D. Norman):

> *«… at statlige innkjøp i prinsippet er et desentralisert ansvar, dvs. at den enkelte virksomhet skal være direkte ansvarlig for egen innkjøpsvirksomhet. En for stor sentralisering av innkjøpene medfører etter ministerens mening en fare for at staten kan utøve en innkjøpsmakt som reduserer konkurranse og effektivitet»*[10]

Anskaffelser.no under DFØ har i dag et rikholdig utvalg av standardavtaler og veiledninger for valg av avtalemal, og for bruk av de enkelte avtalemalene. Nye maler har blitt utviklet etter hvert som markedet og leveransemodellene har endret seg.

Med fremveksten av skytjenester har vi sett en ny utvikling i avtalestrukturen. Leverandørstyrte standardkontrakter har blitt mer vanlige, og disse er ofte ikke tilpasset individuelle kunders behov. Det er nærliggende å trekke parallellen tilbake til IBM, og de øvrige leverandørenes kontrakts-praksis på 1960- og 70 tallet. Det er også en økende bekymring rundt knyttet til innelåsingseffekter, rettigheter til data, personvern, sikkerhet og sårbarhet. Dette er særlig aktuelt, ettersom mange av de største leverandørene er amerikanske selskaper med datasentre i mange jurisdiksjoner rundt i verden, og det det i utgangspunktet kan være full replisering av data på tvers av regionene.

> Med fremveksten av skytjenester har vi sett en ny utvikling i avtalestrukturen.

6 «Mysteriet Norsk Data - hva gikk galt?» Alfatroll Tor Olav Steine Forlag 2020.

7 Jfr Arild Haraldsen *«Arven etter Rolf Skaar»* i Computerworld Norge, 30.5.2023

8 *https://anskaffelser.no/avtaler-og-regelverk/statens-standardavtaler-ssa*

9 Jfr. *Samordning av statlige innkjøp* Kapittel 4.3 (Oslo Economics-rapport 2011-8), s 41 flg.

10 Jfr. *Samordning av statlige innkjøp* Kapittel 4.3 (Oslo Economics-rapport 2011-8), s 43

Staten har i dag en ambisiøs agenda for å styre mer av sine IT-kjøp, med en tydelig retning mot å sentralisere innkjøpene for å oppnå bedre vilkår og priser. Dette har ført til en debatt om hvordan det påvirker små og mellomstore bedrifter, som ofte føler seg utestengt fra konkurransen om store offentlige kontrakter.[11]

Ett eksempel er etableringen av «markedsplass for kjøp av skytjenester» som ble etablert i 2020. Om etableringen het det i statsbudsjettet for 2020 at «Markedsplassen skal gjøre det enklere for virksomhetene å anskaffe sikre, lovlige og kostnadseffektive skytjenester, gi dem oversikt over tilbudet i markedet, prosesstøtte i anskaffelsesprosessen, og støtte til sikkerhets- og risikovurderinger.» Markedsplassen og rammeavtalene som inngås med leverandører skal kunne brukes av statlige etater, kommuner og fylkeskommuner og av leverandørmarkedet for rådgivning om og tilbud av skytjenester.

4. Standard avtalemaler utviklet utenom staten

I løpet av 1980-årene modnet kontrakts-praksis i bransjen, og aktører på både kunde- og leverandørsiden fikk økt kompetanse. Dette tiåret så også fremveksten av balanserte standardavtaler, som Den Norske Dataforeningens (DND) kontrakter fra 1982. Disse ble utformet for å ivareta kundenes interesser, men ga samtidig leverandørene rom for nødvendige tilpasninger.

Senere ble også kontrakts-standarden PS2000 ble utviklet under forskningsprogrammet Prosjektstyring 2000 i regi av NTNU og SINTEF. Kontrakts-standarden ble utviklet for prosjekter innen systemutvikling eller systemleveranser hvor det ikke er hensiktsmessig eller mulig å fastsette nøyaktig eller detaljerte spesifikasjoner i forkant av prosjektet, og den tok sikte på utvikling basert på iterativ metode. Etter at forskningsprogrammet ble avsluttet, har Den Norske Dataforeningen (DND) ved faggruppen for IT-kontrakter, påtatt seg et ansvar for forvaltning og videre utvikling av kontraktstandarden.[12]

5. Veien videre

Fremover vil det være avgjørende å navigere gjennom de utfordringene som har oppstått som følge av teknologisk utvikling. Det vil nødvendigvis innebære en balansegang mellom å sikre gode avtalevilkår for staten og å opprettholde et konkurransedyktig marked for leverandører, inkludert små og mellomstore bedrifter.

Det er også viktig å vurdere hvordan endringer i teknologi, som AI og cloud computing, edge computing og økende omlegging til microtjenestearkitektur, vil påvirke fremtidens IKT-anskaffelser og hvilke juridiske rammer som må utvikles for å håndtere disse nye utfordringene.

Arve Føyen er advokat i enkeltmannsfirma, og arbeider med IKT-juridiske problemstillinger, personvern, juridiske problemstillinger vedrørende Internett, rettigheter til data, programvare og innhold, tilgang til offentlig informasjon og offentlige anskaffelser. Han har lang erfaring med utvikling og bruk av standardkontrakter for IKT-anskaffelser og andre IKT-juridiske problemstillinger og problemstillinger vedr. elektronisk kommunikasjon, arbeider som eksternt personvernombud i flere virksomheter, og benyttes ofte som voldgiftsdommer eller sakkyndig meddommer i tvister for ordinære domstoler.13

11 Jfr. *Artikkel av Lennart Hovland i Anbud 365*, 1. februar 2019

12 *Kilde: Wikipedia*

13 Deler av fremstillingen i denne artikkelen er basert på kapittel 1–3 i boken *«Kontrakter for utvikling av programvare»*, Cappelen Damm Akademisk 2006 Red: Føyen, Arve Madsen, Kristine M. Klüwer, Christine

Referanseliste:

1. Føyen, Arve; Madsen, Kristine M.; Klüwer, Christine (2006). *Kontrakter for utvikling av programvare*. Cappelen Damm Akademisk.
2. Jansen, Arild. *Fra Emma til MinSide*. Innhentet fra: https://www.jus.uio.no/afin/EMMA2007_AJ
3. NOU 1978:48 «Desentralisering og effektivisering av offentlig databehandling»
4. St.meld. nr. 12 (1982–83)
5. https://anskaffelser.no/avtaler-og-regelverk/statens-standardavtaler-ssa/ssa-enes-historie-og-bakgrunn
6. Hoff, Per Morten (2020). *Mysteriet Norsk Data - hva gikk galt?* Alfatroll Tor Olav Steine Forlag.
7. Haraldsen, Arild (2023). *Arven etter Rolf Skaar*. Computerworld Norge, 30. mai 2023.
8. https://anskaffelser.no/avtaler-og-regelverk/statens-standardavtaler-ssa
9. Oslo Economics (2011). *Samordning av statlige innkjøp Kapittel 4.3, s. 41 flg. (Oslo Economics-rapport 2011-8).*
10. Oslo Economics (2011). *Samordning av statlige innkjøp Kapittel 4.3, s. 43 (Oslo Economics-rapport 2011-8).*
11. Hovland, Lennart (2019). Artikkel i Anbud 365, 1. februar 2019.
12. https://no.wikipedia.org/wiki/PS2000

Arbeider med juridiske ekspertsystemer ved Institutt for rettsinformatikk for 40 år siden

Av Johs Hansen Hammer

Først vil jeg få gratulere med jubileet og takke for spalteplass i Lov og Data i jubileumsnummeret. Det innlegg jeg skrev til nr. 1/ 1984 av Lov og Data, kalt *Taxman og Legol: To prosjekter innen normmodellering*, omtalte studieturer jeg hadde til hhv. London School of Economics (LSE) og Rutgers University i New Jersey. Ved Institutt for Rettsinformatikk (IRI) arbeidet vi med ekspertsystemer på det juridiske området. Med studieturene ønsket vi å studere tilnærmingene som var valgt ved LSE og Rutgers til bruk i forbindelse med egne valg.

I dag er Kunstig Intelligens (KI) på mange områder langt utviklet. Med tanke på utvikling innen det juridiske området kan det ha interesse å se tilbake på noe av IRI's arbeide innen ekspertsystemer for ca. 40 år siden.

Jeg tar like godt opp tråden fra artikkelen: I London arbeidet Ronald Stamper og medarbeidere med utvikling av et programmeringsspråk de kalte LEGOL (Legally Oriented Language). Ved Rutgers arbeidet L. Thorne McCarty og medarbeidere med et prosjekt og system kalt Taxman. Her uttrykte de bla. skatteregler for å kunne gjøre analyser av skatteforhold. Dette var to store satsninger på utvikling av juridiske ekspertsystemer på den tiden.

Ved Institutt for rettsinformatikk hadde vi siden 1978 utviklet *System for Analyse av Rettslige Avgjørelser* (SARA). Systemet kunne brukes til å analysere et sett av skjønnsbaserte

Johs Hansen Hammer

avgjørelser hvor problemstillingen var den samme. Senere arbeidet vi ved instituttet med å utvikle *Språk for modellering av rettslige normer* (SMARN). Vi ønsket å kunne simulere rettslige beslutninger for å studere virkninger av et regelverk på en populasjon.

> I dag er Kunstig Intelligens (KI) på mange områder langt utviklet. Med tanke på utvikling innen det juridiske området kan det ha interesse å se tilbake på noe av IRI's arbeide innen ekspertsystemer for ca. 40 år siden.

Etter at jeg ble cand. real i informatikk sommeren 1981, var det min plan å skrive en dr. scient-avhandling med tittel *Matematisk modell av rettslige normstrukturer. Analyse av avveiinger og simulering av komplekse beslutninger*. Mine veiledere var, som for min hovedfagsoppgave, Jon Bing ved IRI og Sverre Spurkland ved Institutt for informatikk. For avhandlingens del arbeidet jeg med en notasjon for å kunne uttrykke meningsinnhold for *pliktnormer* i.

Arbeidet ved IRI med ekspertsystemer er dokumentert i skriftseriene Jus og EDB, hhv CompLex. Publikasjoner i CompLex er tilgjengelige fra denne nettsiden:

https://www.jus.uio.no/ifp/forskning/om/publikasjoner/complex/

System for analyse av rettslige avgjørelser

For en jurist kan det være utfordrende å analysere et materiale av mange avgjørelser truffet ved skjønn, særlig hvor mange momenter kan være relevante. Uten at det er direkte uttrykt i en beslutning, eller at det er gitt retningslinjer om vekting for avveiingen, kan det være krevende å forstå hvordan ulike momenter er vektlagt.

Til grunn for IT-systemet SARA lå en modell for skjønn kalt *vekttallsregelen*. Den var utarbeidet av den juridiske nestor, Torstein Eckhoff, m.fl. Det er en noe forenklet modell av avveiinger. Den bygger på en antakelse om at samme moment vil vektlegges noenlunde likt i de avveiinger hvor momentet er relevant. Vi kunne da gjøre bruk av en såkalt *lineær* modell for å representere beslutningene.

Det falt i min lodd, som informatiker, å designe og programmere systemet SARA. Stud. jur. Mette Borchgrevink hadde ansvaret for den juridiske tilrettelegging og gjennomføring av analyse av et innsamlet materiale av beslutninger. Det var mer enn 200 saker fra Distriktenes Utbyggingsfond (DUF), samlet inn, tilrettelagt og alt analysert av Erik Boe i hans arbeide med sin dr.juris-avhandling[1]. Resultatene av våre analyser ble vurdert, drøftet og dokumentert av Mette Borchgrevink.

SARA hadde et sett av funksjoner for å registrere og analysere sakene. Av særlig interesse var det å undersøke vekting av momenter. SARA hadde et opplegg for å lære om vektingen og beregne vekter. Om brukeren syntes SARA la for mye eller for lite vekt på et moment, kunne denne legge inn en maksimums- og/eller en minimumsgrense for momentets vekt. I senere versjoner kunne brukeren også undersøke hvordan, gitt de beregnede vektene, variasjon av vekt for ett moment påvirket antallet beslutninger hvor beregnet resultat ble feil, dvs. ikke det samme som faktisk resultat.[2] Slik fikk vi et uttrykk for «følsomheten» antallet beslutninger med feil teoretisk resultat hadde for variasjon av vekt for momentet.

I det lille, internasjonale miljøet som var innen rettsinformatikk på denne tiden, var det nokså stor interesse for arbeidet vårt. Det ble presentert ved ulike konferanser. Gjesteforskere og studenter fra flere land kom til Oslo for å sette seg inn i arbeidet. Vi fikk tilbakemeldinger fra mange kollegaer. Noen av disse betraktningene er publiserte.[3]

Jeg hadde et stort tilfang av tilbakemeldinger å gjøre bruk av da jeg videreutviklet SARA for min hovedfagsoppgave i informatikk[4]. Likevel var det Sverre Spurklands brede kunnskap innen matematikk og egne studier av matematisk teori, som fikk mest betydning for den teoriutvikling og de forbedringer som nå fant sted i arbeidet med SARA. I tillegg til hovedoppgaven er også brukerveiledning og programdokumentasjon for SARA publisert.[5]

Juridiske begreper fikk sin matematiske fortolkning. Et par eksempler kan være *motstrid* mellom beslutninger og *presedens* for en beslutning. Innen modellen, og gitt positivt utfall av sakene, så vil det å føye til et proargument opprettholde resultat, likeså å fjerne et motargument. I så fall danner den ene sak presedens for den andre. Men presedens kan også framstå ved at flere beslutninger sammen danner presedens for en annen.

SARA hadde sin variant av det som innen Kunstig Intelligens (KI) kalles maskinlæring. For å lære om vektingen av momenter i sakene baserte vi oss på hver enkelt beslutnings verdier og resultat. Dataene fra alle beslutningene ble benyttet til læring. Ved læringen ville vi finne vekter hvor det teoretiske resultatet for så mange beslutninger som mulig var riktig (1. prioritet), og sammen av feilene for de teoretiske resultater, hvor disse var feil, var så lavt som mulig (2. prioritet). Vektene ble beregnet i et antall *iterasjoner*, helt til tilstrekkelig forbedring verken kunne finnes i form av lavere antall feil eller i form av lavere sum av feil for teoretiske resultater.

SARA garanterte ikke optimal løsning, slik at maksimalt antall saker som samtidig lot seg forklare ville bli funnet.

Brukeren kunne nytte mange ulike kommandoer for å lære om materialets egenskaper. For flere av disse var det mulig å benytte *velgere*, f. eks. for å velge saker kommandoen skulle kjøres for, for å velge avstanden mellom de punkter en funksjon skulle plottes for, etc. Enkelte typer velgere kunne kombineres, slik at fleksibiliteten i bruk av kommandoer og velgere var nokså stor.

SARA ble utover utviklingsarbeidet bare i nokså liten utstrekning benyttet til analyse. En anvendelse som fikk god oppmerksomhet var Jon Bings analyse av 9 beslutninger presenterte i hans selvvalgte forelesning ved sin disputas for sin dr. juris-grad. Problemstillingene var om en person var å anse som bosatt i Norge eller ikke (domicilbegrepet). For to saker som gjaldt samme kvinne, som hadde flyttet fra Norge, fant SARA motstrid. Bing forklarte det med at bosatt-spørsmålet i den ene saken var som del av skattespørsmål, i den andre som del av spørsmål om arv.

Språk for modellering av rettslige normer (SMARN)

Tanker om å bruke SARA for å simulere, evt. eksperimentelt å treffe beslutninger, var utviklet over noe tid[6]. Forslag til hvordan man skulle kunne simulere og automatisere juridiske beslutninger ble utarbeidet. Enkel vilkårsprøving med påføl-

1 *SARA: System for analyse av rettslige avgjørelser*, Mette Borchgrevink og Johs. Hansen, NORIS (33), Skriftserien Jus og EDB 44, Institutt for privatrett, Avd. for EDB-spørsmål, UiO, 1980

2 Verdiene for et moment i en beslutning var +1 for et proargument og -1 for et mot-argument, 0 om momentet ikke var relevant. Vektor-produktet for verdi og vekt kalte vi *teoretisk resultat*. Om teoretisk resultat var det samme som resultatet av beslutningen, sa vi at vektene *forklarte resultatet*.

3 Jf *Notater om deontiske systemer,* Johs. Hansen (red.), CompLex 2/81, Universitetsforlaget, 1981, med innlegg fra Gert Fredrik Malt, Dag Johnsen, Michaael Heathter og Daniel Stripinis.

4 *Et EDB-system for analyse av rettslige avgjørelser*, Hansen, Johs, CompLex 1/81, Universitetsforlaget, 1981

5 *SARA: Brukerveiledning og programdokumentasjon*, Johannes Hansen, NORIS (49), CompLex 7/85, Universitetsforlaget.

6 Jf. søknad om bevilgning til JUS og EDB 1980, forfattet av Jon Bing.

gende beregning av ytelser eller lignende, basert på regler, var 3. generasjons programmeringsspråk godt egnet til. Men det var interesse for imitering av skjønn ved bruk av vekttallsregelen for eksperimentering. F. eks. for å simulere effekter av et regelverk for en gitt populasjon av individer. Støttet av NAVF ble det i 1982 startet et treårsprosjekt for utvikling av et verktøy for *lovmodellering*.

Arbeidet tok utgangspunkt i Jon Bings modell av *juridisk problemløsning*, slik han hadde beskrevet det i artikkelen *Fra problem til resultat*[7]. Dette var en gjengivelse av *juridisk metode*, utarbeidet til bruk i arbeide med tekstsøking. En forankret skisse til *Språk for modellering av rettslige normer* (SMARN) ble publisert[8] og benyttet i arbeide med versjon 1 av SMARN. Programmeringsspråket er i detalj spesifisert i *Simulation and Automation of Legal Decisions*[9], kapitlene 1-3 (dvs. SMARN1). Språket (språkutvidelsen) skulle realiseres ved at en såkalt preprosessor skulle generere programkode for programmeringsspråket SIMULA basert på et program skrevet i SMARN.

I språket ble en størrelse kalt *norm-segment* definert. Det var en sammenstilling av variable for representasjon av opplysninger samt normer for å løse et juridisk problem. Et norm-segment ble implementert i ei *norm-blokk*[10]. Her kunne en deklarere avveiinger, fastregler, diverse typer variable, navngitte betingelser og såkalte normkall. Normkall skulle styre sekvensen for evalueringer i normblokka. Alt dette for å løse et juridisk problem.

Før spesifikasjonen av preprosessoren var fullført, ble det valgt en pilot for implementering - å programmere deler av arveloven – som krevde noen ytterligere egenskaper enn de alt definerte[11]. Dermed måtte språk og spesifikasjoner videreutvikles. Dette er dokumentert i kapitlene 4 og 5. Selv om preprosessoren verken var bygd eller helt ferdig spesifisert, programmerte stud. jur. Espen Ødegaard i samarbeid med meg deler av Arveloven i SMARN.

En notasjon for å uttrykke pliktnormer i

Parallelt med arbeidet med SMARN, arbeidet vi også med å utforme en notasjon for å uttrykke pliktregler i. Nils Kristian Sundbys dr. avhandling *Om Normer* var en helt sentral kilde til kunnskap. Vi så for oss en notasjon til å uttrykke plikter med betoning av størrelser som handlinger, subjekter, objekter og relasjoner, med et mål om å gjøre det lettere å uttrykke plikters meningsinnhold i forbindelse med automatisering eller simulering.

Instituttet hadde fra sin start som Avdeling for EDB-spørsmål en tradisjon for internasjonalt samarbeid. På området ekspertsystemer hadde vi delt erfaringer ved publiseringer, presentasjoner og kollegiale utvekslinger. I et forsøk på å få bedre framdrift i vårt arbeide med deontisk logikk, ble det vinteren og våren 1984 ved IRI arrangert en seminarserie med bidrag fra forskere som Ronald Stamper (LSE), L Thorne McCarty (Rutgers University), Jon Bing, Andrew Jones, rettsfilosofen Gert Fredrik Malt, og fra meg, alle de siste ved UiO. Bidragene fra seminarene er publiserte.[12] Det var etter disse seminarene at studieturene til LSE og Rutgers ble gjennomført.

Det var ulike normlogikker og ulike typer semantikker som det ble nødvendig å sette seg inn i. Alt i alt et ganske stort tilfang av tilnærminger. Bjørn Kirkeruds forelesninger om semantikk for programmeringsspråk på Institutt for informatikk var til stor inspirasjon. I ulike forskningsmiljøer arbeidet man i nokså ulike retninger. I stedet for å legge opp til store og viktige valg her, la vi energi inn i arbeidet med en notasjon for å representere meningsinnhold for pliktnormer i.

Omtale av arbeidet med utarbeidelse av notasjonen for å uttrykke normer i

Jeg vil beskrive visse trekk ved notasjonen, slik at det kan være mulig å få et inntrykk av den. I notasjonen ble en *pliktnorm* karakterisert av tre kjennetegn: En *deontisk modalitet,* m, en handling H og aktører (subjekter) A. Modaliteten forteller om en *type handling,* H, eller dens *unnlatelse,* ¬ H, er påbudt, tillatt eller forbudt for de subjekter som omfattes[13]. Ved å introdusere en *betingelse* for at normen skulle komme til anvendelse, b, så kunne vi uttrykke *betingede pliktnormer.*[14]

Som en felles betegnelse på hva en norm refererer til og regulerer (dens domene) benyttet vi en frase *samling av relaterte fenomener og* benevnte det en *scene*. Sentrale størrelser som scener består av var: *subjekt, objekt, handling* og *relasjon*.

Så definerte vi en *abstrakt pliktoperator* til å være enten *bundet, fri, ikke bundet* eller *ikke fri*[15]. Likeså definerte vi noe vi kalte en *spesifikk pliktoperator*, som en kombinasjon av en slik

7 Jussens Venner 1/75
8 CompLex 2/81, s. 82–107.
9 *Simulation and Automation of Legal Decisions*, Johannes Hansen, NORIS (57), Complex 6/86, Universitetsforlaget, Oslo, 21. august 1986.
10 Blokk-begrepet ble introdusert med programmeringsspråket Algol, og bidro til utviklingen av det vi kaller *strukturert* programmering.
11 Piloten var strengt tatt utenfor valgt anvendelsesområde («scope»).
12 CompLex 8/85 *Modelling Knowledge, Action, Logic and Norms*, Johannes Hansen (ed.), Universitetsforlaget, Oslo, 1985.
13 Dette ble notert (m A H), eksempler: (Påbudt A H), (Forbudt A H),
14 Hvis b så (m A H), f. eks. hvis b så (Tillatt A ¬ H)
15 Vi noterte for abstrakte operatorer M, at de kunne være a) bundet: notert «!», b) fri: «ı», c) ikke bundet: «~!» og d) ikke fri: «~ı».

abstrakt pliktoperator og spesifikke restriksjoner for handlingen (bR), som fulgte av normen[16]. De vanlig brukte *plikt-operatorene* ble så definert ved hjelp av abstrakte operatorer på følgende vis: **påbud** = bundet til å uføre, **forbud** = bundet til å unnlate, **tillatelse** = ikke bundet til å unnlate. Mens **frihet** = verken bundet til å utføre eller til å unnlate.

Mens de fleste forskere som arbeidet med beslektede problemstillinger var opptatt av å diskutere pliktoperatorene **forbud, påbud, tillatelse**, så var det min vurdering da at en *semantikk* innrettet på kontroll med *etterlevelse* (samsvar/compliance) best kunne defineres for spesifikke plikter. Det skulle tilsi at de scener som normer skulle kunne uttrykkes for, som normene selv, med tanke på implementering, ikke kunne være særlig komplekse. En forutsetning for å realisere en formell notasjon ble da at normenes meningsinnhold måtte være nokså enkelt, både for det som angikk selve scena og det som angikk selve plikten.

Utarbeidelsen av en slik notasjon viste seg langt mer omfattende enn antatt. Da min stilling som vit.ass. ved instituttet utløp 31. desember 1984, var SMARN2 definert og preprosesoren nesten ferdig spesifisert. Men arbeidet med dr.scient-avhandlingen var langt fra ferdig. Ikke lenge etter jeg skrev innlegget for Lov og Data, hadde jeg fått tilbud om stilling som spesialrådgiver i Datatilsynet, med ansvar på det tekniske området. Sentrale oppgaver var å stille krav til – som å bedømme - sikkerhet for og kvalitet i personregistre. Etter noe modningstid, takket jeg ja til stilligen.

Selv om jeg hadde halve stillinger ved IRI og DT i en overgangsperiode, gjensto mye arbeid med avhandlingen da jeg sluttet ved IRI.

16 En spesifikk pliktoperator ble notert på formen (M bR), der M var den abstrakte operatoren og bR de spesifikke restriksjoner.

Det var mange nye typer oppgaver for meg å ta fatt på da jeg begynte i Datatilsynet 1. august 1984, f. eks. arbeide med utforming av sikkerhetskrav[17].

Siden jeg hadde en interesse i å søke å klargjøre begrensninger og kompleksitet som forelå mht. å utrykke pliktnormer i en formell notasjon, var jeg ikke inne på tanken om å avgrense arbeidet til visse elementer i pliktutrykkene.

Jeg jobbet på fritiden nokså mye med stoffet fram til ca. 1992. Selv har jeg i ettertid hatt god nytte av notasjonen for pliktnormer, særlig i arbeide med analyse, diskusjon og utforming av informasjons- og IT-sikkerhets-policyer[18].

Til slutt vil jeg nevne at meningen (*semantikken*) til en **påbudsnorm** ble tentativt definert som

a) normens forutsetning om de samlinger av relaterte fenomener som må foreligge (den scene som den normerer). b) normens restriksjoner som den etablerer innen scena: restriksjoner som må være oppfylt i scena, før, mens og etter handlingen utføres,

c) at normen etablerer en binding til å utføre en handling, inkludert det å planlegge (finne og velge) en slik handling.

Meningen til en **forbudsnorm** er noe annerledes: a) man må klargjøre hva man i lys av normen skal unnlate. b) man skal unnlate å gjøre denne/disse handlinger.

Avslutning

Som student, stipendiat og vit.ass. hadde jeg gleden av å være tilknyttet IRI og forløper i ca. 10 år. Vi fikk bidratt til studiet av rettslige avveiinger ved utvikling og bruk av IT-systemet SARA.

Det er en utfordring med skjønn at det ikke kan automatiseres. Man kan imidlertid fastsette en annen mekanisme for å erstatte skjønn. Dette er en politisk/juridisk beslutning som forutsetter tilstrekkelig juridisk kompetanse, dvs. myndighet, og ikke noe den som skal treffe beslutninger etter et fastsatt regelverk kan avgjøre, langt mindre IT-personale.

Man kan forstå avveiinger som en noe underspesifisert måte å løse problemstillinger på, hvor mye overlates til de som skal foreta avveiingene sitt skjønn. Heller enn å granske dette så nært, kan det være at den som har normgivningskompetanse burde spesifisere problemløsningen mer spesifikt enn ved å introdusere en avveiing. Evt. at en bruker avveiinger i en «prøveperiode», for senere å fastsette regler for løsningen av problemstillingene, eventuelt for en delmengde av problemstillingene. En må imidlertid ikke undervurdere det *dynamiske* aspekt som bruk av avveiinger har i rettsordenen. Hvordan utfallet av avveiinger skal bli, kan justeres over tid, ved at nye retningslinjer for avveiingene gis, ved at nye signaler gis av kompetent myndighet, eller at beslutningsfatteren forstår at justeringer bør gjøres.

Innen området lovmodellering definerte vi en utvidelse av programmeringsspråket Simula. Men den preprosessor som skulle oversette fra SMARN til Simula rakk vi ikke å realisere. Dermed fikk vi ikke høstet erfaringer med å imitere skjønnsanvendelser. Kanskje ville de vist at vi skulle begrenset oss til å bruke vekttallsregelen. For det er ikke sikkert at den økte fleksibilitet mht. vekting som SMARN åpnet for ville vist seg nyttig. Selv om det å kunne justere vekter på et moment i en avveiing alt etter hvilke andre momenter som forekom-

17 *SAFE P: Sikring av foretak, EDB-anlegg og personverninteresser etter Personregisterloven,* Johs. Hansen, TERESA (50), Complex 12/88, UiO, 1988

18 *On the Definition and Policies of Confidentiality,* Johs Hansen Hammer (NAV) og Gerardo Schneider (IfI), presentert ved *Third International Symposium on Information Assurance and Security*, Manchester, 28.–30. august 2007

mer i avveiingen, syntes som en ønskelig mulighet å ha.

For å kunne nærme seg et forslag til å erstatte utøvelsen av avveiinger med en modell for å imitere avveiinger, må man forstå avveiingsprosessen godt nok til å kunne treffe godt med modellen. Ellers vil man feile. Her er retningslinjene om hva som er relevante momenter og om vekting, samt empiri om beslutninger, hovedkildene til kunnskap.

Vårt arbeid plasserte vi innen området *ekspertsystemer*, eller *kunnskapsbaserte systemer*. Med litt velvillig bruk av dagens definisjoner kan en nok si at det faller inn under *symbolsk KI*. I dag skjer det store framsteg innen det som kalles *subsymbolsk KI*. Her er sentrale elementer som maskinlæring, nevrale nettverk og språkmodeller i bruk. I det vi fascineres av de nye muligheter, og stiller oss spørsmål om hvordan de best skal tas i bruk, så må vi minne oss om at offentlig og privat forvaltning bruker 3. generasjons programmeringsspråk for å løse store volumer av juridiske problemstillinger. Så er ekspertsystemer i omfattende bruk, som i *regelmotorer*, f. eks. i AltInn og i Elektronisk Mottak i NAV, for å behandle innkommende meldinger.

Det er stor interesse for å kunne automatisere stadig flere prosesssteg, som av ulike grunner, p.t. er manuelle, slik at lengre deler av en prosess-kjede kan være automatisk. Jeg ser ikke for meg at subsymbolsk KI vil få noen rolle å spille her, utover å kunne være støtte i manuelle prosess-steg.

Men så spiller jo subsymbolsk KI allerede en stor rolle i chatboter og i språkmodeller generelt. Henvendelser fra befolkningen tar mye kapasitet fra forvaltning og næringsliv, og brukervennlig effektivisering er viktig. Til en lang rekke ulike typer oppgaver vil f. eks. språkmodeller kunne bidra. Jeg vil tro at med de språkmodeller som er i bruk innen KI allerede, så vil en også kunne vesentlig forbedre effektiviteten i framhentingen av relevante rettskilder ved løsning av juridiske problemstillinger.

Her blir kontrollen med utforming av språkmodeller en utfordring. Den som tilrettelegger en språkmodell for avansert bruk, må kunne avgrense og kontrollere kilder som benyttes og juridiske forhold knyttet til bruk av kildene. Det er jo selvsagt at tilstrekkelige og relevante kilder som trengs for løsningen av en gitt problemstilling må dekkes.

Ideelt bør jo den som gjør seg bruk av en språkmodell kunne ettergå de kilder som ligger til grunn for et svar, deres gyldighet, autentisitet, integritet, notoritet, etc., og også stille vilkår til de kilder som skal kunne brukes i svar. Og ikke minst be om forklaring av hvorfor en bestemt konklusjon er foreslått[19]. Siden tolkning og harmonisering av rettskilder er så sentral del av juridisk metode, er det lett å se for seg sterke begrensninger i anvendelse av selv avanserte språkmodeller på det juridiske området.

Det vi gjorde i SARA er å sammenligne med bruk av maskinlæring med ett-lags nevralt nettverk (lineær modell). Med bruk av maskinlæring og to-lags nevrale nettverk, har en trolig gode muligheter for å få til bedre imitering av utført skjønn. Det skyldes jo delvis at en slik modell er ikke-lineær, og kan justere vekter basert på hvilke kombinasjoner av momenter som forekommer. Men jeg vil tro at man neppe kan vise til så elegante matematiske uttrykk for juridiske størrelser, som det vi etablerte.

Subsymbolsk AI baserer seg ikke på eksplisitt representasjon av semantikk. Det vil derfor være noe «tentativt» over løsning av juridiske problemer vha. slike metoder. Det kan i mange sammenhenger kanskje være godt nok for rådgiving og veiledning, når tilstrekkelig forbehold også presenteres, men ikke for juridiske beslutninger.

Vi fikk også i noen grad bidratt i arbeidet med deontisk logikk ved instituttet. Mitt bidrag ble vel først og fremst å starte opp et slikt arbeid der. Hvorvidt min måte å uttrykke pliktoperatorer på kan bli fruktbar, har jeg her ikke argumentert nærmere for. Har jeg truffet nokså godt i utlegningen av dette, så illustrerer det hvor rikt et meningsinnhold pliktnormer kan romme, også i selve pliktmodalitetene.

For å kunne automatisere juridisk problemløsning, der en ønsker å representere pliktoperatorene, bør derfor trolig disse både ha et nokså enkelt meningsinnhold og et innhold som er fast over tid.

For automatisk løsning av juridiske problemstillinger er det uansett avgjørende å opprettholde høye krav til representasjonen av de normer som skal ligge til grunn for problemløsningen og prosessen som leder fram til denne, som en viktig del av det hele.

Johs Hansen Hammer

Cand.real informatikk UiO (1981). Student og forsker (1978–1984) ved Institutt for rettsinformatikk. Spesialrådgiver i Datatilsynet (1984–1992). IT-sikkerhetsleder i Skatteetaten (1992–2001). Konsulent i PwC og selvstendig (2001–2005). Seniorrådgiver i NAV (2006–2020). Nå pensjonist.

Har fått bidra til utforming, innføring og videreutvikling av informasjons- og IT-sikkerhetsregimer (strategier og policyer). Likeså til innarbeiding av sikkerhet i rutiner og behandlinger, applikasjoner, plattformer og infrastruktur.

19 Her kan man ha forhåpninger til prosjekter som LEXplain («Explainability requirements for AI used in legal decision-making») og deres arbeid med «forklarbar kunstig intelligens» (XAI)

Registrerte personers rettigheter i et 50-årsperspektiv[1*]

Av Dag Wiese Schartum

1. Innledning med problemstilling

I en artikkel i 1969 i tidsskriftet Databehandling, uttrykte Disponent Gunnar Fornehed i Bull/GE sin frustrasjon over sine landsmenn: *«At [den personliga integriteten] skulle befinna sig i farzonen om man bygger upp informationsbankar råder det vid det här laget ingen som helst tvivel om, men märkligt nog tycks 'Svensson' inte ännu inse hur allvarlig situationen blir när han blir post i en databank.»* Han listet deretter opp 3 ½ side fingerte, men realistiske, personopplysninger som allerede var registrert om svenske borgere i forskjellige databanker. Fornehed minnet om at disse lett kunne integreres i én stor databank.[2]

Fornehed og mange andre mente altså det var grunn til bekymring. Men hva slags lovgivning burde man velge for å beskytte befolkningen? Som den første nasjonale loven av sitt slag i verden, var den svenske Datalagen av 1973 på mange måter et lovgivningseksperiment. Usikkerheten var stor om hvordan databanker og ADB-baserte personregistre burde reguleres. Således uttalte lovgiver eksplisitt at Datalagen var et foreløpig tiltak, og at det ikke var usannsynlig at lovgivningen senere ville bli utformet på mer detaljert måte.[3]

Dag Wiese Schartum

Den svenske datalagen skulle forhindre «otillbörligt intrång i registrerads personliga integritet» (7 §) med forholdsvis enkle midler. Hovedgrepet var konsesjonsordning og krav om tillatelse fra Datainspektionen. Dessuten fikk Datainspektionen vid og skjønnsmessig myndighet. Det var i stor grad Datainspektionen som skulle sørge for at folks personlige integritet ble beskyttet. På mange måter hadde Datalagen en «patriarkalsk» tilnærming: Hovedgrepet var at Datainspektionen skulle passe på borgerne ved å vurdere et stort antall konsesjonssøknader.[4] Samtidig ble det gitt enkelte individuelle rettigheter slik at den enkelte kunne ivareta sine egne interesser. Hvor viktige var individuelle rettigheter i Datalagen 1973, og hvordan tenkte man om individuelle rettigheter på den tiden denne loven ble til? I artikkelen gjennomgår jeg også hvordan lovgivningen om individuelle rettigheter har utviklet seg i løpet av de 50 årene som har gått siden Datalagen ble vedtatt.

> Hvor viktige var individuelle rettigheter i Datalagen 1973, og hvordan tenkte man om individuelle rettigheter på den tiden denne loven ble til?

2. Rettighetene i Datalagen 1973

Datalagen inneholdt tre rettighetslignende bestemmelser, se 8–10 §§.[5] Dette gjaldt bestemmelser om uriktige og misvisende personopplysninger, komplettering av ufullstendige opplysninger, og adgangen for enkeltpersoner til å inspisere opplysninger om egen person.

Med referanse til Aurenhammer, fremhever Peter Seipel retten til å inspisere egne personopplysninger som «Magna Carta of the data protection».[6] En slik rett fantes i Datalagen 10 §. Her pålegges den registeransvarlige å underrette om innholdet av personopplysninger som inngår i et register, eventuelt underrette om at slike opplysninger ikke finnes. Plikten ble utløst av en skriftlig og underskrevet begjæring fra vedkom-

1 * En noe annen versjon av denne artikkelen er publisert i M. Brinnen, C. M. Sjöberg, D Törngren, D. Westman, og Sören Öman (red.), «Dataskyddet 50 år – historia, aktuella problem och framtid». Utgiver: eddy.se ab, Stockholm 2024, s. 63–76.

2 Artikkelen er gjengitt i Samuelsen 1972, s. 214–217.

3 Seipel 1974, s 54. Kreditupplysningslag (1973:1173) fra samme år, hadde en mer detaljert utforming, se Hafli 1977, s. 7 og Seipel 1974, s. 54.

4 Slik var det også med lignende lovgivning i andre land på 1970-tallet.

5 I avsnitt 5 diskuterer jeg hva en rettighet kan sies å være.

6 Seipel 1974, s 60.

mende enkeltperson. Hver registeransvarlig hadde kun plikt til å gi en og samme enkeltperson tilgang til opplysningene én gang per år.

Det var ingen mekanisme for å gjøre registrerte personer oppmerksom på at det fantes personregistre med opplysninger om ham eller henne. I mangel av annen kunnskap måtte den som ønsket å inspisere sine opplysninger, derfor først be om innsyn i Datainspektionens fortegnelse over personregistre. Slikt innsyn ble gitt i henhold til offentlighetsprincipen. Datalagen 1973 gav kun rett til å se egne opplysninger, og det var ingen videre rett til å få kunnskap om den faktiske bruken av opplysningene. Hvert register skulle ha et formål (7 § 1 st.) og Datainspektionen skulle ha tilgang til denne informasjonen (17 §). Først flere år senere fikk de registeransvarlige plikt til å føre fortegnelse over personregistre de hadde,[7] men heller ikke da fikk registrerte personer lovfestet rett til å se disse opplysningene. Kunnskapsgrunnlaget for å sende begjæring om å se egne personopplysninger var med andre ord meget begrenset.

Også spørsmål om retting, endring, utelatelse og komplettering av personopplysninger var regulert i Datalagen 1973, se 8 § og 9 §. Bestemmelsen i 8 § gjaldt adgang til å kreve gransking av om opplysninger var uriktige eller misvisende. Enhver begrunnet mistanke om dette utløste plikt for registeransvarlige til å foreta «skälig utredning» av spørsmålet, uavhengig av hvem som reiste spørsmålet. Var det en registrert person som hadde meldt mistanke om at personopplysninger var uriktige eller misvisende, skulle de ha bistand fra en person hos den registeransvarlige. Den registrerte skulle dessuten underrettes av denne personen om hvilke tiltak registeransvarlige ville iverksette for å rette på forholdet.

Bestemmelsen i 9 § regulerte situasjoner der personopplysninger var ufullstendige, og påla en plikt til å komplettere opplysningene. Det var også plikt til å komplettere ved å ta inn *personer* som en ut ifra formålet med registret måtte forvente å finne opplysninger om. Det skulle gjennomføres slik komplettering «som behövs». Det var altså ingen ubetinget plikt til å komplettere, med mindre «ofullständigheten kan antagas medföra otillbörligt intrång i personlig integritet eller fara för rättsförlust». Bestemmelsen gav ikke registrerte personer en direkte rett til å kreve komplettering.[8]

Vernet av den enkelte registrerte person var etter Datalagen 1973 ikke begrenset til de nevnte rettighetene i 8 – 10 §§. I tillegg kunne den enkelte klage til Datainspektionen. Inspektionen skulle påse at automatisk databehandling «icke medför otilbörligt intrång i personlig integritet».[9] Henvendelser fra enkeltpersoner med påstand om «otilbörligt intrång» måtte derfor følges opp. Selv om Datainspektionen tok imot individuelle klager, var det imidlertid ikke i loven formulert en tydelig individuell klagerett.

Ovenfor har jeg betegnet bestemmelsene i 8 § og 10 § *rettigheter*, men fremhevet at bestemmelsen i 9 § ikke gav noen direkte rett for enkeltpersoner. Alle tre bestemmelser er plassert i kapittelet om «Den registeransvarliges skyldighet». Ingen av bestemmelsene bruker ord som «rätt» eller «rättighet». I Datalagen 1973 blir ordet «rätt» knyttet til Datainspektionen, myndigheter og mottakere av personopplysninger. Heller ikke den norske personregisterloven (vedtatt 1978) hadde klart formulerte rettigheter.[10] Slik sett er kontrasten til dagens lovgivning stor.[11]

Det er neppe grunn til å forstå den manglende rettighetsperspektivet i Datalagen 1973 og andre personvernlover på 1970-tallet, som uttrykk for uvilje mot at den enkelte skulle få innflytelse over egen situasjon. Det er derimot viktig å huske at de aller færreste mennesker på 1970-tallet hadde kunnskaper om og erfaringer med databanker, personregistre og «ADB»; dette var lenge før PCens og mobiltelefonens tid. Folks forutsetninger for å kunne ivareta egne interesser ved å utøve individuelle rettigheter, var derfor meget begrenset. Slik sett var det nærliggende at vern om den personlige integriteten primært måtte sikres i relasjonen mellom de registeransvarlige og tilsynsmyndigheten.

3. Rettigheter i tidligere lover og lovforslag på 1960-tallet12

Før vedtakelsen av Datalagen 1973, var det diskusjoner i flere land om behovet for datalover og hva slike lover burde inneholde. Her vil jeg belyse hvordan spørsmålet om den enkeltes rettigheter ble diskutert. Jeg begynner med en artikkel i Scientific American fra september 1966, skrevet av professor John McCarthy. Artikkelen, med tittel «Information», inneholder et samlet forslag til individuelle rettigheter knyttet til

7 Datalagen 7 a §.

8 Dersom en ufullstendighet representerte misvisende opplysning, er det imidlertid mulig bestemmelsen i 8 § kunne komme til anvendelse.

9 Jf. Datalagen 1973, 15 §.

10 I bestemmelsen om retting og komplettering av personopplysninger i § 8 i den norske loven, var den registrerte ikke en gang nevnt. Bare bestemmelsen om innsyn var formulert som rettighet: «Alle har rett til å få opplyst hvilke opplysninger om dem selv som lagres eller bearbeides ved elektroniske hjelpemidler.» (§ 7).

11 Spørsmålet er imidlertid hva det vil si at registrerte personer har en rett, og hvor stor betydning det har at en i lovgivningen bruker klare rettighetsbetegnelser. Dette kommer jeg tilbake til i avsnitt 5.

12 Takk til bibliotekar Tormod Andersen for meget verdifull bistand ved utarbeidelsen av dette avsnittet.

personvern og databanker. Alt tyder på at forslaget er det aller første av sitt slag.[13]

Nedenfor vil jeg også gjennomgå rettigheter i det første *lovforslaget* om personvern og databanker. Forslaget var fremmet i det engelske underhuset, men ble ikke vedtatt.[14] Til slutt skal jeg kort seg på hvordan spørsmålet om rettigheter ble ivaretatt i den første *vedtatte loven* i den Vest-Tyske delstaten Hessen. De nevnte tre kildene er av interesse når en skal danne seg bilde av rettighetstenkningen knyttet til personvern, databehandling og rettigheter i tiden rett før Datalagen 1973 ble til.

Det første brede forslaget til datalovgivning ble fremmet i en fagartikkel av professor John McCarthy ved Standford University. McCarthy var blant annet en av grunnleggerne av kunstig intelligens som fagdisiplin.[15] I en artikkel som primært redegjorde for tekniske aspekter ved prosessering av informasjon ved hjelp av datamaskiner, forslår McCarthy en «Computer Bill of Rights».[16] Forslaget hadde fem hovedelementer: *i)* Rett til å gjøre seg kjent med sine filer med opplysninger; *ii)* rett til å hindre at visse opplysninger blir registrert; *iii)* rett til å kreve at visse tilgangsrestriksjoner ble iverksatt; *iv)* rett til å kreve at tilgang til filer med opplysninger om finansielle forhold må godkjennes av aktuell person; og *v)* plikt til at datasystemer må logge hver gang det blir gitt tilgang til filer med opplysninger om enkeltpersoner. McCarthy understreket dessuten at regler om tilgang til slike filer måtte være klare og tydelige og godt publiserte. Datamaskinprogrammer som iverksetter tilgang til filer måtte, ifølge McCarthy, i tillegg være åpent tilgjengelig for alle, inklusive borgerrettighetsorganisasjoner som f.eks. American Civil Liberties Union.

Et engelsk privat lovforslag om *Data Surveillance Bill* (1969) fikk oppmerksomhet i den internasjonale debatten om datalovgivning og personvern.[17] Dette var trolig det første formelle lovforslaget om personvern og databanker. Forslaget var utarbeidet før delstaten Hessens datalov og ble fremmet i det britiske parlamentet i 1969, men ble forkastet og fikk ikke en «second reading».[18] Lovforslaget hadde vidt virkeområde og omfattet en rekke registre i offentlig og privat sektor.[19] Det ble forslått bestemmelser om aktiv informasjonsplikt for operatører av databanker: Senest to måneder etter at en persons navn først var registrert i en databank,[20] skulle operatøren av databanken sende en utskrift til personen som inneholdt alle opplysninger i databanken som gjaldt vedkommende person.[21] Unntak ble gjort for databanker i politiet, sikkerhetstjenestene og de væpnede styrkene.[22] Den enkelte person kunne deretter når som helst kreve tilsvarende utskrifter fra databanken mot betaling som registermyndigheten fastsatte for hver gang. Utskriftene skulle inneholde informasjon om det *angitte formålet* med bruken av opplysningene, det *faktiske formålet* for bruk siden den siste utskriften, samt navn og adresser på mottakere som hadde mottatt data siden siste utskrift.[23]

Personer som hadde mottatt utskrift av sine data som beskrevet ovenfor, kunne kreve alle eller noen opplysninger om seg endret eller slettet. Begrunnelsen for slike krav kunne være at de registrerte opplysningene var uriktige, urettferdige eller ikke oppdaterte, vurdert ut ifra det angitte formålet med opplysningene. Kravet måtte sendes registeringsmyndigheten som kunne avgjøre saken. I tillegg kunne mottakere av de aktuelle dataene varsles.

Delstaten Hessens datalov fra 1970 var begrenset til databehandling som skjedde i eller på vegne av offentlige myndigheter og virksomheter i delstaten. [24] Loven hadde enkle bestemmelser som gav individuelle rettigheter. Det sentrale var en rett til å kreve uriktige opplysninger rettet.[25] Denne retten hadde enhver «agrieved party»,[26] det vil si rettigheten var ikke begrenset til personer det var registrert opplysninger om. Registrerte personer hadde i tillegg en generell rett til å klage og til å kreve opphør av enhver ulovlig bruk av opplysninger om dem.[27] Kravene til lovlighet gjaldt fasene innsamling, overføring og lagring, og stilte krav til at oppslag i registre, endring, utrekk og destruksjon av opplysninger bare kunne utføres av autoriserte personer. Alle som mente at deres rettigheter hadde blitt krenket, kunne

13 Jeg bygger denne antakelsen på den omfattende litteraturoversikten i «Computers and Privacy: A Survey» i Hoffman 1969 som primært dekker USA, og på oversikten i Niblett 1971 som er skrevet for OECD med hovedfokus på Europa.

14 Se Van Alsenoy 2019, s. 164.

15 *John McCarthy (computer scientist) - Wikipedia* <https://en.wikipedia.org/wiki/John_McCarthy_(computer_scientist)>

16 McCarthy 1966, s 72.

17 Samuelsen 1972, s 180. Forslaget ble fremmet av *MP Kenneth Baker* med flere.

18 Forslaget er trykket i Samulesen 1972, bilag 5 (s. 226–231).Kenneth Baker M.B la forslaget frem for Underhuset, og Lord Windlesham la fram forslag med identisk ordlyd for Overhuset (Niblett 1971, s. 32).

19 Se forslagets paragraf 1(1).

20 Registrering skulle skje hos «Registrar of Restrictive Trading Agreements», jf. paragraf 1(1) i lovforslaget. Dette organet var allerede opprettet i 1956 og skulle bidra til å fremme konkurranse og motvirke handelshindringer. Organiseringen viser trolig at forslaget til Data Surveillance Bill også var konkurransepolitisk motivert.

21 Se forslagets paragraf 4(1).

22 Jf. forslagets paragraf 2(1).

23 Se forslagets paragraf 4(2) bokstavene a–c.

24 Se «Hessen Datenschutzgesetz vom 7. Oktober 1970», Gesetz- und Verordnungsblatt für das Land Hessen (HE GVBI), Section 1.

25 Se section 4(1)og Van Alsenoy 2019, s. 167.

26 Jf. uoffisiell oversettelse i Niblett 1971, s. 48.

27 Se section 4(2). Van Alsenoy 2019, s. 167 omtaler dette som «blocking ».

henvende seg til Personvernkommisjonæren.[28] Kommisjonæren hadde imidlertid ikke myndighet til å gi bindende direktiver, men måtte nøye seg med å varsle ansvarlig myndighet om at bestemmelser i Dataloven var overtrådt.[29]

Gjennomgangen ovenfor viser ganske forskjellige tilnærminger til spørsmålet om individuelle rettigheter. De mest progressive og «moderne» ideene ble formulert av teknologen McCarthy. Når det gjelder rettigheter og beskyttelse av den enkeltes interesser, var det britiske lovforslaget mer konkret enn loven som ble vedtatt i Hessen. Det er overraskende at loven i Hessen ikke hadde egne bestemmelser om innsyn i og inspeksjon av de registrertes egne opplysninger.[30] Det engelske forslaget fra 1969 gikk meget langt i å skape åpenhet. Den aktive plikten for operatørene av databanker til å informere registrerte personer ved å sende dem utskrift av opplysninger om dem, er mer i slekt med GDPR artikkel 13 og 14 om informasjonsplikt, enn GDPR artikkel 15 om rett til innsyn. Inspeksjonsretten i Datalagen 1973, 10 §, gav til sammenligning langt svakere rettigheter for registrerte personer. Selv om det engelske forslaget aldri ble vedtatt, og kanskje ikke var et realistisk utgangspunkt for lovgivning, er det likevel interessant å merke seg det meget store spennet mellom aktiv og omfattende støtte til åpenhetsprinsippet i Data Surveillance Bill 1969, og en mer «passiv» og begrenset inspeksjonsrett i Datalagen 1973.

Vektlegging av datakvalitet og rett til å kreve endring og sletting, synes å være felles for tidlige dataloven. Her er imidlertid Datalagen 1973, 8 §, mye klarere og mer detaljert enn den relativt enkle bestemmelsene i Hessens datalov og Data Surveillance Bill. Særlig er det grunn til å trekke frem det svenske kravet om «skälig utredning», plikten til å underrette den registrerte om iverksatte tiltak, og plikten til å bistå de registrerte. Det finnes ikke bestemmelsen i det engelske lovforslaget og i Hessens lov som tilsvarer Datalagen 1973, 9 §, om komplettering av ufullstendige opplysninger. Samlet sett synes Datalagen å legge spesielt stor vekt på datakvalitet, og loven la til rette for at registrerte personer kan bidra aktivt til dette.

4. Oversikt over den enkelte rettigheter – type og innhold

Registrertes rettigheter har en langt mer fremtredende plass i dagens felle europeiske lovgivning enn i Datalagen 1973. Forskjellene viser seg for det første i lovstrukturen. Datalagens bestemmelser om rettigheter var del av kapittelet om «Den registreransvariges skyldigheter». I OECDs retningslinjer om personvern fra 1980,[31] var registrertes rettigheter formulert som et grunnleggende prinsipp for nasjonal lovgivning på området. Således ble det formulert et «Individual Participation Principle» i Section 13. I EUs Personverndirektiv, 25 år etter Datalagen, inngikk rettigheter i kapittel II om «Alminnelige vilkår for lovlig behandling av personopplysninger». I gjeldende personvernforordning (GDPR) har lovgiver samlet alle rettigheter i kapittel III om «Den registrertes rettigheter».[32] I dagens lovgivning er rettighetene med andre ord gitt en helt sentral plass. I tillegg til bestemmelser som er tydelig formulert som rettigheter, inngår to bestemmelser i kapittel III om den behandlingsansvarliges plikt til å informere de registrerte.[33] Dessu-

	Datalagen 1973	DVD 1995	GDPR 2016
Innsyn/inspeksjon	10 §	Art. 12	Art. 15
Korrigering, komplettering, endring, utelatelse (jf. datakvalitet)	8 § og 9 §	Art. 12(b)	Art. 16
Sletting	(12 §)	Art. 12(b)	Art. 17
Samtykke		Art. 7(a), 8(2)(a), jf. 2(h)	Art. 6(1)(a), 9(2)(a), jf. 4(11)
Protestere		Art. 14	Art. 21
Helt automatisk/manuell		Art. 15	Art. 22
Begrenset behandling			Art. 18
Dataportabilitet			Art. 20
Språk			Art. 12(1)
Fremgangsmåter		Art. 12(a)	Art. 12 (3) og (4)

Tabell 1: Utvikling av typer rettigheter for registrerte personer.

28 Se section 11.
29 Hafli 1977, s. 21.
30 En del av forklaringen kan være at loven kun gjaldt «records and data within the purview of the Land authorities and the public corporations, institutions and establishments under the jurisdiction of the Land.» (Nibletts oversettelse, referert i Samuelsen 1972, s. 220) En mulighet er at registrerte kunne ha innsynsrettigheter vedrørende sine personopplysninger i samsvar med delstatens offentlighets- og forvaltningslovgivning, men dette har jeg ikke undersøkt.
31 Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal data, adopted 23/09/1980.
32 Bortsett fra retten til å gi og trekke tilbake samtykke, jf. artikkel 4(11).
33 Se artikkel 13 og 14.

ten er det tatt inn en bestemmelse om gjennomføring av rettigheter.[34]

Også når det gjelder *typer* rettigheter[35] har det vært en klar utvikling. Nedenfor har jeg satt opp en tabell som stikkordsmessig angir de ulike rettighetene i Datalagen 1973, Personverndirektivet (DPD) og Personvernforordningen (GDPR), og den eller de bestemmelsene som primært omhandler hvert rettighetsspørsmål, se Tabell 1.

I tillegg til slike bestemmelser som Datalagen 1973 tydelig angav som rettighet vedrørende inspeksjon av egne personopplysninger samt datakvalitet, er spørsmålet om sletting i dag tydelig regulert som en individuell rettighet.[36] Dessuten har det kommet til flere nye typer rettigheter.

Personverndirektivet innførte *samtykke* som rettslig grunnlag, dvs. som en rett for registrerte personer til i visse tilfeller å kunne bestemme om behandling av opplysninger om dem skulle være lovlig eller ikke. Personvernforordningen videreførte retten til å samtykke. Samtykke var verken del av Datalagen 1973, OECDs retningslinjer om personvern (1980) eller Europarådskonvensjonen om personvern (1981). Seipel 2001 (s. 139) hevder at informert samtykke var viktig også i Datalagen 1973. For å kunne mene dette tøyer han imidlertid samtykkebegrepet svært langt. Seipels poeng var at Datalagen 3 § 2. st. påla Datainspektionen å legge vekt på registrerte personers virkelige eller antatte holdninger, når inspektionen skulle ta stilling til hva som skulle regnes som «otillbörligt intrång». Dette er imidlertid veldig forskjellig fra samtykke som individuell rettighet slik det ble introdusert i Personverndirektivet.

Personverndirektivet innførte også en rett for den registrerte til i visse tilfeller å *protestere* mot at personopplysninger om ham eller henne blir behandlet. Protestretten i Direktivet hadde bakgrunn i den franske personvernloven av 1978.[37] Retten ble videreført i personvernforordningen. Personverndirektivet innførte dessuten en bestemmelse om rett til i visse tilfeller motsette seg å bli undergitt helt automatiske beslutninger. En lignende bestemmelse er tatt inn i Personvernforordningen, og denne bestemmelsen omfatter også profilering.[38]

Vedtakelsen av Personvernforordningen innebar også to nye rettigheter for registrerte personer som ikke fantes i Personverndirektivet. For det første ble det vedtatt en rett til å kreve *begrenset behandling* av egne personopplysninger i tilfeller der den registrerte mener opplysningene er uriktige eller at behandlingen er ulovlig. Krav om begrenset behandling er også aktuelt når opplysningene ellers skulle vært slettet fordi behandlingsformålet ikke lenger begrunner lagring, men den registrerte trenger opplysningene for å fastsette, gjøre gjeldende eller forsvare et rettskrav. Dessuten er begrenset behandling aktuelt når den registrerte har protestert mot en behandling.

Retten til *dataportabilitet* var den andre nye rettigheten som Personvernforordningen introduserte. Registrerte personer har rett til å motta egne personopplysninger i maskinlesbart format fra den behandlingsansvarlige. Retten gjelder kun opplysninger som den registrerte selv har gitt til. Retten til dataportabilitet gjelder også overføring av nevnte maskinlesbare opplysninger til en annen behandlingsansvarlig. Dataportabilitetsretten er imidlertid begrenset til tilfeller der behandlingsgrunnlaget er samtykke eller avtale med den behandlingsansvarlige, og forutsetter dessuten at behandlingen utføres automatisk. Retten til dataportabilitet har vært sett på som utvidelse av retten til innsyn, men kan sies å være en mer radikal rettighet,[39] bl.a. fordi den innebærer plikt for behandlingsansvarlige til å utføre praktiske handlinger (overføring) når registrere personer ber om det.

I tillegg til nye rettigheter for registrerte personer introduserte Personvernforordningen krav til det språket og den kommunikasjonsmåten behandlingsansvarlige skal benytte ovenfor registrerte og andre. Erkjennelsen om at det ofte kan være vanskelig å forstå innhold av kommunikasjon som gjelder digital databehandling, er gammel. I John McCarthy forslag til Computer Bill of Rights, inngikk det f.eks. et krav om at alle regler om tilgang til datalagre skulle være klare, bestemte og godt kunngjort.[40]

I henhold til personvernforordningen skal informasjon fra behandlingsansvarlige om rettigheter fremlegges på «kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk».[41] Personvernforordningen stiller altså krav til behandlingsansvarliges språk. Kravet om klarhet og kunngjøring mv i forslaget fra McCarthy gjaldt imidlertid *loven selv*.

Personvernforordningen representerer en relativt systematisk tilnærming til spørsmålet om hvordan henvendelser fra registrerte personer skal bli behandlet. Særlig vil jeg trekke frem klare fristbestemmelser, regler om kostnader og adgangen til å kreve sikker identifikasjon.[42] Av størst betydning for registrerte personer som ikke blir hørt når de fremsetter krav om å bruke en rettighet, er imidlertid en «begrunnelsesplikt» for den behandlingsansvarlige som helt eller delvis motsetter

34 Se artikkel 12.
35 Her har jeg ikke anledning til å gå nærmere inn på innholdet av hver rettighet.
36 Paragraf 12 i Datalagen 1973 er satt i parentes fordi den ikke var formulert som rettighet.
37 Zanfir-Fortuna 2020, s. 510.
38 Jf. GDPR Artikkel 4(4).
39 Jf. Lynskey 2020, s. 500.
40 Se McCarthy 1966, s. 72.
41 Se artikkel 12(1).
42 Se artikkel 12(3) - (6).

seg å innvilge rettigheten. Således heter det i artikkel 12(4) at den behandlingsansvarlige må angi årsaken til at behandlingsansvarlige ikke vil treffe tiltak slik den registrerte krever. «Tiltak» referer til slike handlinger som innvilgelse av rettigheter innebærer, det vil for eksempel si det å gi innsyn, slette personopplysninger, begrense behandlingen av opplysninger mv. Forordningen stiller ingen direkte krav til den saksbehandling behandlingsansvarlige må utføre før de treffer sin avgjørelse, jf. kravet til «skälig utredning» i Datalagen 1973, 8 §. Trolig vil anvendelsen av prinsippet om lovlighet, rettferdighet og åpenhet (artikkel 5(1)(a)) begrunne et tilsvarende krav til forsvarlig og balansert saksutredning, men dette fremgår ikke direkte og er usikkert.

I denne gjennomgangen har jeg ikke hatt anledning til å gå nærmere inn på det detaljerte innholdet av de ulike rettighetene, men har i stedet forholdt meg til *typer* rettigheter. Dette gir selvsagt et noe forenklet bilde av hvordan registrertes rettigheter kan sies å ha utviklet seg de siste 50 årene. Hovedbildet er imidlertid klart: Fra å være spredte bestemmelser i tidlig lovgivning, er spørsmålet om rettigheter nå tydelig løftet frem og utgjør et eget, sentralt kapittel i Personvernforordningen. Antallet rettigheter har økt gradvis. Slik jeg har klassifisert aktuelle bestemmelser, er det for hver vesentlige reform av personvernregelverket i EU, lagt til nye rettigheter. Rekkefølge mellom de aktuelle bestemmelsene i rettighetskapittelet (kap. III), angir en forsiktig systematikk. For eksempel er alle bestemmelser som bidrar til åpenhet (artikkel 13–15) satt etter hverandre, først i kapittelet. De markerer dermed en åpenhet som er grunnleggende for de øvrige rettighetene. Det er også henvisningsstrukturer som angir viktige samspill mellom bestemmelsene om protest, begrenset behandling og sletting av personopplysninger. Ut over dette

	Rett	Rett/Plikt	Plikt
Samtykke	X		
Innsyn	X		
Begrenset behandling	X		
Protest	X		
Dataportabilitet	X		
Korrigering, komplettering, endring		X	
Sletting		X	
Informasjon			X

Tabell 2: Klassifisering av typer rettigheter for registrerte personer.

fremstår rettighetene likevel som en «liste» mer enn et systematisk sammenhengende hele av bestemmelser som registrerte personer kan benytte seg av. Bestemmelsene kan gi gode muligheter for enkeltpersoner som evner å forstå og håndtere den juridiske kompleksiteten. For andre kan den lett skape stor usikkerhet om hva en egentlig har rett til, jf. neste og siste avsnitt.

5. Hva er egentlig en rettighet?

Når jeg her stiller spørsmålet om hva en rettighet i personvernlovgivningen egentlig er, er det ikke for å gjøre filosofiske eller rettsteoretiske analyser. Perspektivet mitt er snarere praktisk-juridisk, og gjelder både hvordan rettighetsbestemmelser har vært formulert, og hvordan spørsmål om konkret anvendelse av rettigheter skal avgjøres.

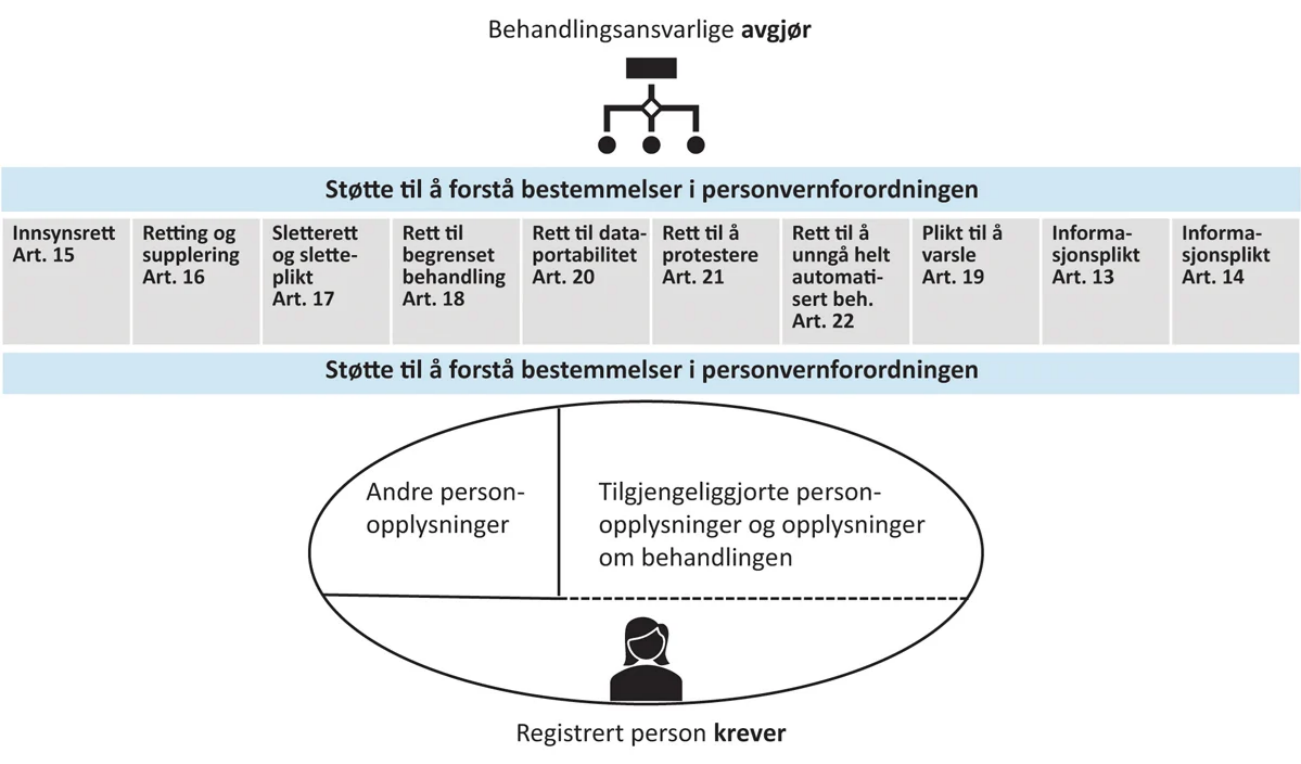
En kan for det første tenke seg at registrerte kunne ha rett til å *bestemme selv*, dvs. treffe valg på egenhånd på måter som får bestemmende betydning for hvordan opplysningene om dem blir behandlet. Registrertes samtykke er en slik rett. For det andre kan rettigheter handle om rett til å *kreve* at noe skal skje, f.eks. at den behandlingsansvarlige skal gi innsyn, slette opplysninger osv. Slike rettigheter som har vært del av personvernlovgivningen siden Datalagen 1973.

Når standardformuleringen i Personverndirektivet er «Den registrerte skal ha rett til [et tiltak eller handling fra den behandlingsansvarlige]», må det ses som en slags informasjon til registrerte personer om at de kan bruke sin ytringsfrihet til å fremsette krav overfor de som behandler personopplysninger om dem. Slike bestemmelser skaper også plikt for de behandlingsansvarlige til å vurdere slike krav. Det er likevel grunnleggende opp til den behandlingsansvarlige å vurdere hensyn og argumenter som kan tale for eller mot at kravet skal etterkommes. Samtidig må de imidlertid forholde seg til den rettslige rammen som Personvernforordningen utgjør, ikke minst formålsbestemmelsen (artikkel 1) og personvernprinsippene (artikkel 5).

Det er ikke alltid stor forskjell på om vi forstår «rettighetsbestemmelser» som rettigheter for registrerte, eller om vi også ser visse plikter som behandlingsansvarlige har overfor registrerte som en slags rettighet. Ofte gjelder både rett og plikt samtidig. I andre tilfeller er *kun* plikt eller rett det riktig perspektiv. Jeg har illustrert dette skillet i Tabell 2 ovenfor.[43]

I tabellen deler jeg bestemmelser som vanligvis betegnes rettigheter i to grupper; de der bare den regis-

43 Jeg har ikke tatt med bestemmelsen i artikkel 22 om retten til ikke være gjenstand for helt automatiserte avgjørelser, herunder profilering. Årsaken er at denne er blitt fortolket av som noe annet enn en rettighet.



trerte kan fremsette krav («Rett»), og de der registrerte kan fremsette krav *samtidig* som behandlingsansvarlige har en selvstendig plikt, *uavhengig av om krav er fastsatt* («Rett/Plikt»). Til høyre har jeg tatt med rene plikter til å gi informasjon (jf. artikkel 13 og 14 GDPR). Når slike plikter er formulert for å stille den registrerte i en bedre situasjon enn uten plikten, kan pliktene sies å være beslektet med rettigheter fordi de støtter opp om samme formål som rettighetsbestemmelser. Slik fremmer informasjonsplikter for behandlingsansvarlige og innsynsretten for registrerte samme formål om å skape åpenhet om behandlingen.

Hvis vi betrakter de tidlige rettighetsbestemmelsene i lys av denne klassifiseringen, blir det tydelig hvorfor bestemmelser som i 1973 ikke eksplisitt var formulert som rettighetsbestemmelser likevel ble oppfattet å være rettigheter. Samtidig blir det mer synlig hvordan det i nyere lovgivning har vært lagt større vekt på å eksponere rettighetsperspektivet; både ved å betegne noe som rett, og ved å plassere bestemmelser som kan sies å være beslektet med rettigheter, i samme kapittel.

6. Avslutning

I sin artikkel fra 1966 fremhever McCarthy at «The right to keep people from keeping files on us must […] be invented, then legislated and actively be enforced.»[44] Han peker på behovet for stadig å tenke nytt om rettigheter fordi den teknologiske utviklingen går så raskt at grunnleggende rettigheter vi «alltid» har hatt ikke er tilstrekkelige. I artikkelen har jeg blant annet vist hvordan vi i mer enn 50 år gradvis har «funnet opp»[45] nye rettigheter, og hvordan slike rettigheter gradvis har blitt en stadig viktigere del av personvernlovgivningen. Fra den spede begynnelsen har vi i dag en rekke enkeltstående rettigheter. Spørsmålet kan reises om den samlede effekten kan bli bedre?

Den norske Personvernkommisjonen pekte i 2022 på behovet for en digital *rettighetsplattform*, se figuren nedenfor.[46] Kommisjonen mente at en slik plattform kan gi teknologisk støtte for registrerte personer til å se rettigheter i sammenheng, og til å hjelpe den enkelte til å gjøre aktivt bruk av sine rettigheter.

> I artikkelen har jeg blant annet vist hvordan vi i mer enn 50 år gradvis har «funnet opp» nye rettigheter, og hvordan slike rettigheter gradvis har blitt en stadig viktigere del av personvernlovgivningen.

Tanken om en rettighetsplattform bygger på en forutsetning om at den enkelte har rett til direkte til-

44 McCarthy 1966, side 72.

45 Jf. McCarthys formulering i sitatet ovenfor.

46 Se NOU 2022: 11 Ditt personvern – vårt felles ansvar – Tid for en personvernpolitikk, avsnitt 11.4.3. Schartum var medlem av Kommisjonen.

gang til de fleste opplysninger om dem, dvs. tilgang uten å måtte spørre den behandlingsansvarlige eller andre. Slik kan krav om digitalt *tilgjengeliggjorte* personopplysninger ses på som den nye «Magna Carta of the data protection».[47] Kombinert med teknologiske verktøy med praktiske funksjoner for å kreve og avgjøre spørsmål om rettigheter, kan rettighetene med andre ord få langt større effekt enn når de kun fremkommer som lovtekst.

Dag Wiese Schartum er professor ved Senter for rettsinformatikk, Det juridiske fakultetet. Schartum arbeider primært med spørsmål om automatiseringsvennlig lovgivning, automatisering av rettslige avgjørelser, og personvern - særlig i samband med nevnte automatisering. I 1994 etablerte han masterstudiet i Forvaltningsinformatikk som han fremdeles har ansvaret for. Han har skrevet en rekke bøker og artikler.

47 Jf. referansen i Seipel 1974, s 60, nevnt i avsnitt 2.

Litteratur

Bygrave 2020: Lee A. Bygrave, «Article 22 Automated individual decision-making, including profiling», i C. Kuner, L.A.Bygrave og Christopher Docksey, *The EU General Data Protection Regulation (GDPR) A Commentary*, Oxford University Press 2020, s. 401–412.

Hafli 1977: Tor Hafli, *En komparativ studie av datalover*, Institutt for Privatrett, Avdeling for edb-spørsmål, Universitetet i Oslo, Skriftserien for jus og edb, Oslo 1977

Lynskey 2020: Orla Lynskey, «Article 20 Right to data portability», i C. Kuner, L.A.Bygrave og C. Docksey, *The EU General Data Protection Regulation (GDPR) A Commentary*, Oxford University Press 2020, s. 497–507.

McCarthy 1966: John McCarthy: Information, *Scientific American,* Volume 215, n. 3, s. 64–73.

Niblett 1971: G.B.F. Niblett, *Digital Information and the Privacy Problem*, OECD Informatics Studies 2, Paris 1971.

Polcák 2020: Radim Polcák, «Article 12 Transparent information, communication and modalities for the excercise of the rights of the data subject», i C. Kuner, L.A.Bygrave og C. Docksey, *The EU General Data Protection Regulation (GDPR) A Commentary*, Oxford University Press 2020, s. 398–412.

Samuelsen 1972: Erik Samuelsen, *Statlige databanker og* personlighetsvern: rapport fra et forskningsprosjekt, Universitetsforlaget, Oslo 1972.

Seipel 1974: Peter Seipel: «Legal Controls of the Storage and Use of Personal Daata. An Appraisal of the Swedish Approach», i Hafli 1977, *En komparativ studie av datalover*, Institutt for Privatrett, Avdeling for edb-spørsmål, Universitetet i Oslo, Skriftserien for jus og edb, Oslo 1977, s. 53–65.

Seipel 2001: Peter Seipel: «Sweden», i Peter Blume (ed.) *Nordic Data Protection*, DJØF Publishing, Cobenhagen 2001, s. 115–151.

Zanfir-Fortuna 2020, Gabriela Zanfir-Fortuna, «Article 21 Right to object», i C. Kuner, L.A.Bygrave og C. Docksey, *The EU General Data Protection Regulation (GDPR) A Commentary*, Oxford University Press 2020, s. 508–521.

Van Alsenoy 2019: Brendan Van Alsenoy, «The Emergence of Data Protection Law», i *Data Protection Law in the EU: Roles, Responsibilities and Liability*, (KU Leuven Centre for IT & IP Law Series) Intersentia 2019.

Artificial Intelligence (AI) and Law

Av Stein Schjølberg, pensjonert sorenskriver.[1]

1. The History

Artificial Intelligence (AI) is a description first used at a conference in the United States in the 1950-ties on the intelligent reasoning by using computers. It was a conference for researchers, and discussions on the possibilities for developing computer programs that would include the special signs and symbols for intelligence. This research continued in the 1960ties and 1970ties, but it was more structured in the mid 1980ties:

Artificial Intelligence as applied in the legal field can be subdivided into two categories: expert systems and knowledge-based systems; and enhancements to legal information retrieval systems. Expert and knowledge-based systems are therefore computer applications that contain knowledge and expertise which they can apply in solving problems.

Artificial Intelligence and Law (AI) was an object of research in the 1990ties. Professor Jon Bing at the University of Oslo, Norway, established research with other universities. It was especially a cooperation with the Law School, University of Strathclyde, Glasgow, Scotland.

I participated in this research and cooperation, together with Professor Jon Bing.

International Conference on Artificial Intelligence and Law (ICAIL) has been held every second year since the first conference in 1987 at the Northeastern University in Boston, USA.

Stein Schjølberg

The Third International Conference on Artificial Intelligence & Law was held at the St. Catherine´s College, Oxford University, on June 25-28. 1991. One of the speakers was Professor Jon Bing. The conference introduced *Case-Based Reasoning* as follows:

The field of Artificial Intelligence (AI) and Law seeks both to develop useful applications of computers to law and to investigate fundamental mechanisms of legal reasoning.

An International Conference on Computers and Law was held in Montreal, Canada, September 30 - October 3, 1992. Professor Jon Bing was one of the speakers and gave a presentation on: *Perspectives for the Development of Computers and Law and Computer Law: The Next 10 years.*

The Fifth International Conference on Artificial Intelligence and Law was held at the University of Maryland in USA on May 21-24. 1995. I was a delegate at this conference. The purpose of the conference was described as follows:

The field of AI and Law employs Artificial Intelligence techniques to study fundamental mechanisms of legal reasoning and to develop practical computer applications for the legal profession.

At the National Conference for Judges in Lillehammer, Norway on June 22-25, 1995. I gave a presentation on *Artificial Intelligence and Law – Expert systems for Judges.*

The Technology Renaissance Courts Conference was held in Singapore in September 1996. Richard Magnus, the leader of Singapore Subordinate Courts gave a presentation of *The Impact of Global Court Technology – Hyperlinking Global Judicial and Legal Systems.* I was also a delegate at the Conference.

> The field of Artificial Intelligence (AI) and Law seeks both to develop useful applications of computers to law and to investigate fundamental mechanisms of legal reasoning.

The Chief Justice Carsten Smith, Supreme Court of Norway, was not able to participate and sent his visual message to the Conference, including as follows:[2]

We must never forget that the main element in the judicial process is the human element – combined with the touch of the heart – to balance conflicting interests.

1 Based on *A presentation at The International Conference on Cyberlaw, Cybercrime & Cybersecurity 2024*, November 13-15, 2024, New Dehli, India.

2 See Stein Schjolberg: Judicial Decision Support Systems from a Judge´s Perspective, International Journal of Law and Information Technology, Volume 6 Number 2 Summer 1998, Oxford University Press, England. (1998).

The Sixth International Conference on Artificial Intelligence and Law (ICAIL-97) was held at the University of Melbourne, Australia, on June 30-July 3, 1997. Professor Jon Bing and I participated at the conference, both as speakers.

The First International Workshop on Judicial Decision Support Systems (JDSS) was also held at the Conference. My presentation at the Workshop was on *Judicial Decision Support Systems from a Judge´s Perspective,* and included:

In this technological environment, Judicial Decision Support Systems have been developed to assist the judge in his decision making. Such systems must not make the decisions, but only be used as a new remedy in the decision process. The judge must always be able to choose the proposed solution or reject it independently.

The National Center for State Courts in the United States organized the Fifth National Court Technology Conference in Williamsburg, September 1997. I made a presentation in the Session No. 1003 on: *Artificial Intelligence/Expert Systems – Decision Support Systems for Judges on Internet.*

The Seventh International Conference on Artificial Intelligence and Law (ICAIL-99) was held at the University of Oslo, on June 14-18. 1999. The conference included The Second International Workshop on Judicial Decision Support Systems (JDSS).

My presentation on *Judicial Decision Support Systems from a Judge´s Perspective,* included as follows:

It provides the opportunity for Supreme Courts around the world to serve the global communities as a global database, and the integration of Judicial Decision Support Systems on the Internet is an important challenge. All the Supreme Court decisions around the world should have a short case summary, with the possibilities of a retrieval system based on structured classifications or keywords.

The publication, *International Review of Law Computers & Technology,*[3] included a foreword from me, as follows:

From a judge´s perspective, we are used to problem solving in our discretionary judgements. We do not need support systems making the final decision, but systems with updated and comprehensive information on previous similar court decisions applied on the facts in the individual case brought before us. The judge should only be assisted in the decision making, leaving the judge to choose the proposed solution or reject it. Decision support systems should only be used as a remedy in the decision process, without affecting judicial independence.

The Third International Symposium on Judicial Decision Support Systems (JDSS) was held on Chicago-Kent College of Law, Chicago, May 25-26. 2001. The invitation to the Symposium included as follows:

As we begin a new century, electronic systems to support decision-making are increasingly envisaged by officials, scholars, lawyers and judges themselves as integral to the armory of the modern judge. Yet, how such judicial systems are designed, implemented and used remains relatively unexplored. Indeed, how do these questions connect with visions of justice?

The Symposium had almost 100 delegates, and included seven Sessions:

- What can JDSS do to Improve Access to Justice.
- Assistance in Argumentation and Document Drafting.
- Knowledge, Science and the Construction of "Intelligence".
- Authority of JDDS: how do and ought judges to use "support?"
- Democracy, Ownership and Public Participation.
- Perspectives on Judicial Discretion & Evaluation of JDSS.
- The Future of the Study of JDSS & Close.

I was in charge of the discussions in the concluding Session, *The Future of the Study of Judicial Decision Support Systems.* In my presentation I concluded as follows:

On behalf of the Program Committee, I will thank you very much for all the interesting papers and discussions. You have brought our conference further from the Melbourne and Oslo conferences. We would like to continuously develop Judicial Decision Support Systems and would appreciate your comments very much. As a judge I have an open mind to what systems that will be recognized as JDSS. Have a safe trip home.

2. Global organizations on Artificial Intelligence (AI)

2.1. A United Nations Resolution on Artificial Intelligence (AI)

United Nations General Assembly adopted on 11. March 2024 a landmark Resolution on Artificial Intelligence (AI). The Resolution was called *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development.*[4]

The General Assembly emphasized:[5]

Same rights, online and offline

The Assembly called on all Member States and stakeholders "to refrain from or cease the use of artificial intelligence systems that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights."

"The same rights that people have offline must also be protected online, including throughout the life cycle of artificial intelligence systems," it affirmed.

The Assembly also urged all States, the private sector, civil society, research organizations and the media, to develop and support regulatory and governance approaches and frameworks related to safe, secure and trustworthy use of AI.

3 See *https://www.ingentaconnect.com/content/routledg/cirl/2000/00000014/00000003;jsessionid=24fcfmut1muq0.x-ic-live-01*

4 See *https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf*

5 See *https://news.un.org/en/story/2024/03/1147831*

Closing the digital divide

The Assembly further recognized the "varying levels" of technological development between and within countries, and that developing nations face unique challenges in keeping up with the rapid pace of innovation.

It urged Member States and stakeholders to cooperate with and support developing countries so they can benefit from inclusive and equitable access, close the digital divide, and increase digital literacy.

2.2. A Convention on Artificial Intelligence (AI)

The Council of Europe *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* was adopted on May 17. 2024.

The Framework Convention is presented by the Council of Europe as follows:[6]

The Convention is the first-ever international legally binding treaty in this field. It aims to ensure that activities within the lifecycle of artificial intelligence systems are fully consistent with human rights, democracy and the rule of law, while being conducive to technological progress and innovation. The Convention aims to fill any legal gaps that may result from rapid technological advances. In order to stand the test of time, the Framework Convention does not regulate technology and is essentially technology neutral.

The Framework Convention was drafted by the 46 member states of the Council of Europe, with the participation of all observer states: Canada, Japan, Mexico, the Holy See and the United States of America, as well as the European Union, and a significant number of non-member states: Australia, Argentina, Costa Rica, Israel, Peru and Uruguay.

In line with the Council of Europe's practice of multi-stakeholder engagement, 68 international representatives from civil society, academia and industry, as well as several other international organisations were also actively involved in the development of the Framework Convention.

The Framework Convention covers the use of AI systems by public authorities – including private actors acting on their behalf – and private actors.

The Convention offers Parties two modalities to comply with its principles and obligations when regulating the private sector: Parties may opt to be directly obliged by the relevant Convention provisions or, as an alternative, take other measures to comply with the treaty's provisions while fully respecting their international obligations regarding human rights, democracy and the rule of law.

Parties to the Framework Convention are not required to apply the provisions of the treaty to activities related to the protection of their national security interests but must ensure that such activities respect international law and democratic institutions and processes. The Framework Convention does not apply to national defense matters nor to research and development activities, except when the testing of AI systems may have the potential to interfere with human rights, democracy, or the rule of law.

The Framework Convention was open for signatures in Vilnius on September 5. 2024, including:

Preamble:

The member States of the Council of Europe and the other signatories hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on the respect for human rights, democracy and the rule of law;

Concerned that certain activities within the lifecycle of artificial intelligence systems may undermine human dignity and individual autonomy, human rights, democracy and the rule of law:

Chapter I - General provisions and Chapter II - General obligations includes:

Article 1 – Object and purpose

1. *The provisions of this Convention aim to ensure that activities within the lifecycle of artificial intelligence systems are fully consistent with human rights, democracy and the rule of law.*
2. *Each Party shall adopt or maintain appropriate legislative, administrative or other measures to give effect to the provisions set out in this Convention. These measures shall be graduated and differentiated as may be necessary in view of the severity and probability of the occurrence of adverse impacts on human rights, democracy and the rule of law throughout the lifecycle of artificial intelligence systems. This may include specific or horizontal measures that apply irrespective of the type of technology used.*

Article 2 – Definition of artificial intelligence systems

For the purposes of this Convention, "artificial intelligence system" means a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment.

Article 4 – Protection of human rights

Each Party shall adopt or maintain measures to ensure that the activities within the lifecycle of artificial intelligence systems are consistent with obligations to protect human rights, as enshrined in applicable international law and in its domestic law.

Article 5 – Integrity of democratic processes and respect for the rule of law

1. *Each Party shall adopt or maintain measures that seek to ensure that artificial intelligence systems are not used to undermine the integrity, independence and effectiveness of democratic institutions and processes, including the principle of the separation of powers, respect for judicial independence and access to justice.*
2. *Each Party shall adopt or maintain measures that seek to protect its democratic processes in the context of activities within the lifecycle of artificial intelligence systems, including individuals'*

6 See *https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence*

fair access to and participation in public debate, as well as their ability to freely form opinions.

The scope of the Convention is described in Article 3, and covers the activities within the lifecycle of artificial intelligence systems that have the potential to interfere with human rights, democracy and the rule of law

Chapter III includes the principles related to activities within the lifecycle of artificial intelligence systems. Chapter IV includes the remedies and Procedural safeguards. Chapter V describes the assessment and mitigation of risks and adverse impacts. Chapter VI includes the

implementation of the Convention, and Chapter VII describes the Follow-up mechanism and co-operation. At the end of the Convention, Chapter VIII includes the Final clauses, such as

Reservations in Article 34 and Denunciation in Article 35.

The Convention is signed by 10 States, including European Union (EU), (October 2024).[7] Norway is one of the States that has signed.

3. Other International initiatives

3.1. European Union

European Union has on June 13. 2024 adopted:

REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (Artificial Intelligence Act)

The Artificial Intelligence Act has 113 Articles.[8] The AI Act ensures that Europeans can trust what AI has to offer. While most AI systems pose limited to no risk and can contribute to solving many societal challenges, certain AI systems create risks that we must address to avoid undesirable outcomes:[9]

Although existing legislation provides some protection, it is insufficient to address the specific challenges AI systems may bring.

The new rules:

- *address risks specifically created by AI applications*
- *prohibit AI practices that pose unacceptable risks*
- *determine a list of high-risk applications*
- *set clear requirements for AI systems for high-risk applications*
- *define specific obligations deployers and providers of high-risk AI applications*
- *require a conformity assessment before a given AI system is put into service or placed on the market*
- *put enforcement in place after a given AI system is placed into the market*
- *establish a governance structure at European and national level*

3.2. The AI Bletchley Summit 2023

The Bletchley Declaration

The Bletchley Declaration was adopted by countries attending the AI Safety Summit at Bletchley Park on 1-2 November 2023[10]. The discussions that took place at the AI Safety Summit brought together stakeholders from European Union, 27 governments, leading AI companies, civil society and academia.

The UK is publishing the Declaration not as a UK government policy document:[11]

Artificial Intelligence (AI) presents enormous global opportunities: it has the potential to transform and enhance human wellbeing, peace and prosperity. To realize this, we affirm that, for the good of all, AI should be designed, developed, deployed, and used, in a manner that is safe, in such a way as to be human-centric, trustworthy and responsible. We welcome the international community's efforts so far to cooperate on AI to promote inclusive economic growth, sustainable development and innovation, to protect human rights and fundamental freedoms, and to foster public trust and confidence in AI systems to fully realize their potential.

3.3. The AI Seoul Summit 2024

On May 21–22, 2024, the Republic of Korea and the United Kingdom cohosted *the second AI summit following the United Kingdom's* launch of the series in 2023:[12]

The "AI Seoul Summit," as it was billed, gathered leaders from government, industry, and civil society to discuss global collaboration on AI safety, innovation, and inclusivity. This "minisummit" took place both virtually and in Seoul for two days of back-to-back events. Overall, the event succeeded in its goal to continue momentum after the landmark 2023 UK AI Safety Summit. Technically there were two conferences, the AI Seoul Summit and AI Global Forum, but the events were held concurrently, in the same location, and with mostly the same participants.

Seoul Declaration

The Seoul Declaration[13] aims to enhance international cooperation on AI governance by engaging with various global initiatives:

1. *We, world leaders representing Australia, Canada, the European Union, France, Germany, Italy, Japan, the Republic of Korea, the Republic of Singapore, the United Kingdom, and the United States of America, gathered at the AI Seoul Summit on 21st May 2024, affirm our common dedication to fostering international cooperation and dialogue on artificial intelligence (Al) in the face of its*

7 See *https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225*

8 See *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689*

9 See *https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai*

10 See *https://www.gov.uk/government/publications/ai-safety-summit-2023-round-table-chairs-summaries-2-november*

11 See *https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023*

12 See *https://www.csis.org/analysis/ai-seoul-summit*

13 See *https://aiseoulsummit.kr/press/?uid=41&mod=document*

unprecedented advancements and the impact on our economies and societies.

4. Artificial Intelligence (AI) and Cybercrime

4.1. INTERPOL

INTERPOL published in June 2023: *The Toolkit for Responsible AI Innovation in Law Enforcement (AI Toolkit)*:[14]

In recent years we have seen Artificial Intelligence (AI) technologies become embedded in society and our daily lives.

AI technologies also have huge potential to support the work of law enforcement agencies. Successful examples of areas where AI systems are successfully used include automatic patrol systems, identification of vulnerable and exploited children, and police emergency call centres.

At the same time, current AI systems have limitations and risks that require awareness and careful consideration by the law enforcement community to either avoid or sufficiently mitigate the issues that can result from their use in police work.

With the recent developmental leaps in AI capabilities, particularly around Generative AI, the public debate around legal and ethical implications of AI systems, as well as the negative effects they could have on society and humanity, has exploded. It is important that these concerns are addressed in a timely fashion, particularly in a law enforcement context.

4.2. Europol

Europol has on March 27, 2023, updated on June 11, 2024,[15] made the following information on *ChatGPT - the impact of Large Language Models on Law Enforcement.*

Europol has focused on three groups of criminal activity of most concern for Europol:

- *Fraud and social engineering: ChatGPT's ability to draft highly realistic text makes it a useful tool for phishing purposes. The ability to reproduce language patterns can be used to impersonate the style of speech of specific individuals or groups. This capability can be abused at scale to mislead potential victims into placing their trust in the hands of criminal actors.*
- *Disinformation: ChatGPT excels at producing authentic sounding text at speed and scale. This makes the model ideal for propaganda and disinformation purposes, as it allows users to generate and spread messages reflecting a specific narrative with relatively little effort.*
- *Cybercrime: In addition to generating human-like language, ChatGPT is capable of producing code in a number of different programming languages. For a potential criminal with little technical knowledge, this is an invaluable resource to produce malicious code.*

4.3. FBI on Artificial Intelligence (AI)

The FBI has the following approach to Artificial Intelligence (AI):[16]

Our approach to AI fits into three different buckets—identifying and tracking adversarial and criminal use of AI, protecting American innovation, and FBI AI governance and ethical use.

- *The FBI is focused on anticipating and defending against threats from those who use AI and ML to power malicious cyber activity, conduct fraud, propagate violent crimes, and threaten our national security; we're working to stop actors who attack or degrade AI/ML systems being used for legitimate, lawful purposes.*
- *The FBI defends the innovators who are building the next generation of technology here in the U.S. from those who would steal it. This effort is also related to defense against malicious cyber activities, since all-too-often our adversaries are stealing our trade secrets, including AI, to turn it against the U.S. and U.S. interests.*
- *The FBI is also looking at how AI can help us further exercise our authorities to protect the American people—for instance, by triaging and prioritizing the complex and voluminous data we collect in our investigations, making sure we're using those tools responsibly and ethically, under human control, and consistent with law and policy.*

On May 8. 2024, FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence:[17]

The FBI San Francisco division is warning individuals and businesses to be aware of the escalating threat posed by cyber criminals utilizing artificial intelligence (AI) tools to conduct sophisticated phishing/social engineering attacks and voice/video cloning scams. The announcement, made today from the RSA cybersecurity conference at the Moscone Center in San Francisco, coincides with the division's outreach efforts to include an FBI booth at the conference and participation in multiple conference panel sessions during the week of May 6, 2024.

AI provides augmented and enhanced capabilities to schemes that attackers already use and increases cyber-attack speed, scale, and automation. Cybercriminals are leveraging publicly available and custom-made AI tools to orchestrate highly targeted phishing campaigns, exploiting the trust of individuals and organizations alike. These AI-driven phishing attacks are characterized by their ability to craft convincing messages tailored to specific recipients and containing proper grammar and spelling, increasing the likelihood of successful deception and data theft.

5. Judicial Decisions Support Systems

Courts around the world are increasingly using computer technology in their decision making.

14 Se *https://www.interpol.int/How-we-work/Innovation/Artificial-Intelligence-Toolkit*

15 See *https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement*

16 See *https://www.fbi.gov/investigate/counterintelligence/emerging-and-advanced-technology/artificial-intelligence*

17 See *https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence*

Legal information retrieval systems on Internet are now providing access to relevant information for the decisions.

Computers in courtrooms has enabled the judge access to a wide range of information on Internet, providing direct access to information for using it in the decision making, and to Artificial Intelligence (AI).

In this development, Judicial Decision Support Systems have been developed to assist the judge in the decision making. Such systems using Artificial Intelligence must not make the decisions, but only be used as a new remedy in the decision process. The judge must always be able to choose the proposed solution by Artificial Intelligence, or independently reject it.

The wise advice by Chief Justice Carsten Smith, the Supreme Court of Norway, at a conference in Singapore in 1996 was:

We must never forget that the main element in the judicial process is the human element – combined with the touch of the heart – to balance conflicting interests.

The institution Lovdata was established in 1981, by the Department of Justice and the Faculty of Law at the University of Oslo in Norway. Lovdata has published the Lov & Data since 1984.

Lov & Data is the leading publication in the Nordic countries on the development of new legal information, for all the users of the judicial systems. Lov & Data will be one of the leading publications in the future for the discussions of the legal regulations of Artificial Intelligence (AI).

Stein Schjølberg, pensjonert sorenskriver.

CJEU case C-159/23 on copyright protection of computer program's variable content

Av Jalmari Männistö

On 17th of October the Court Justice of the European Union ("CJEU") handed down its decision in the case C-159/23 Sony Computer Entertainment Europe Ltd v. Datel Design and Development Ltd and Others ("Case"). The Case concerned the scope of copyright protection of computer programs and is thus somewhat of a rare treat as these decisions are far and few between. In summary, the CJEU did not recognise that a computer program's content of a variable gained copyright protection as a part of a computer program and thus changing it did not amount to prohibited alteration of protected material. While the outcome is fairly simple, its implications are not necessarily that. To understand the decision and its reasoning there needs to be a short evaluation of the underlying legal principles and facts for the Case.

> The Case concerned the scope of copyright protection of computer programs and is thus somewhat of a rare treat as these decisions are far and few between.

Legal background

In the EU, protection of computer programs is harmonised under copyright as literary works. This is done particularly through various EU directives such as the computer programs directive (91/250/EC), the information society directive (2001/29/EC) and the software directive (2009/24/EC), of which the first and last regulate computer programs specifically and which in turn are transposed into national legislation (such as the Finnish Copyright Act that ironically recognised protection of computer programs under copyright before the EU). This essentially means that the *code* which composes the computer program is protected under copyright, which entails a prohibition of unwarranted reproduction, alteration, communication to the public etc. More specifically case law grants protection to the *source- and object code* of the computer program which forms its main executable text.[1] This code is then *text* which is granted copyright but importantly only insofar that text is the result of its creator's (author) conscious and creative choices.

Jalmari Männistö

Herein the distinction between *traditional* literary works and computer programs starts to become evident. Novels, poems, plays etc. are naturally creative in the whole of their expression but in the case of computer programs, parts of their text can be deemed as non-expressive of the author's creativity and thus not qualify for protection.[2] As computer programs exist in a functional technical environment where they need to be drafted in a specific way for the computer to interpret their functionality, those parts of the computer program which exist as a technical necessity do not gain protection under copyright. This means for example that the choice of a programming language or using certain technical solutions does not gain protection under copyright.

A major part of the CJEU's limited case law on computer programs has specifically addressed the scope of protection for computer programs. Most importantly the CJEU held famously in the SAS-case that the *functionality* of the computer program is not protected under copyright as it is outside of the direct expression of the author contained in the protected text (e.g. source code) and other interpreta-

1 See software Directive 2009/24/EC recitals 7, 10–11

2 For Finnish viewpoint prior to Computer programs directive 91/250/EC see Finnish HE 161/1990 p. 16 and Finnish Copyright Council TN 1989:7

tion would be against the objectives of international protection.[3] Similarly in IT Development case it was recognised that alterations specifically to the source code constitute infringement of copyright *an sich*.[4] Lastly (and importantly for the Case) neither are the methods by which the user makes use of the computer program, such as a graphical user interface, protected as computer programs.[5] Excluding user interfaces, the CJEU has not previously evaluated the protectability of certain parts of computer programs' code via differentiation of its component or module (sections by which the computer program can be divided via its functionality) and has opted for determining whether a part in question enables the infringement (alteration or reproduction) of the clearly protected part of the program.

The legal background for the evaluation of the protection (and in a way prohibited alterations) of computer programs is then to exclude all technically necessary and non-original material from the evaluation. Therefore, protectability and originality of a computer program is not all of its code, but merely those text and components which the author has made a conscious and creative effort in.[6] This is particularly difficult considering the context that computer programs, unlike traditional written works, exist purely in a digital format which means that their use and management creates reproduction and alterations of works within and between executing computers.[7]

The Case

In the Case at hand the CJEU was asked by the Bundesgerichtshof (German Federal Court of Justice) to evaluate whether the *content of the variable* produced by software A was protected so that the alteration made to it by software B was infringing its copyright by altering it while it was stored in the random-access memory (RAM) of the executing device.

For the sake of technical understanding, a *variable* is a part of computer program's code which designates a name and storage location (depending on the used programming language) for a specific data that is the *content of a variable*. This *content of a variable* can be quite literally anything from simple data to complex functions or combination of different variables. Both the variables, their parameters (how they are used) and *contents of the variables* arise from the source code of the computer program but may be altered in the course of its execution in the computer itself. Depending on its design, the RAM is used to store values, functions and other material necessary for the computer program's proper execution. In a nutshell, a computer program (such as an internet browser) stores data (such as content of the website or amount of *clicks*) which it needs/uses for its functioning on the RAM.

Background of the Case

The applicant in the Case, Sony Computer Entertainment Europe Ltd ("Sony") sold a video game console and accompanying games to the market. Datel Design and Development Ltd (along with its corporate group) ("Datel") developed and provided a software which upon installation to the console allowed users to alter certain aspects of their game experience (such as speed/boost of a vehicle) and how they controlled the game. Datel's software did this by altering certain values of data stored in the console's RAM (which is used to store data and material needed for execution of the software) which then the game used in its continuous processing.

Sony brought a claim in the Hamburg Regional Court against Datel alleging that Datel's software alters Sony's software in a manner contrary to copyright protection. Essentially Sony's argument was that the data transferred "outside" of the executing file of the computer program (meaning the RAM) is still within the scope of the "computer program" and thus protected, and in any case the set of instructions contributing to the achieved planned results or enabling certain sought functionality should be treated as part of the program, including data. In Sony's words the protection should be afforded to "the game experience created by the programmer". The Regional Court upheld Sony's claim in part whereas the Higher Regional Court dismissed Sony's action in its entirety. The referring German Federal Court of Justice (highest appellate court of civil and criminal matters) asked CJEU essentially two questions concerning the interpretation of the software directive 2009/24: first whether a content of a variable transferred to RAM belongs to the scope of protection of copyright of the primary computer program, and second whether its alteration by

3 C-406/10 – SAS Institute Inc. v World Programming Ltd, paras 38-40, and by analogy Case C-5/08 Infopaq International; "international protection" referring to the Berne Convention article 2 referenced in the decision.

4 C-666/18 – IT Development SAS v Free Mobile SAS, paras 32-34

5 C-393/09 – Bezpečnostní softwarová asociace, para 41

6 The practical test is also known as "Abstraction-filtration-comparison -method" following from the Computer Associates International Inc. v. Altai Inc. 982 F.2d 693 (2d Cir. 1992); Similarly followed in Finland via HelHo 1999:T:3571 and in the Finnish Copyright Council practice TN:2013:1

7 See software directive 2009/24/EC recital 13 and art.5(1) for exception on necessary exceptions.

another concurrent program would be an infringement of copyright.[8]

Legal evaluation of the CJEU

As a preliminary point, the CJEU's own evaluation of the facts and law is rather short and refers to the accompanying opinion of the Advocate General[9] ("Opinion") in its most important parts which is why both will be evaluated simultaneously.

The CJEU's evaluation starts by recognising and reiterating the distinction of computer software protectability to "*expression in any form of a computer program*" (as in article 1 of the software directive) excluding its underlying principles and ideas with a specific reference to limitations found in case law to graphical user interfaces (as merely ways in which the computer program is used) and functionality *per se* (as other interpretation would allow monopolisation of ideas). The CJEU's interpretation of the directive is then that it strictly and primarily protects the source- and object code of the computer program instead of means by the computer program and its functionalities are used as especially only the source- and object codes allow for the reproduction (prohibited copying) of the said computer program. Impliedly, as the *contents of the variables* do not make reproduction of the protected computer program possible, they do not have protection of copyright as computer programs. This strict view then excludes the contents of the variables in question as they are stored separately from the executable source code and because they do not by themselves allow for the reproduction of the protected computer program. Furthermore, the CJEU recognised in accordance with the Opinion as described below contents of the variables were not "forms of expression" but rather merely means of which users make use of the computer program's features. As the answer to the protectability of content of variables was negative CJEU did not separately assess the second question as an alteration to a non-protected part could not have been infringing.

The Opinion's argumentation (which the CJEU makes extensive and specific references to) contains more evolved legal argumentation on the specific role of variables and their content. The Opinion again maintains that the limitation of computer programs' protection to their text (code) which is the sole reflection of the author's intellectual creation is an intentional choice by the legislature to allow for competing software to exist. The Opinion recognises that *parameters of a variable*, meaning e.g. memory location, name and type of data are clearly capable of originality and thus protection under the software directive. Whereas the Opinion takes a rather strong stance on *content of the variable* not being an *element of computer program's code*. The Opinion maintains that in the current situation, the contents to be changed (and seeking protection) are not original expression to be granted protection as they are merely data external to the code that is reused in the running of the program and that "do not exist at the moment that the program is created by its author or when it is loaded into the computer's memory since they are generated only while the program is running". It is reiterated that the contents in question are the result of user's use of and progress in the computer program which "cannot be foreseen in advance, such as the [user's] behaviour". The *content of the variables* concerns then merely the operation of the program's pre-determined function and sequence. Thus, the Opinion takes a clearer and stronger stance that the *content of variables* does not gain protection as part of the computer program due to their lack of ability to infringe on the source code, but also due to their lack of originality as *text* and connection to the source code itself.

The CJEU also interestingly in multiple parts recognises a policy goal of limited protection of computer programs especially stating that the protection regime (according to computer programs directive) should not limit independent development (of software), block technical progress nor hinder the creation of alternative implementations or compatible products (while not using the same protected expression).

Analysis

The CJEU's ruling above has broadly two different facets: evaluation of copyright infringement and potential originality of variable's content.

First, the CJEU's outcome on the Case is not very surprising. As Datel's program was intentionally not able to supplement or reproduce any of the primary expression (source code) the underlying computer program was executing, it was clear that there was no infringement from a broader view on goals of copyright protection in the EU. However, the CJEU's heavy emphasis on this non-effect to the copyrightable material seems very much a case-by-case evaluation that could be very different upon just a slightly different technical implementation. What is noteworthy are the different factors which the CJEU used in determining in favour of non-infringement: alteration did not make any changes to the source code (or its execution), Datel's software had to run simultaneously with Sony's

8 Referring respectively to article 1 (referring to scope of application) and article 4(1)(b) (concerning restricted act of alteration) of the software directive 2009/24/EC; see para 24 of the Case

9 Opinion of Advocate General Szpunar delivered on 25 April 2024, ECLI:EU:C:2024:363

and the pro-competition stance of the underlying legal regime.[10]

Second, the evaluation of *contents of variables* lacking originality is much more interesting. Due to the multiple references by the CJEU to the core parts of the Opinion it is safe to assume that the legal analysis on *content of the variables* presented in the Opinion is applicable to the CJEU's outcome. As outlined above, the Opinion takes a rather strict stance on the possibility of *contents of variables* being protected as parts of computer program. It is however somewhat unclear as to which part of the Opinion's analysis is intended to be general and which *in casu* as all of the analysis happens under the title "Application in the present case". Therefore, especially considering the specific facts of the Case, the Opinion's established legal rule cannot necessarily apply for all *contents of variables* but rather should be understood within very specific caveats:

- In the Case the content of the variable was very simple in nature. Its originality by itself (which was not in dispute) was undoubtably not sufficient for copyright protection, but it would be interesting to consider what the outcome would have been if the variable or the content of it would have been more integral to the normal and proper functioning of the system. While it is reasonable that a mere alteration in a minor part of an expression does not infringe on the text, an alternative situation where alteration prohibits a certain part of intended expression could bring a different outcome.
- A non-negligible part of the analysis focused on the fact that the contents of the variable were transferred to the RAM wherein they were used by Sony's program and altered by Datel's. This distinction from other processing is a bit confusing, because the CJEU has not previously made a determination based on where a part of software code (which includes values) is transferred to. From the technology neutral point of view (as in the applicable software directive) the memory storage location should by all logic be non-determinative for the legal evaluation. It is not uncommon that both executable program and variables it generates are uploaded to RAM. As computer memory is not necessarily segmented in a way that makes a significant difference to its execution, it is not clear why this was part of the CJEU's reasoning.
- Especially the Opinion made a strong stance that a *content of a variable* is "not an element of *a computer program's code*" (note object of the sentence). This evaluation can be understandable from the point of view where we refer to simple values which the computer program generates during runtime following a player's actions. The stance is however less understandable when it is taken to refer *contents of variables* by default, as one can easily consider those variables which can generate contents that are not simple and "generated" only as a technical solution (not set value). Furthermore, and continuing from point above, nothing necessarily stops the content of the variable from being embedded into the clearly protected source code. From this point of view, both the originality of *contents of variables* and their inseparability from the source code could be challenged.
- Lastly, when the Opinion considers Sony's arguments on the protectability of "game experiences" it is important to note that the referring court made the request for a preliminary ruling only on the basis of the software directive. It would be interesting to consider whether Sony's argument to the protectability of content of variables (as comprising game experience) would have succeeded under a different legal norm especially as the CJEU has recognised in its case law the special nature of video games comprising of software and non-software elements.[11] It is also noteworthy that the Case did not concern technical protection mechanisms which Datel would have had to circumvent.

In conclusion, the Case offers some inherently valuable evaluation on the consideration of IPR infringement of computer programs' text through alteration of its parts, and a more academically interesting analysis on the originality and connection standards for computer programs' parts and code.

Jalmari Männistö, Board member of Finnish IT-law association (IT-oikeuden yhdistys), Associate - IP & Technology, Roschier Attorneys.

10 In paras 36 and 48 of the Case the CJEU made an analogy to the SAS Institute case C-406/10 and a direct reference to the explanatory memorandum to the Proposal for a Council Directive on the legal protection of computer programs (OJ 1989 C 91)

11 C-355/12 Nintendo Co. Ltd et al v. PC Box Srl, para 23; Similarly, it is worth to note that the Case concerned protection only under the software Directive 2009/24/EC and not e.g. the Information Society Directive 2001/29/EC to which the CJEU made explicit distinction and reasoning in the paras 27-29 of the Case.

DPIA og FRIA – Når inntrer plikten til å gjennomføre vurderingene og hvordan samspiller regelsettene?

Av Torben Aronsen Manndal

1. Innledning

I dagens digitale samfunn har bruk av kunstig intelligens blitt stadig mer fremtredende og relevant på tvers av ulike sektorer og bransjer. Den økende bruken av kunstig intelligens skyldes dens allsidige anvendelser og potensial til å transformere hvordan vi jobber, kommuniserer og lever.

Bruk av kunstig intelligens medfører likevel en betydelig risiko for fysiske personer.[1] EU har sett problemstillingen, og har de siste årene jobbet med verdens første regulering av kunstig intelligens. Resultatet av dette arbeidet er AI ACT, som trådte i kraft 1. august 2024.[2] Bestemmelsene vil gradvis inntre de neste årene.[3]

Dersom en aktør benytter et KI-system ved behandling av personopplysninger innenfor EUs grenser eller behandler personopplysningene til personer bosatt innenfor EU må dessuten bestemmelsene i personvernforordningen (GDPR) etterfølges. En av de viktigste bestemmelsene i GDPR er plikten til å gjennomføre en vurdering av personvernkonsekvenser (DPIA) forut for en planlagt behandling.[4]

1 De Gregorio og Dunn (2022) s. 489.
2 The AI Act Explorer (Tilgjengelig her: *https://artificialintelligenceact.eu/ai-act-explorer/*) (sist endret 13. juni) (sist lest 30. november)
3 EU Artificial Intelligence Act, Implementation Timeline (Tilgjengelig her: *https://artificialintelligenceact.eu/implementation-timeline/*) (sist endret 1. August 2024) (sist lest 30. november 2024).
4 GDPR art. 35.

Torben Aronsen Manndal

Dette vil være særlig viktig hvor behandlingen gjennomføres ved bruk av KI.

I min masteroppgave fra våren 2024 undersøkte jeg når den behandlingsansvarlige er forpliktet til å vurdere personvernkonsekvenser for fysiske personers rettigheter og friheter når behandlingen av personopplysninger gjennomføres ved bruk av kunstig intelligens. Oppgaven reiste to primære problemstillinger; når inntrer plikten, og hvordan er regelsettet harmonisert med AI Acts krav til å gjennomføre en forhåndsvurdering av fundamentale rettigheter ved førstegangs bruk av et høy risiko KI-system (FRIA).[5]

Denne artikkelen vil oppsummere funnene i masteroppgaven, og tar sikte på å bistå aktører som etter GDPR og AI Act vil være forpliktet til å gjennomføre både DPIA og FRIA.

5 AI Act art. 27.

2. Pliktsubjekter

Etter GDPR er det den behandlingsansvarlige som er forpliktet til å gjennomføre en DPIA.[6] Den behandlingsansvarlige er legaldefinert som den som bestemmer formålet med behandlingen og hvilke midler som skal benyttes, som blant annet at behandling skal skje ved bruk av kunstig intelligens.

Etter AI Act er tre nærmere angitte grupper av brukere (deployer) forpliktet til å gjennomføre en FRIA.[7] Brukere er legaldefinert som enhver «natural or legal person, public authority, agency or other body using an AI system under its authority». De tre gruppene av brukere er offentligrettslige organer, private aktører som tilbyr tjenester av allmenn interesse, og brukere av systemer som angitt i AI Act Annex III nr. 5 bokstav b[8] og c.[9]

3. DPIA og FRIAs funksjon i regelverkene

Personvernforordningens overordnende formål er å «sikre vern av fysiske personers rettigheter og friheter».[10] Dette er gitt utslag i en rekke risikovurderinger i GDPR, herunder også plikten til å gjennomføre en vurdering av personvernkonsekvenser.

6 GDPR art. 4 nr. 7.
7 AI Act art. 3 nr. 4.
8 KI-systemer som skal gjennomføre kredittvurderinger.
9 KI-systemer som skal gjennomføre risiko- og prisvurderinger ved livs- og helseforsikringer.
10 GDPR art. 1 nr. 2.

Hvor en vurdering av personvernkonsekvenser derimot skiller seg fra de øvrige risikovurderingene i personvernforordningen er at den potensielt kan forplikte den behandlingsansvarlige til å unnlate å gjennomføre den planlagte behandlingen.

Risikovurderingene i GDPR art. 24, 25 og 32 har tilnærmet identisk utforming, og det fremkommer at det skal gjennomføres «egnende tekniske og organisatoriske tiltak» etter en vurdering hvor det tas hensyn til behandlingens «art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighetsgrad». Det bestemmelsene har til felles er at risikonivået ved den konkrete behandlingen tilsier hvor omfattende de egnende tekniske og organisatoriske tiltakene som må gjennomføres er. Et høyt risikonivå tilsier således ikke at en behandling må avsluttes, men forplikter den behandlingsansvarlige til å gjennomføre mer omfattende tiltak for å på en tilstrekkelig måte oppnå den konkrete artikkelens formål.

Derimot fremkommer det av kravet til minsteinnholdet i en vurdering av personvernkonsekvenser at det skal gjennomføres en nødvendighets- og proporsjonalitetsvurdering.[11] Dersom en behandling ikke er proporsjonal eller nødvendig sett i lys av dens tiltenkte formål kan den behandlingsansvarlige dermed bli forpliktet til å unnlate å gjennomføre behandlingen.

At det er inntatt et krav til vurdering av personvernkonsekvenser i forordningen kan følgelig anses som en erkjennelse fra lovgiver at risikovurderingene ikke nødvendigvis tilstrekkelig ivaretar fysiske personers rettigheter og friheter dersom det foreligger høy risiko ved en behandling. GDPR art. 35 funksjon i forordningen er dermed å fungere som en sikkerhetsventil for å ivareta fysiske personers rettigheter og friheter.

11 GDPR art. 35 nr. 7 bokstav b.

FRIA har en liknende funksjon i AI Act. Ettersom vurderingen beror på om «fundamental rights» blir påvirket fremstår det tydelig at bestemmelsens formål er å minimere potensielle skader på slike rettigheter som kan inntreffe ved bruk av KI-systemet. Dette vil gjøres i tillegg til arbeidet utvikleren har gjort for å minimere slike risikoer under utviklingen av systemet. En begrunnelse til at lovgiver har valgt å ta inn et krav om forhåndsvurdering i AI ACT kan være at det vil være utfordrende for utviklere å vurdere og implementere skadeforebyggende tiltak for alle potensielle risikoer et KI-system kan utgjøre for fundamentale rettigheter under utviklingsfasen. En FRIA vil dermed i praksis fungere som en sikkerhetsventil for de potensielle risikoene utvikler ikke har greid å ta stilling til i utviklingsfasen.

4. Når inntrer plikten til å gjennomføre en DPIA ved behandling av personopplysninger ved bruk av KI

For at plikten til å gjennomføre en DPIA skal inntre må to vilkår være oppfylt. Det må foreligge «høy risiko», og denne risikoen må gjelde fysiske personers «rettigheter og friheter».[12]

Risiko er ikke definert i GDPR, men er anerkjent som en beskrivelse av et scenario og dets konsekvenser, hvor man tar hensyn til både sannsynlighet og skadeomfang.[13] Ordlyden «høy risiko» angir altså et krav om at alminnelig risiko ikke er tilstrekkelig for at vilkåret skal anses oppfylt, men at det kreves en mer omfattende risiko.

Heller ikke «rettigheter og friheter» er definert i forordningen. Ordlyden gir anvisning på et begrep som burde forstås vidt, men gir ingen pekepinn til hvilke rettigheter og friheter som vil være relevant. Det kan stilles spørsmål til hvorvidt ordlyden utelukkende omhandler forpliktelsene og prinsippene som er spesifisert i GDPR,[14] eller om ordlyden er en henvisning til GDPRs formålsbestemmelse og dermed også rettighetene og frihetene som nedfelles i EU-pakten.[15] Problemstillingen er ikke rettslig avklart.

Det finnes en rekke ulike KI-systemer, med varierende bruks- og virkeområder. I min masteroppgave undersøkte jeg hvilke nærmere aspekter og egenskaper ved ulike KI-systemer som ville medføre høy risiko for fysiske personers rettigheter og friheter når systemet behandler personopplysninger, og følgelig utløse plikten til å gjennomføre en DPIA. Det vil tas utgangspunkt i prinsippene som er nedfelt i GDPR art. 5, da de utgjør positive rettigheter som den registrerte kan påberope seg.

Generativ KI

Et velkjent problem ved bruk av kunstig intelligens er dets tendens til å *hallusinere*. Dette forstås som når KI-systemet genererer falskt eller meningsløst innhold og presenterer det som sannhet.[16] I en studie fra 2023 ble det undersøkt i hvilken grad fem utvalgte generative KI-systemer produserte hallusinerende innhold. Det mest presise systemet var ChatGPT-4, som hallusinerte i 6 % av tilfellene. Det minst presise systemet var TruthGPT, som hallusinerte i 77 % av tilfellene.[17]

Bruk av generativ KI i behandlinger av personopplysninger kan dermed utgjøre en risiko for brudd på prinsippet om riktighet,[18] da også usann informasjon vil anses som personopplysninger.[19] Et eksempel på et slikt brudd på prinsippet om riktighet er når Metas chatbot Blen-

12 Se GDPR art. 35 nr. 1.
13 Se blant annet GDPR fortalepunkt 75 og 76.
14 Se blant annet GDPR kapittel 2 og 3.
15 Se GDPR art. 1 nr. 1.
16 Se Feuerriegel mfl. (2024) s. 111.
17 Se McIntosh mfl. (2023) s. 3.
18 Se GDPR art. 5 nr. 1 bokstav d.
19 Se Opinion 4/2007 on the Concept of Personal Data s. 6.

derBot hevdet at den nederlandske politikeren Maria Schaake var en terrorist.[20]

Fremskritt i det tekniske nivået vil redusere prosentandelen hallusinasjon,[21] og følgelig hvor regelmessig prinsippet om riktighet brytes ved behandlinger av personopplysninger ved bruk av generativ kunstig intelligens. Likevel vil disse fremskrittene muliggjøre at kunstig intelligens tas i bruk i behandlinger av større viktighet,[22] hvor skadepotensialet ved behandling av personopplysninger øker.

Skjeve maskinlæringsalgoritmer

Et KI-system vil kun være like objektivt som sin utvikler. Gjennom utviklingsfasen til en maskinlæringsalgoritme vil det benyttes treningsdata, som for eksempel personopplysninger.

Treningsdataen vil gjenspeile utviklerens verdenssyn, og maskinlæringsalgoritmen blir således et produkt som viderefører utviklerens etablerte oppfatninger. Dersom utviklerens etablerte oppfatninger inkluderer fordommer eller stereotyper vil dette videreføres ved bruk.[23] Slike maskinlæringsalgoritmer kalles *skjeve maskinlæringsalgoritmer*. Et KI-system som består av slike maskinlæringsalgoritmer, vil være forutinntatt.[24]

Problematikken oppstår særlig dersom KI-systemer skal brukes til å ta beslutninger som tildeler eller fratar fysiske personer muligheter eller ressurser. Eksempler på dette er hvor KI-systemet skal bidra i ansettelsesprosesser eller avgjøre lånesøknader. Skjevhet i maskinlæringsalgoritmen kan medføre at fordelingen av muligheter eller ressurser primært tilfaller en gruppe, på bekostning av de resterende gruppene. Forutinntatt kunstig intelligens vil da videreføre skjevheten i treningsdataen under beslutningsprosessen, noe som kan resultere i forskjellsbehandling mellom individer. Et KI-system bestående av skjeve maskinlæringsalgoritmer som benyttes i beslutningstakningsprosesser vil medføre en høy risiko for brudd på prinsippet om rettferdighet i GDPR art. 5 nr. 1 bokstav a.

Kontinuerlig lærende KI-systemer

Prinsippet om formålsbegrensning utgjør primært en begrensning under utviklingen av KI-systemer. Prinsippet medfører at all dataen som samles inn under utviklingen må ha «spesifikke, uttrykkelige angitte og berettigede formål, og ikke viderebehandles på en måte som er uforenlig med disse formålene».[25] For å oppnå ønsket prestasjonsnivå ved KI-systemet behøves det store mengder data.[26] På grunn av den store mengden data som kreves, kan det være utfordrende for utviklerne å samle inn den nødvendige dataen uten å bryte prinsippet.

Dersom utviklerne likevel oppnår ferdigstillelse av KI-systemet uten å bryte med prinsippet vil faren være avverget. KI-system er da *offline*,[27] og maskinlæringsalgoritmen vil ikke endres ved bruk. Den vil da ikke lære av personopplysningene den blir presentert for, men utelukkende vurdere de opp mot formålet den er satt til. Det vil da heller ikke være noe fare for at prinsippet om formålsbegrensing brytes.

Det oppstår derimot en særegen problemstilling ved *online* KI-systemer,[28] altså hvor maskinlæringsalgoritmen kontinuerlig lærer og forbedrer seg gjennom brukstiden. KI-systemet vil da være i bruk, men fortsatt utvikles. KI-systemets utvikling er direkte tilknyttet personopplysningene det mottar mens det brukes. Det vil således være vanskelig å forutse nøyaktig hva den konkrete maskinlæringsalgoritmen vil lære, og hvordan den vil utvikle seg.[29]

Slike KI-systemer kan tilegne evnen til å løse problemer det i utgangspunktet ikke var programmert til. Dette kan medføre at personopplysninger potensielt viderebehandles for formål som ikke er forenlig med det initiale formålet. Det kan dermed foreligge høy risiko for at kontinuerlig lærende KI-systemer vil bryte med prinsippet om formålsbegrensning.

«Svart boks» -maskinlæringsalgoritmer

Noen KI-systemer er så teknologiske avanserte at det oppstår et fenomen kalt «*svart boks*». Med dette menes mennesker vil ha vanskeligheter med å påvise hvordan systemet kom frem til en konkret avgjørelse.[30]

Ved behandling av personopplysninger ved bruk av «svarte boks» -maskinlæringsalgoritmer kan det være vanskelige å forstå og forklare hvordan KI-systemet tar beslutninger. Dersom den behandlingsansvarlige ikke kan beskrive hvordan KI-systemet kom frem til det konkrete svaret, kan det heller ikke påvises hvilke parametere maskinlæringsalgoritmen la vekt på i avgjørelsen. Slike avgjørelser vil ikke være forutsigbar eller oversiktlig for den registrerte.

Behandling av personopplysninger ved bruk av KI-systemer bestående av «svart boks» -maskinlæringsalgoritmer vil dermed utgjøre en høy risiko for brudd på prinsippet om åpenhet.[31]

20 Se Heikkilä (2022).
21 Se McIntosh mfl. (2023) s. 3. Prosentandelen hallusinasjon ble redusert med 7 % i overgangen fra ChatGPT 3.5 til ChatGPT 4.
22 Se Hauglid og Mahler (2023) s. 3. Bruk av generative KI til blant annet diagnostiserings- og beslutningsstøtte for helsepersonell.
23 Bala (2019) s. 263.
24 De Gregorio og Dunn (2022) s. 489.
25 Se GDPR art. 5 nr. 1 bokstav b.
26 Se Hauglid og Mikalsen (2022) s. 423.
27 Vokinger mfl. (2022) s. 14.
28 Ibid.
29 Se Zemčík (2021) s. 362.
30 Janiesch mfl. (2021) s. 688.
31 Se GDPR art. 5 nr. 1 bokstav a.

Plikten til å vurdere personvernkonsekvenser vil følgelig inntre.

5. Når inntrer plikten til å gjennomføre FRIA?

Som nevnt ovenfor i punkt 2 er kun tre grupper brukere forpliktet til å gjennomføre en FRIA. Vilkårene for når plikten til å gjennomføre en FRIA inntrer følger av AI Act art. 27 nr. 1. Det første vilkåret er at KI-systemet som tas i bruk må være klassifisert som høy-risiko. Hvorvidt det konkrete KI-systemer er å anse som høy-risiko følger av AI Act art. 6. Det andre vilkåret er at brukeren av KI-systemet ikke har tatt det i bruk tidligere.

Etter at KI-systemet er tatt i bruk foreligger det dessuten en plikt til å gjenta vurderingen dersom den initiale vurderingen er utdatert eller ikke treffende.[32]

6. Hvordan er regelsettene harmonisert?

Vilkår for inntredelse

Selv om det kan påstås at regelsettene har samme funksjon i sine respektive forordninger er vilkårene for når plikten til å gjennomføre DPIA og FRIA inntrer svært ulike. Dette har bakgrunn i forordningenes ulike risikotilnærming. Bestemmelsene i GDPR forutsetter at den behandlingsansvarlige mest presist kan vurdere risikoene ved de aktuelle behandlingene og hvilke tiltak som må gjennomføres for å redusere denne.[33] EU har derimot tatt motsatt risikotilnærming ved arbeidet med AI Act. Hvilke forpliktelser forordningen tillegger det aktuelle pliktsubjektet avhenger av hvordan risikokategori KI-systemet aktøren benytter seg av er plassert i.

Materielt innhold

GDPR art. 37 nr. 7 bokstav a–d fremstiller bare minstekravene til vurderingen av personvernkonsekvenser, og enkelte behandlinger vil dermed kreve mer omfattende vurderinger for å tilstrekkelig vurdere personvernkonsekvensene. Den behandlingsansvarlige er forpliktet til å minst beskrive de planlagte behandlingene og deres formål. Videre må det gjennomføres en nødvendighet- og forholdsmessighetsvurdering for behandlingen sett i forhold til dens formål. Deretter må risikoene for de registrertes friheter beskrives. Avslutningsvis må det beskrives hvilke planlagte tiltak som skal gjennomføres for å håndtere disse risikoene.[34]

AI ACT art. 27 nr. 1 bokstav a–f fremstiller hvilke konkrete vurderinger som skal gjennomføres i en forhåndsvurdering. For det første må det inkludere en beskrivelse av prosessene ved bruk av høyrisiko KI-systemet i samsvar med dets tiltenkte formål. Videre må tidsperioden og hvor ofte systemet skal brukes beskrives. Deretter må det vurderes hvilke kategorier av fysiske personer og grupper som sannsynligvis vil bli påvirket ved den konkrete bruken, samt de spesifikke skaderisikoene det er sannsynlig vil påvirke de identifiserte personene eller gruppene. Videre må det beskrives hvilke tiltak det er tatt for å sørge for menneskelig tilsyn over systemet. Avsluttende må vurderingen inneholde tiltakene som skal gjennomføres dersom risikoene materialiserer seg, samt hvordan intern styring og klager skal håndteres.[35]

Forordningenes ulike risikotilnærming medfører at brukeren etter AI Act er forpliktet til å gjennomføre mer detaljerte og omfattende vurderinger enn hva den behandlingsansvarlige er etter GDPR. Vurderingene som skal gjennomføres har likevel flere likheter.

Harmoniserende bestemmelse i AI Act art. 27 nr. 4

Som følge av disse likhetene har EU inntatt en bestemmelse som beskriver forholdet mellom DPIA og FRIA i AI Act art. 27 nr. 4.

Ordlyden lyder slik:

If any of the obligations laid down in this Article is already met through the data protection impact assessment conducted pursuant to Article 35 of Regulation (EU) 2016/679 (…), the fundamental rights impact assessment referred to in paragraph 1 of this Article shall complement that data protection impact assessment.

En naturlig språklig forståelse av ordlyden «complement» taler for at dersom en DPIA etter GDPR art. 35 nr. 1 har oppfylt «obligations» etter AI Act art. 27 så behøver ikke en FRIA å gjenta den konkrete forpliktelsen. Bestemmelsen er med andre ord ment å virke ressursbesparende for brukeren, ved at aktøren slipper å gjennomføre den samme vurderingen to ganger. For å klargjøre i hvilken grad regelsettene er harmonisert er det nødvendig å avgjøre innholdet av ordlyden «obligations».

En naturlig forståelse av ordlyden obligations vil være et ansvar for å gjennomføre en konkret handling. Oversatt til norsk vil dette være forpliktelser. Problemstillingen blir således å klarlegge omfanget av hver forpliktelsene som oppstilles i AI Act art. 27.

AI Act art. 27 nr. 1 pålegger brukeren til å gjennomføre en forhåndsvurdering av konsekvensene for fundamentale rettigheter, og presenterer seks nærmere presiserte vurderinger som inngår i denne helhetlige vurderingen. Videre pålegges brukeren å gjenta vurderingen dersom den ikke anses som presis etter KI-systemet er tatt i bruk.[36] Brukeren pålegges dessuten å oversende resultatet av forhåndsvurderingen til den nasjonale tilsynsmyndigheten.[37] Sistnevnte utgjør utvilsomt en separat forpliktelse.

Det oppstår dermed et spørsmål om de nærmere presiserte vurderingene som oppstilles i art. 27 nr. 1

32 Se AI Act art. 27 nr. 2.
33 Se De Gregorio og Dunn (2022) s. 489.
34 Se GDPR art. 35 nr. 7 bokstav a-d.
35 Se AI Act art. 27 nr. 1 bokstav a-f.
36 Se AI Act art. 27 nr. 2.
37 Se AI Act art. 27 nr. 3.

bokstav a–f utgjør separate forpliktelser eller om de samlet utgjør en forpliktelse. Ordlyden i AI Act art. 27 nr. 4 isolert sett gir ingen veiledning for hvordan tolkningsalternativ som burde legges til grunn. Det fremkommer ingen avklaring fra fortalen, og det foreligger heller ingen avklaring i form av retningslinjer fra AI Office.[38] For å besvare problemstillingen må det dermed tas utgangspunkt i en kontekstuell- og formålsorientert tolkning av bestemmelsen i sin helhet.

I AI Act art. 27 nr. 2 benyttes ordlyden «obligation» om den generelle plikten til å gjennomføre en forhåndsvurdering for første gangen det konkrete KI-systemet tas i bruk. Dette taler sterkt i retning av at vurderingene etter AI Act art. 27 nr. 1 bokstav a–f samlet er å anse som en forpliktelse. Dessuten brukes ordlyden «elements» i art. 27 nr. 2 om de ulike vurderingene i nr. 1 bokstav a–f. Ordlyden element forstås som en enkel komponent i en større helhet. Ordlyden omtaler altså hver enkeltstående vurdering i AI Act art. 27 nr. 1 bokstav a–f som en enkel komponent. Dette taler også for at de enkelte vurderingene samlet utgjør en forpliktelse.

Dersom det legges til grunn at de enkelte vurderingene i AI Act art. 27 nr. 1 bokstav a–f samlet utgjør en enkelt forpliktelse vil det derimot samsvare dårlig med formålet bak bestemmelsen. AI Act art. 27 nr. 4 formål er å effektivisere prosessen når den brukeren er forpliktet til å gjennomføre en forhåndsvurdering av fundamentale rettigheter, men allerede har gjennomført en vurdering av personvernkonsekvenser. Dette begrunnes i ordlyden «complement», og at brukeren ved forhåndsvurderingen da ikke behøver å gjenta den allerede oppfylte forpliktelsen.

Hvis en forhåndsvurdering av fundamentale rettigheter skal «complement» den allerede gjennomførte vurderingen av personvernkonsekvenser må det naturligvis være gjenværende forpliktelser i førstnevnte. Hvis det da legges til grunn at hver enkeltvurdering i AI Act art. 27 nr. 1 bokstav a–f samlet utgjør en enkelt forpliktelse vil det således ikke gjenstå ytterligere forpliktelser som må utføres etter bestemmelsen. Det vil da heller ikke være noe formål i å forsøke å effektivisere prosessen. Tolkningsalternavet vil altså medføre at AI Act art. 27 nr. 4 mister sin hensikt. Hvilket tolkningsalternativ som er korrekt, er ikke tydelig og problemstillingen har ikke et klarlagt svar. Problemstillingen behøver således rettslig avklaring i fremtiden.

Kan en DPIA oppfylle en «obligations» oppstilt i AI Act art. 27?

Da det nærmere innholdet i ordlyden «obligations» ikke er rettslig avklart vil begge tolkningsalternativene drøftes.

Tas det utgangspunkt i det første tolkningsalternativet blir problemstilling om en vurdering av momentene oppstilt i GDPR art. 35 nr. 7 bokstav a–d også vil behandle *alle* enkeltvurderingene som oppstilles i AI Act art. 27 nr. 1 bokstav a–f.

Til tross for fellestrekkene mellom vurderingene er det fundamentale ulikheter i deres rekkevidde. Selv om en vurdering av personvernkonsekvenser skal inneholde de planlagte tiltakene for å håndtere risikoene ved en behandling,[39] vil dette ikke nødvendig overlappe med kravet om at en FRIA skal inneholde en beskrivelse av tiltakene som er tatt for å sørge for menneskelig tilsyn over KI-systemet.[40] AI Act art. 27 nr. 1 bokstav f krever dessuten at tiltakene som skal gjennomføres dersom de aktuelle risikoene materialiserer seg skal beskrives, samt hvordan intern styring og klager skal håndteres. Dette er den behandlingsansvarlige ikke forpliktet til å inkludere i gjennomføringen av vurderingen av personvernkonsekvenser.

Den mest sentrale ulikheten i vurderingene er likevel omfanget av relevante rettigheter som skal inngå i vurderingen. En FRIA skal vurdere konsekvensene for alle potensielle berørte fundamentale rettigheter. Dette forstås som at alle rettighetene som fremkommer av EU-pakten vil være relevante i vurderingen. En vurdering av personvernkonsekvenser vil derimot hovedsakelig omhandle behandlingens potensielle konsekvenser for personvernet.

Dersom enkeltvurderingene oppstilt i AI Act art. 27 nr. 1 bokstav a–f samlet utgjør en enkelt forpliktelse vil en vurdering av personvernkonsekvenser ikke kunne oppfylle denne.

Den neste problemstillingen blir dermed om en vurdering av personvernkonsekvenser kan oppfylle en forpliktelse dersom enkeltvurderingene som oppstilles i AI Act art. 27 nr. 1 bokstav a–f utgjør separate forpliktelser.

Ordlyden anvendt i GDPR art. 35 nr. 7 bokstav a og AI Act art. 27 nr. 1 bokstav a inneholder store likheter. Av førstnevnte fremkommer det at en vurdering av personvernkonsekvenser blant annet skal inneholde en «[s]ystematic description of the envisaged processing operations and the purposes of the processing».[41] Av sistnevnte fremkommer det at en FRIA skal inneholde «a description of the deployer´s processes in which the high-risk AI system will be used in line with its intended purpose».[42] Begge vurderingene skal beskrive de planlagte behandlingene og dets formål. Det er dermed rimelig å legge til grunn at en vurdering av personvernkonsekvenser vil oppfylle kra-

38 Se AI Act art. 3 nr. 47.

39 Se GDPR art. 35 nr. 7 bokstav d.

40 Se AI Act art. 27 nr. 1 bokstav e.

41 Se GDPR art. 35 nr. 7 bokstav a.

42 Se AI Act art. 27 nr. 1 bokstav a.

vet som oppstilles i AI Act art. 27 nr. 1 bokstav a.

En vurdering av personvernkonsekvenser kan således oppfylle en forpliktelse dersom enkeltvurderingene som oppstilles i AI Act art. 27 nr. 1 bokstav a–f utgjør separate forpliktelser.

7. Hvordan kan behandlingsansvarlige som tar i bruk KI ved behandlinger av personopplysninger bistås?

Det er i artikkelen redegjort for hvilke ulike tekniske aspekter ved kunstig intelligens som kan utgjøre en høy risiko for fysiske personers rettigheter og friheter. Ved bruk av slike KI-systemer vil plikten til å vurdere personvernkonsekvenser inntre. Det vil likevel kunne være utfordrende for den behandlingsansvarlige å presist vurdere om vilkårene er oppfylt da det krever omfattende tekniske kunnskaper om det konkrete KI-systemets teknologiske evner. EU har sett problemstillingen og har derfor pålagt leverandører en informasjonsplikt ovenfor brukere.[43]

Det er etter min mening likevel ikke tilstrekkelig med denne informasjonen for tilfellene hvor brukeren skal gjennomføre en behandling av personopplysninger. Jeg er her av den oppfatning at informasjonsplikten ikke gir tilstrekkelig veiledning for hvordan brukeren, som etter reglene i GDPR er den behandlingsansvarlige, skal vurdere hvorvidt bruken av KI-systemet kan medføre høy risiko for rettigheter og friheter. Dette kan derimot løses ved å lage veiledninger som har fokus på etterlevelse av bestemmelsen i begge forordningene.

Artikkelen har videre funnet at hvorvidt regelsettene i GDPR art. 35 og AI Act art. 27 er harmonisert beror på innholdet i ordlyden «obligations». Jeg er her av den oppfatning at hver enkeltvurdering opplistet i AI Act art. 27 nr. 1 bokstav a-f utgjør separate forpliktelser. Det legges avgjørende her avgjørende vekt på at dette tolkningsalternativet vil medføre bedre harmoni mellom regelsettene i GDPR art. 35 og AI Act art. 27. Problemstillingen burde likevel avklares av EU.

43 Se bla. AI Act art. 13 og AI Act art. 26 nr. 9

8. Kilder

EU-rett

Direktiver og forordninger

EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av Side 51 av 57 personopplysninger og om fri utveksling av slike opplysninger samt om opphe-ving av direktiv 95/46/EF (generell personvernforordning) [PVF, GDPR]

Veiledninger

Article 29 Data Protection Working Party. WP136, Opinion 4/2007 on the concept of personal data, Adopted 20 June 2007

Artikler

Bala, Nila. «THE DANGER OF FACIAL RECOGNITION IN OUR CHILDREN'S CLASSROOMS.» Duke Law and Technology Review, vol. 18, no. 1, 2019, s. 249-267.

De Gregorio, Giovanni, and Pietro Dunn. «THE EUROPEAN RISK-BASED APPROACHES: CONNECTING CONSTITUTIONAL DOTS IN Side 54 av 57 THE DIGITAL AGE.» Common Market Law Review, vol. 59, no. 2, 2022, s. 473–500.

Feuerriegel, Stefan, mfl. «Generative AI.» Business & Information Systems Engineering, vol. 66, no. 1, 2024, s. 111–12

Hauglid, Mathias Karlsen, and Tobias Mahler. «Doctor Chatbot: The EU's Regulatory Prescription for Generative Medical AI.» Oslo Law Review, vol. 10, no. 1, 2023, s. 1–23.

Hauglid, Mathias K., and Karl Øyvind Mikalsen. «Tilgang Til Helseopplysninger i Maskinlæringsprosjekter.» Lov Og Rett, vol. 61, no. 7, 2022, s. 419–439.

Heikkilä, Melissa. «What Does GPT-3 'Know' about Me?» MIT Technology Review.Com, 2022, p. MIT Technology Review.com, 2022-08-31.

Janiesch, Christian, mfl. Machine Learning and Deep Learning. Electronic Markets, vol. 31, no. 3, 2021, s. 685-695

McIntosh, Timothy R., et al. «A Culturally Sensitive Test to Evaluate Nuanced GPT Hallucination.» IEEE Transactions on Artificial Intelligence, 2023, s. 1–13.

Vokinger, Kerstin Noëlle, et al. «Lifecycle Regulation and Evaluation of Artificial Intelligence and Machine Learning-Based Medical Devices.» Cambridge University Press, 2022, s. 13–21.

Zemčík, Tomáš «Failure of Chatbot Tay Was Evil, Ugliness and Uselessness in Its Nature or Do We Judge It through Cognitive Shortcuts and Biases?» AI & Society, vol. 36, no. 1, 2021, s. 361–367

Internettadresser

The AI Act Explorer (Tilgjengelig her: https://artificialintelligenceact.eu/ai-act-explorer/) (sist endret 13. juni) (sist lest 30. november)

EU Artificial Intelligence Act, Implementation Timeline (Tilgjengelig her: https://artificialintelligenceact.eu/implementation-timeline/) (sist endret 1. August 2024) (sist lest 30. november 2024).

Torben Aronsen Manndal. Advokatfullmektig ved LAG advokat AS.

Data Vaccination: Balancing Data Security and Utility

Av Changkyu Choi and Marius Aasan

Changkyu Choi

Marius Aasan

The recent decision by the newly elected President of the United States to designate an anti-vaccine theorist as the prospective Secretary of the Department of Health and Human Services prompts reflection on the implications for public health and immunization in society as a whole. Vaccines act as a critical safeguard against pathogens in an increasingly globalized world, where the degree of separation between individuals is much lower than in previous times, increasing the likelihood of interactions between humans and other species across the globe.

The notion of safety through vaccination provides an interesting analogy for data security and privacy in the information era. Digital interactions between online users have become a major source of large-scale data-gathering efforts, and collecting and processing vast amounts of data has become central to business operations. The momentum of data acquisition and curation has only increased with the rise of artificial intelligence (AI) systems, which can automate the curation of enormous quantities of data. As a result, privacy is facing growing threats from malicious attacks and unauthorized use.

Foundation models

A recent trend in AI is the increased use of foundation models for data processing pipelines. At their core, these foundation models are trained to learn relationships and associations from raw data through a form of semantic data compression. Documents, images, and signals are compressed into a latent vector representation space. While this compressed representation abstracts away the original input dimensions, it remains fundamentally rooted in the structure and semantics of the input data.

> The notion of safety through vaccination provides an interesting analogy for data security and privacy in the information era.

Today, large-scale training is often conducted using *contrastive learning* raw data is processed in a way that similar data points are mapped closer together in the representation space, while dissimilar data points are mapped further apart. This learning paradigm is commonly categorized as *self-supervised learning*, distinguishing it from traditional frameworks where *supervision* provides explicit guidance for learning.

In a supervised learning setup, human annotations are required to define a specific class or target variable that the model aims to predict for each individual data point. By exposing the model to a sufficient number of annotated examples during training, it learns to associate input data with the corresponding annotations. In contrast, the self-supervised learning paradigm circumvents the need for costly and labor-intensive human annotations by leveraging intrinsic structures or relationships within the data itself. This approach has emerged as a pivotal innovation, facilitating the development of more general and scalable foundation models.

The dilemma

Foundation models enable fast and high-quality information retrieval through *vector databases*, which offer remarkably efficient storage and retrieval of data. While this form of information retrieval provides significant societal benefits, it also raises critical concerns, particularly regarding data security. A single vector, or a collection of vectors, can potentially be exploited to infer sensitive

details such as an individual's location, health status, personal relationships, or economic information.

This pressing challenge lies at the forefront of current AI research: is it possible to *obfuscate* sensitive data embedded within representation vectors while preserving their utility for legitimate applications? Extending the analogy, can we *vaccinate* representation vectors against privacy risks while minimizing the loss of their representational power and functionality?

Information theory and compression

To achieve an optimal balance between ensuring security and preserving utility, it is crucial to mathematically formulate these two contrasting concepts, enabling the AI model to learn the optimal representations. Within the field of information theory, this challenge is addressed through a mathematically rigorous framework known as the *informational bottleneck*.

This framework can be understood as a process of funneling raw data through a bottleneck to distill its most essential semantic information into a compressed representation space. When processing high-dimensional raw data, models employ this approach to retain only the information most relevant for downstream tasks. Typically, the system is divided into two components: an *encoder*, which compresses the raw data into a succinct representation, and a *decoder*, which retrieves the necessary information for downstream tasks. The term "bottleneck" highlights the constrained dimensionality of the encoded data, defining the representation space where these effective vector representations reside.

Adversarial attacks

One particularly fruitful area of AI research has focused on developing methods to both create and defend against *adversarial attacks*—small perturbations specifically designed to cause a model to consistently misclassify data. The art of designing such attacks lies in identifying minimal perturbations to input data that remain imperceptible to human observers while being effective at deceiving the model. The theoretical advancements in adversarial attacks have significantly improved model robustness, paving the way for more secure and accurate AI systems in everyday practical applications.

By subverting the principles underlying adversarial attacks, we find that the problem can be reposed as a way to mitigate privacy concerns in vectors extracted from foundational models. Our research focuses on the discovery of *representational vaccines*, where a representation vector is *vaccinated* by adding a carefully crafted vaccine vector. Within this framework, the highest level of security is achieved when the data becomes completely unidentifiable, for instance, by introducing strong, unstructured, noise-like representations. However, this approach inherently reduces utility, as the resulting vectors lose all representational power. Conversely, the highest utility is achieved when the vaccine vector is weak, but this compromises security, as insufficient protection leaves the data vulnerable to unauthorized use.

The challenge of designing data vaccines parallels the task of creating adversarial attacks but operates in a different domain. While attacks manipulate raw data, vaccines act within the latent representation space. Our research applies the trade-off between utility and security to establish principles that enable models to learn representations that optimally balance these competing objectives. Leveraging the informational bottleneck framework, we systematically process representations to eliminate information outside the scope of the model's intended use, thereby aligning security and utility in a structured and principled manner.

VACCINE

Our proposed method—appropriately named VACCINE (Visually Alike, Covertly Contaminated, Information-theoretic Neural Embeddings)—is designed to mitigate risks associated with the unauthorized exploitation of data in AI systems. Specifically, our approach focuses on learning *secure representations* that cannot be utilized for unauthorized tasks. These representations are designed such that, even if exposed, they cannot be easily repurposed for illegitimate or unauthorized uses. Importantly, these learned representations retain the functional utility of the data, ensuring its continued applicability for legitimate purposes. Consequently, achieving an optimal balance between ensuring security and preserving utility is a critical challenge that ultimately determines the success of data vaccinations.

The development of representational data vaccines is grounded in the the information bottleneck framework. Within this framework, our proposed VACCINE learns the vaccine representation to ensure that vaccinated data retains *sufficient* information for task-specific functionality in authorized systems. Conversely, for unauthorized systems that attempt to exploit the underlying data structure, the vaccine representation is tailored to obscure exploitable information while preserving only the *minimal* structural information of the original data within the vaccinated data space.

This is achieved by learning a representation that minimizes the mutual information between the vaccinated data and the original data for *security*, under the condition that functional *utility* is preserved. We conducted experiments on image reconstruction tasks to evaluate functionality. The reconstructions of both the vaccinated data and the original data appear visually alike; however, their structural information differs significantly. For instance, the closest data sample to a gi-

Illustrasjon: Colourbox.com

ven instance in the original data may no longer be the closest in the vaccinated data.

Implications for legal practice and regulation

Our research focuses on improving the alignment of technological innovation with regulatory compliance, while retaining the practical utility of AI models for the benefit of society as a whole. Work on representational vaccines offers a promising approach to embedding secure representations within data processing pipelines, providing a proactive solution to the unauthorized exploitation of sensitive data.

The principles and techniques described in our research aim to align data-driven AI systems with evolving legal standards and regulatory requirements. By safeguarding sensitive information at a fundamental representational level, methods like VACCINE offer jurists and policymakers valuable tools to translate legal mandates surrounding data minimization, privacy, and compliance into practical technical measures.

Nevertheless, the adoption of these technologies raises important questions about legal accountability, ownership of modified data, and the ethical boundaries of data obfuscation. As foundational AI models are integrated into critical infrastructure, the responsibility for ensuring secure and ethical AI systems will increasingly intersect with privacy laws in complex and unforeseen ways. For legal practitioners, understanding the trade-offs between security and utility in modern large-scale data acquisition and curation is becoming ever more essential. A detailed knowledge of how these pipelines are constructed can help inform future discussions on liability, compliance, and the creation of legal frameworks that accommodate the evolving landscape of AI technologies.

> By safeguarding sensitive information at a fundamental representational level, methods like VACCINE offer jurists and policymakers valuable tools to translate legal mandates surrounding data minimization, privacy, and compliance into practical technical measures.

Changkyu Choi, he received his PhD in machine learning from UiT The Arctic University of Norway in 2023 and is currently a postdoctoral researcher at Visual Intelligence (VI), a Norwegian Centre for Research-Based Innovation. His research interests focus on robust representation learning in latent spaces, with a particular emphasis on shared representations across diverse data modalities, such as image-language and natural image-marine acoustics. Based at the VI Oslo Hub at the University of Oslo, he actively collaborates with the VI Tromsø Hub at UiT, where he contributes to ongoing research projects and teaches advanced topics in machine learning.

Marius Aasan is a PhD researcher in the Digital Signal Processing and Image Analysis group at the Institute of Informatics at the University of Oslo, as well as a researcher in the Visual Intelligence consortium. His research investigates geometric priors and hierarchical learning on natural images and seismic data, and probabilistic modelling of hierarchical structures in signals. His work involves explainability and interpretability in artificial intelligence systems, representation learning, and theoretical machine learning.

Når kan behandlingsansvarlige belage seg på 'berettiget interesse' som behandlingsgrunnlag? Nye retningslinjer fra EDPB

Av Cecilie Island og Melissa Jakobsen Tveit

Cecilie Island

Melissa Jakobsen Tveit

1. Innledning

Den 8. oktober kom EDPB med et forslag til en ny veileder som analyserer retten til å behandle personopplysninger på bakgrunn av berettigede interesser etter GDPR art. 6 (1) (f).

Artikkelen oppstiller tre kumulative vilkår – for det første må det foreligge en «berettiget interesse» som begrunner behandlingen. Deretter må behandlingen være «nødvendig for formål» knyttet til disse interessene. Avslutningsvis må de berettigede interessene til den behandlingsansvarlige eller tredjeparter veie tyngre enn de registrertes interesser eller grunnleggende rettigheter og friheter etter en interesseavveining.

Veilederen er et førsteutkast, og det gjenstår fortsatt å se hva som blir det endelige resultatet av høringsprosessen. I denne artikkelen vil vi redegjøre for det vi anser som foreløpige nøkkelpunkter å ta med seg ved vurderingen av «berettiget interesse» som rettslig grunnlag, og se til hvordan kriteriet kan anvendes i praksis ved å peke på ulike typetilfeller som er særlig aktuelle for næringsdrivende.

2. Hva er en «berettiget interesse»?

a. En vurdering i tre steg

Veiledningen fremhever at det første steget i vurderingen av om artikkel 6 nr 1. bokstav f kan tjene som rettslig grunnlag, er å fastslå om behandlingen forfølger en «berettiget interesse». EDPB definerer en «interesse» som «a stake or benefit that a controller or third party may have in engaging in a specific processing activity» (s. 7). GPDR angir ingen definisjon av hva som skal til for at en interesse er «berettiget». Veiledningen fremhever at det derimot må foretas en konkret vurdering, hvor det oppstilles tre kumulative vilkår: (i) interessen må være lovlig, ved å ikke stride imot EU-retten eller nasjonal lovgivning, (ii) interessen må være tilstrekkelig presist angitt, ved å være definert på en klar og forståelig måte, og (iii) interessen må være til stede på tidspunktet på behandlingen, ved å ikke være spekulativ eller hypotetisk.

b. Kommersielle interesser kan være berettiget

I veiledningen anerkjenner EDPB, i det minste indirekte, at også en kommersiell interesse kan utgjøre en berettiget interesse. Veiledningen ble utgitt få dager etter at EU-domstolen avsa *Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens* (C-621/22).

> I veiledningen anerkjenner EDPB, i det minste indirekte, at også en kommersiell interesse kan utgjøre en berettiget interesse.

Spørsmålet for domstolen var om et tennisforbund manglet rettslig grunnlag for å dele medlemmers data med sponsorer for markedsføringsformål, fordi en slik kommersiell interesse ikke er lovfestet. Domstolen kom til at det er ingenting i veien for at en kommersiell interesse

kan utgjøre en berettiget interesse, så lenge interessen ikke er direkte lovstridig. Til tross for hvor nært i tid dommen er avsagt veilederens publisering, har ikke dette gått EDPB hus forbi. Tilsynet viser i fotnote 28 til avgjørelsen, og tilslutter seg domstolens syn ved en presisering om at hvorvidt en kommersiell interesse faktisk er berettiget må vurderes konkret i den enkeltes sak.

Selv om dette har vært antakelsen i praksis, har det likevel vært tvil blant enkelte forfattere om rene kommersielle interesser faktisk ville holde som en berettiget interesse for domstolene. Denne avklaringen gir derfor næringsdrivende nyttig støtte for å behandle opplysninger etter artikkel 6(1)(f) når det gjelder det som i den gamle veilederen ble ansett å være mindre «aktverdige interesser», slik som muligheten til å drive markedsføring.

3. Nødvendighet

Dersom man kommer til at det foreligger en «berettiget interesse», avhenger vurderingen av hvorvidt bokstav f kan benyttes som rettslig grunnlag av om behandlingen er «nødvendig» for formål knyttet til de berettigede interessene som forfølges. Veiledningen fremhever at det i denne sammenheng er sentralt å huske på at nødvendighetskriteriet har en selvstendig betydning i EU-retten, og at forordningsteksten skal tolkes i lys av dette. Dette innebærer at dersom den berettigede interessen som forfølges kan oppnås på en måte som er mindre inngripende for den registrerte, vil behandlingen være ulovlig. Særlig prinsippet om dataminimering vil her være viktig, ved at behandlingen av personopplysninger skal begrenses til det som er adekvat, relevant og nødvendig for å oppnå formålet med behandlingen.

4. Interesseavveiningen

Videre må behandlingen ikke utveies av den registrertes interesser eller grunnleggende rettigheter. Det må foretas en avveining av virksomhetens behov for behandlingen mot den den registrertes personvern, hvor den behandlingsansvarlige må identifisere og beskrive de aktuelle rettighetene og interessene som skal ivaretas, behandlingens innvirkning på de registrerte, de registrertes berettigede forventninger til behandlingen og eksistensen av risikoreduserende tiltak. Risikoreduserende tiltak må ikke forveksles med de kravene den behandlingsansvarlige allerede er underlagt for å sikre overholdelse av GDPR, og går altså ut på å utvide de registrertes eksisterende rettigheter. Det understrekes at formålet med å foreta en interesseavveining ikke er å unngå alle personverninngrep, men å unngå *uforholdsmessige* inngrep ved å balansere aktuelle interesser på begge sider mot hverandre.

5. Transparens

Når det kommer til de registrertes rettigheter i forbindelse med behandlingen, fremheves særlig viktigheten av å oppfylle kravene til transparens og informasjon til de registrerte i henhold til artikkel 13, 14 og 15. Dette innebærer at de registrerte på en enkel og tydelig måte skal gis informasjon om behandlingens grunnlag. For eksempel er en generell henvisning til «bekjempelse av svindel» ikke tilstrekkelig. I tillegg bør de registrerte gis informasjon om vurderingene som er gjort i forkant av innhentingen, herunder vurderingen av om det foreligger en berettiget interesse, og av behandlingens nødvendighet og forholdsmessighet. Informasjonen kan gjerne gis lagvis i en personvernerklæring. I alle tilfeller bør den registrerte opplyses om muligheten til å be om slik informasjon.

6. Avklaring rundt praktiske eksempler

Overordnet

Veilederen beskriver en rekke praktiske scenarier der artikkel 6(1)(f) kan utgjøre et relevant behandlingsgrunnlag. Selv om interessene i disse tilfellene kan vurderes som berettigede, kreves det en konkret vurdering i hver enkelt sak basert på de gjennomgåtte vilkårene – behandlingen kan ikke skje automatisk. Denne avklaringen tilfører imidlertid noe nytt, da det tidligere har vært usikkerhet om flere av disse praktiske eksemplene faktisk kunne kvalifisere som berettigede interesser.

Behandling av barns personopplysninger

Når bestemmelsen anvendes for behandling av barns personopplysninger, påpeker EDPB behovet for spesiell beskyttelse, ettersom barn har begrenset forståelse av risikoene de utsettes for. EDPB presiserer at hensynet til barns personvern bør vanligvis gis forrang, særlig ved profilering og markedsføring av tjenester rettet mot barn. Den behandlingsansvarlige må dokumentere at barnets beste har vært et ledende hensyn i vurderingen, og dokumentasjonen bør tilpasses barnets alder og forståelsesnivå.

Svindelforebygging

Svindelforebygging kan også utgjøre en berettiget interesse, og dette omfatte avdekking av svindel. Selv om behandlingsansvarlig kan ha en berettiget interesse i å rapportere svindel til myndighetene, må dette gjøres på en måte som er relevant og nødvendig for å nå formålet, og ellers være i tråd med GDPRs grunnprinsipper.

Behandling som utføres av offentlige myndigheter

Det presiseres at offentlige myndigheter i noen tilfeller også kan bruke artikkel 6 (1) (f) som grunnlag for behandling. Dette er imidlertid kun aktuelt når behandlingen ikke er relatert til utførelsen av deres spesifikke oppgaver eller utøvelsen av deres spesielle rettigheter som offentlige myndigheter, men omhandler andre aktiviteter som lovmessig utføres, der dette er tillatt av det nasjonale rettssystemet.

Direkte markedsføring

EDPB bekrefter også at direkte markedsføring kan være en berettiget interesse. Dette har ikke vært umiddelbart klart, og denne presiseringen er derfor praktisk for annonsører. Selv om fortalen 47 nevner berettiget interesse som et mulig rettslig grunnlag for direkte markedsføringsformål, understreker EDPB at dette ikke er en generell godkjenning. Vurdering av berettiget interesse krever en detaljert vurdering som tar hensyn til markedsføringens art (mer eller mindre inngripende metoder), forholdet til den registrerte (f.eks. er behandlingen mindre inngripende dersom den registrerte har et løpende kundeforhold), og de registrertes forventninger.

I norsk reguleres dette allerede av markedsføringsloven (mfl.) § 15, hvor det fremgår at det er forbudt å sende elektroniske markedsføringshenvendelser til enkeltpersoner uten at de på forhånd har gitt sitt samtykke. Unntaket er hvis det allerede eksisterer et kundeforhold der kundeinformasjonen er samlet inn i forbindelse med et salg. Det vises også til at visse markedsføringsmetoder kan anses som særlig påtrengende fra den registrertes perspektiv, særlig hvis de baseres på omfattende behandling av potensielt ubegrensede data. For eksempel vil balansevurderingen sjelden gi et positivt resultat for påtrengende profilering og sporing, som innebærer å spore individer på tvers av flere nettsteder, enheter eller tjenester.

EDPB minner oss på at den registrerte uansett for alle tilfeller av direkte markedsføring - påtrengende eller ei - har en uberettiget rett til å protestere etter GDPR artikkel 21 (2).

Konsernintern overføring for interne administrative formål

Dersom den behandlingsansvarlige er en del av et konsern, kan konsernselskapene ha en berettiget interesse i å overføre personopplysninger innenfor konsernet for interne administrative formål. Dette kan ifølge EDPB omfatte behandling av kunders eller ansattes personopplysninger for å blant annet forbedre tjenester, lage statistikk over kundeforhold, og for å vurdere om organisatoriske endringer må gjøres for bedre å beholde kundene i fremtiden.

Overføring av personopplysninger til kompetente myndigheter

En viktig presisering EDPB gjør er å bekrefte at virksomheter kan ha en berettiget interesse i å dele personopplysninger med myndigheter i enkelttilfeller eller ved gjentatte kriminelle handlinger eller trusler mot offentlig sikkerhet. I *Meta v. Bundeskartellamt* (C-252/21) vurderte EU-domstolen om Meta kunne samle inn og dele data med politiet for å håndtere kriminelle handlinger, brudd på regler og skadelig atferd. Domstolen konkluderte med at private aktører ikke kan anse dette som en berettiget interesse, da det ikke er knyttet til deres økonomiske mål. EDPB modifiserer dette noe, ved å understreke at private aktører kan bruke berettigede interesser for å rapportere om kriminelle handlinger de tilfeldigvis blir kjent med, men ikke kan samle inn data systematisk for politiformål hvor virksomheten er økonomisk og kommersiell i sin natur. I tillegg kan en behandlingsansvarlig ha en berettiget interesse i å dele data med myndigheter utenfor EU for å unngå sanksjoner, men dette er kontekstavhengig og kan overstyres av den registrertes rettigheter.

7. Avsluttende kommentarer

Veiledningen presiserer hvordan behandlingsansvarlige skal vurdere om behandlingen er lovlig etter artikkel 6 (1) (f). Sentralt står «trestegsvurderingen» som må foretas ved vurderingen av om interessen som forfølges er berettiget. I tillegg understreker veiledningen at berettiget interesse ikke skal benyttes som en «siste utvei» når andre behandlingsgrunnlag er utilgjengelige. Likevel er vurderingen av hva som utgjør en berettiget interesse ofte kompleks. Hva kunden forventer av behandlingen, og om den er overraskende for kunden, kan være vanskelig å forutsi for den behandlingsansvarlige, noe som kan skape usikkerhet både for den behandlingsansvarlige og den registrerte. Det er derfor viktig at behandlingsansvarlige nøye vurderer disse faktorene for å sikre at behandlingen er forutsigbar og rettferdig for den registrerte.

Veiledningen er et førsteutkast og var på høring frem til 20. november. Den er derfor fortsatt åpen for endringer i tråd med eventuelle høringsinnspill som ble sendt inn innen fristen. Likevel antas det at mye av innholdet, spesielt det som bygger på nyere rettspraksis- og utvikling fra EU-domstolen, vil bli videreført etter at høringsarbeidet er avsluttet.

Cecilie Island og Melissa Jakobsen Tveit, advokatfullmektiger. Arbeider i Advokatfirmaet Wiersholms avdeling for teknologi, media, telekom og immaterialrett.

Schjødt

Halvor Manshaus

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

Nasjonalstater og hacking

Dette er et spesielt nummer av Lov & Data, som nå kan markere 40 år. Det er all grunn til å gratulere en publikasjon som har blitt stående som en sentral leverandør av oppdatert informasjon og oppdaterte rettskilder innenfor sitt område. De rettslige spørsmålene som diskuteres her får stadig økende betydning i et samfunn som på alle måter har tatt skrittet inn i den digitale tidsalder.

Anledningen markeres med en litt lengre artikkel enn vanlig, der vi skal se på spennende spørsmål knyttet til jurisdiksjon, personvern, immunitet og mer når hacking skjer på tvers av landegrenser. Gratulerer!

Halvor Manshaus, AI bilde Midjourney.

Hackere og hacking

I takt med at teknologi og kommunikasjon i stadig større grad flettes sammen, åpnes det samtidig for nye sårbarheter og fremgangsmåter for å angripe kritiske IT-systemer. Dette har også betydning for hvordan hacking foregår, og ikke minst hvem som hacker. På norsk introduserte Språkrådet for flere år siden alternativet *datasnok* om den som hacker. Dette norske alternativet spiller særlig på at hackeren snuser rundt i andres saker uten tillatelse.

Dagens hackere er imidlertid en langt mer mangfoldig gruppe, og drives av mer enn bare ren nysgjerrighet og et behov for å teste grenser. Hackere operer ikke bare alene, men danner ofte større fellesskap som ikke bare driver organisert hacking, det utvikles også felles verktøy for å drive med hacking i stor stil. Ved at disse verktøyene gjøres tilgjengelig for andre via ulike kanaler på Internett, åpnes det for at alt fra proffe hackere til såkalte script kids kan laste ned ferdige dataprogrammer som kan brukes til dataangrep og hacking. Tilnavnet

«script kids» spiller på at dette åpner for at personer som ikke selv besitter den nødvendige kunnskapen eller kompetansen til å drive med direkte hacking enkelt kan bruke slike verktøy. Et kjent eksempel er hvordan hackere først sprer ondartet programvare som infiserer tusenvis av datamaskiner rundt på Internett. Senere brukes disse infiserte maskinene i koordinerte angrep som bombarderer nettsider eller andre målskiver med gjentatte henvendelser eller kommandoer, slik at mottakeren ikke er i stand til å motta andre henvendelser eller går fullstendig ned for telling.I veiledningen anerkjenner EDPB, i det minste indirekte, at også en kommersiell interesse kan utgjøre en berettiget interesse.

I takt med utviklingen har vi sett mer avanserte angrep vokse frem, der det brukes kombinasjon av overvåkning og spesialutviklede programmer som er i stand til å lamme store virksomheter. Slike programmer kan være utviklet av hackere, som beskrevet ovenfor, men også av private firmaer som selger dette omtrent som leverandører i våpenindustrien. Jeg har i denne spalten tidligere skrevet om hackere som krever løsepenger for å gjenåpne systemer eller for å hindre spredning av nedlastet konfidensiell informasjon. Hack-for-hire er også blitt et kjent begrep, der hackere tar på seg oppdrag for å finne informasjon eller data som kan brukes til ulike formål av oppdragsgiveren gjennom hacking. Dette er et blitt et økende problem knyttet til industrispionasje og rene sabotasjeaksjoner.

Hackere blir også rekruttert som hel- eller deltidsansatte på lønningslisten til ulike land rundt om i verden. Det er lett å forstå at land som driver med dette ønsker å bygge opp kompetanse innen hacking for å forebygge og hindre angrep mot egne nasjonale interesser. Men dette er ressurser som ikke bare brukes defensivt. I media kan vi nokså regelmessig lese om angrep mot digital infrastruktur der det er klar mistanke om at andre land står bak handlingene. Et av de første store angrepene der det ble klart antydet at det sto en fremmed statsmakt bak, var «Operasjon Aurora» som fant sted i 2009 og 2010. Navnet på operasjonen ble gitt av sikkerhetsselskapet McAfee, som oppdaget navnet på binærfilene som hadde båret frem angrepet.[1] De mente at dette mest sannsynlig var kodenavnet som var blitt brukt av hackerne. Kanskje utgjør dette navnet samtidig en referanse til panserkrysseren Aurora, som kveldstid den 25. oktober 1917 avfyrte skuddet som signaliserte stormingen av vinterpalasset i Petrograd. Selve granaten som ble skutt var en tom hylse uten eksplosiver, men ringvirkningene av dette ene skuddet ble enorme og markerte starten på oktoberrevolusjonen. Kanskje er det i stedet en referanse til en fargefull soloppgang, en aurora, symbolikken peker i alle fall i retning av en begivenhet som er starten på noe større.

Operasjon Aurora er et spesielt tilfelle, det var et av de første store koordinerte angrepene mot private aktører som kom frem i media og ble formidlet til allmenheten. Angrepet sendte ut sjokkbølger i hele IT-verden. Spesielt omfanget, ressursene og koordineringen som lå bak angrepet var oppsiktsvekkende. Det fortalte om stor kompetanse hos hackerne, og en målrettet plan som styrte det hele.

Google var det første og eneste selskapet som gikk åpent ut og delte informasjon om dette omfattende angrepet. Det er ikke vanlig at virksomheter går ut med denne type informasjon, som man ofte ønsker å holde skjult – så fremt dette er mulig. Analysen i ettertid har vist at angrepet ble gjennomført gjennom flere ledd, og at en viktig faktor var en såkalt «zero-day» sårbarhet i Internet Explorer. Begrepet beskriver en situasjon der det foreligger en sårbarhet eller åpning i et program som foreløpig er ukjent.

Google la selv ut en blogpost til omverden i januar 2010 om det som hadde skjedd, og det ble samtidig gjort klart at Google mistenkte Kina for å stå bak.[2] Google har senere laget en serie på YouTube over 6 episoder som blant annet tar for seg denne hendelsen («Hacking Google»). Her beskrives det omfattende arbeidet som ble lagt ned for å kartlegge og stanse angrepet. I innlegget på bloggen tilbake i 2010 fortalte Google selv om omfanget av angrepet:

> *"Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident--albeit a significant one--was something quite different."*

Allerede på dette tidspunktet hadde man grunn til å tro at minst 20 andre store virksomheter var omfattet. Dette tallet er senere blitt oppjustert kraftig, og inkluderer virksomheter innen finans, teknologi, media osv. I tillegg ble det opplyst at angrepet blant annet var rettet mot gmail-kontoer knyttet til kinesiske menneskerettsaktivister. Det ble også avdekket flere andre angrep.

Google avsluttet dette innlegget med å vise til at man nå måtte vurdere Googles satsning i Kina, som da var godt på vei.

> *"These attacks and the surveillance they have uncovered--combined with the attempts over the past year to further limit free speech on the web--have led us to conclude that we should review*

1 Wired, artikkel 14. januar 2020 *https://www.wired.com/2010/01/operation-aurora/*

2 Blogpost fra Google «A new approach to China» 12. Januar 2010 *https://googleblog.blogspot.com/2010/01/new-approach-to-china.html*

the feasibility of our business operations in China. We have decided we are no longer willing to continue censoring our results on Google.cn, and so over the next few weeks we will be discussing with the Chinese government the basis on which we could operate an unfiltered search engine within the law, if at all. We recognize that this may well mean having to shut down Google.cn, and potentially our offices in China."

Konklusjonen ble at Google avviklet satsningen og trakk seg ut av Kina. Google har senere gått tilbake inn i Kina, men med en begrenset tilstedeværelse. Det har aldri blitt bekreftet om det er Kina som står bak. Selve hacker-gruppen som antas å stå bak angrepet er blitt kjent under navnet «Elderwood», et annet ord som har gått igjen i datafiler benyttet i forbindelse med angrepene.[3] Denne gruppen kjennetegnes ved at de har brukt et stort antall slike zero-day sårbarheter som omtalt ovenfor, angivelig flere hundre slike angrep skal ha blitt utført.[4] Dette er en krevende form for hacking, som i tillegg krever spesiell kompetanse. Alle kjente sårbarheter blir normalt fortløpende utbedret ved patching og nye oppdateringer. Det å avdekke stadig nye svakheter i det omfang som Elderwood tilsynelatende har gjort sier i seg selv mye om slagkraften til disse hackerne.

Som flere andre store IT-virksomheter står Google i dag bak en rekke tiltak mot organisert hacking. Selskapet viser blant annet til at krigen i Ukraina er et eksempel på at hacking nå inngår som en naturlig del av arsenalet til nasjonalstatene og brukes i moderne krigføring:

"A lot has changed in our approach since Aurora. And perhaps no example illustrates that shift more clearly than our response to the war in Ukraine.

…

Russia's invasion sparked, not just a military and economic war, but also a cyber war and an information war. In recent months, we have witnessed a growing number of threat actors– state actors and criminal networks–using the war as a lure in phishing and malware campaigns, embarking on espionage, and attempting to sow disinformation."

We launched Project Shield, bringing not just journalists, but vulnerable websites in Ukraine under Google's security umbrella against DDOS attacks. While you can DDOS small sites, it turns out that it's pretty tough to DDOS Google. We disrupted phishing campaigns from Ghostwriter, an actor attributed to Belarus. And we helped the Ukrainian government modernize its cyber infrastructure, helping fortify it against attack."

DDOS er en form for angrep der mottakeren overbelastes med henvendelser fra en rekke ulike avsendere, derav navnet Distributed Denial Of Service attack. Dette ble diskutert kort ovenfor i forbindelse med amatør-hackere omtalt som script kids. Dette er også en angrepsform som kan gjøres langt mer sofistikert, og som raskt kan sette ut et stort antall nettsider og servere som er eksponert gjennom Internett.

Vår moderne verden går altså over i en fase der vi må legge til grunn at ulike nasjonalstater sitter med sine respektive hackere som tester og utfordrer hverandre. De jobber både med forsvar og konsolidering på egen side, men som vi forstår brukes disse også i offensive angrep, spionasje, desinformasjon med mer. Det som gjør denne virksomheten spesielt vanskelig å forfølge er at den som regel utøves innenfor hjemstatens grenser, men rammer mottakeren som kan sitte et helt annet sted på kloden. Det vanskeliggjør ikke bare sporing og etterforskning, men åpner for kompliserte rettslig spørsmål knyttet til jurisdiksjon og det folkerettslige suverenitetsprinsippet. Statsimmunitet er et utslag av dette prinsippet, og innebærer at en konkret stat ikke kan saksøkes for de nasjonale domstoler i en annen stat.

For å illustrere denne problemstillingen skal vi her se nærmere på en ny og viktig avgjørelse fra Storbritannia. Den engelske Court of Appeal avsa 4. oktober 2024 avgjørelse i saken *Shehabi & Anor v Kingdom of Bahrain* (2024 EWCA Civ 1158 (Shehabi)). Dette er den første saken der en engelsk appelldomstol anser hacking utført fra utlandet som en «act in the UK» i lovens forstand. Loven det er snakk om i denne saken var State Immunity Act fra 1978 (SIA).

I Norge følger vi som kjent det dualistiske prinsipp, der det må en særskilt gjennomføringsakt til før en konvensjon kan anvendes direkte i norsk rett. Dette har vi kombinert med presumsjonsprinsippet, som innebærer at norsk lov skal tolkes og forstås slik at den på best mulig vis samsvarer med våre internasjonale forpliktelser. Ved direkte motstrid vil likevel norsk lov måtte gå foran.

Prinsippet om stats- og diplomatisk immunitet er en viktig del av folkeretten, og gir vern mot fremmede staters domstoler og andre maktutøvende myndigheter. På dette området legger norsk rett til grunn en annen tilnærming, der folkeretten ved motstrid med norsk internrett har forrang. Dette omtales gjerne som sektormonisme, der den utenlandske regelen gjøres til norsk rett innenfor et avgrenset område.

Shehabi-saken handlet nettopp om en fremmed stats angivelige bruk av hacking for å overvåke individer som nå var bosatt i England. De to saksøkerne, Dr. Saeed Shehabi og Moosa Mohammed, hevdet

3 *https://www.theverge.com/2012/9/7/3300306/symantec-elderwood-gang-hackers-investigation*

4 *https://www.reuters.com/article/business/hundreds-more-cyber-attacks-linked-to-2009-google-breach-idUSL2E8K7A9E/*

at agenter fra Bahrain tok i bruk programmet FinSpy for å hacke eller infiltrere deres datamaskiner. Programmet skal deretter ha blitt brukt til å overvåke alt som skjedde på de infiserte enhetene. FinSpy er en avansert form for spyware som lar operatøren få kontroll over et målrettet system. I dette tilfellet skal programmet ha blitt brukt til å samle omfattende data og muliggjøre sanntids avlytting og overvåkning.

Ifølge de to saksøkerne ble hackingen utført ved å sende infiserte e-poster, som installerte FinSpy-programvaren på den lokale bærbare datamaskinen da de ble åpnet. Dette ga agentene tilgang til private filer, kommunikasjon og nettleserhistorikk, chat logger, kontaktlister, bilder, databaser og annet materiale. I tillegg kunne de samtidig aktivere mikrofoner og kameraer for å overvåke saksøkernes fysiske omgivelser når de hadde med seg maskinen. Hackingen muliggjorde også sporing av lokasjon og bevegelser ved hjelp av lokasjonsdata, så lenge en infisert bærbar datamaskin var med en av saksøkerne.

Denne muligheten til å overvåke omgivelsene er verdt å merke seg. Bakgrunnen for overvåkningen skal ha vært at begge saksøkerne har vært fremtredende medlemmer av den politiske opposisjonen til Bahrains regime og har markert seg i pro-demokratiske bevegelser. Dr. Saeed Shehabi er journalist og grunnlegger av Al Wefaq, et politisk parti i Bahrain. Shehabi har bodd i Storbritannia siden 1973, hvor han ble innvilget asyl og senere britisk statsborgerskap. Fra sitt eksil i England skal han ha fortsatt sitt engasjement for politisk reform i Bahrain. Moosa Mohammed er også en bahrainsk opposisjonsfigur som har vært involvert i ulike politiske aktiviteter. Etter å ha flyktet fra Bahrain i 2006, ble han innvilget flyktningstatus i England. Han har jobbet for å synliggjøre menneskerettighetsbrudd i Bahrain og har vært en tydelig kritiker av regimet, særlig i forbindelse med Bahrains behandling av politiske dissidenter.

Saksøkerne skal ha blitt klar over hackingen i kjølvannet av at WikiLeaks i august 2014 publiserte dokumenter som omhandlet Bharains bruk av FinSpy-programvaren. En organisasjon med navnet Bahrain Watch identifiserte deretter saksøkerne som en av målene for denne operasjonen.

Staten Bahrain bestred alle anklagene fra saksøkerne. I underinstansen ble det likevel vist til sakkyndigrapporter som etter rettens vurdering sannsynliggjorde et hendelsesforløp i tråd med saksøkernes påstander. I ankeomgangen var dette bevisspørsmålet imidlertid ikke et tema til behandling. Det må understrekes at ankedomstolen altså ikke skulle ta stilling til om Bahrain rent faktisk hadde utført handlingene. Samtlige spørsmål gjaldt altså den prejudisielle vurderingen av immunitetsspørsmålet. Det materielle spørsmålet knyttet til ansvar for selve handlingen vil dermed bli avgjort i den etterfølgende hovedsaken.

Saudi Arabia har for øvrig vært gjennom en lignende sak, som også ble behandlet av den samme dommeren i første instans. Dette endte med et lignende resultat, der nasjonalstaten ble felt. Saudi Arabia anket avgjørelsen, men anken ble avvist grunnet manglende sikkerhet for sakskostnader, slik at spørsmålet om immunitet aldri ble realitetsbehandlet av ankedomstolen. Shehabi-saken er altså første en gang en ankedomstol i Storbritannia ser nærmere på forholdet mellom statlig immunitet og hacking av denne typen.

SIA paragraf 5 sto sentralt i saken, ettersom det er denne bestemmelsen som oppstiller unntaket fra immuniteten som fremmede stater nyter under engelsk rett.

> ***Personal injuries and damage to property.***
> *A State is not immune as respects proceedings in respect of—*
> *(a) death or personal injury; or*
> *(b) damage to or loss of tangible property,*
> *caused by an act or omission in the United Kingdom.*

Saken gjaldt altså tolkning og anvendelse av bestemmelsen på denne konkrete saken.

Ankesaken var avgrenset til tre konkrete spørsmål knyttet opp mot selve hackingen, som alle gjaldt rettslige forutsetninger for å kunne holde Bahrain ansvarlig.

1. Hvorvidt handlingene til Bahrains agenter i det hele tatt utgjorde en handling i Storbritannia etter SIA

   Bahrain anførte at de påberopte handlingene uansett ikke hadde skjedd i Storbritannia, ettersom hacking var utført fra utlandet. Dermed skulle det være Bahrain, og ikke Storbritannia, som hadde jurisdiksjon over saken. For en britisk dommer å avgjøre saken ville dermed utgjøre et brudd suverenitetsprinsippet og den underliggende jurisdiksjonslæren. Bahrain holdt altså fast ved sin immunitet. Domstolen måtte dermed vurdere om fjernmanipulasjonen av datamaskiner i Storbritannia, utført fra utlandet, kunne regnes som en handling som fant sted i Storbritannia.

2. Hvorvidt oppheving av Bahrains immunitet etter SIA var avhengig av at samtlige av de skadevoldende handlinger måtte anses å være utført i Storbritannia

   Bahrain mente også at unntak fra immunitet etter bestemmelsen kun er aktuelt der handlingen «an act» i sin helhet foregår i Storbritannia. Her måtte man anse i det minste deler av handlingen for å være utført i eller fra Bahrain.

3. Hvorvidt psykiske skader utgjør «personskade» etter § 5 i State Immunity Act 1978

Som et siste punkt mente Bahrain at slik psykologisk skade som var anført av saksøkerne, ikke omfattes av SIA § 5 ettersom dette ikke utgjorde «injury» i lovens forstand.

Til det første spørsmålet landet ankedomstolen på at handlingene måtte anses å ha funnet sted i Storbritannia. Dette til tross for at det ble lagt til grunn at agentene ikke på noe tidspunkt hadde vært fysisk til stede i Storbritannia. Retten tar utgangspunkt i lovens ordlyd, gir i avsnitt 34 av avgjørelsen ikke uttrykk for noen tvil rundt dette spørsmålet. Retten slår fast at det ville være oppkonstruert og lite prinsipielt å trekke opp et skille mellom handlingen i utlandet og virkningen i Storbritannia, og fremhever at handlingen griper direkte inn i Storbritannias jurisdiksjonsområde:

> *"In my judgment, as a straightforward use of language, the remote manipulation from abroad of a computer located in the United Kingdom is an act within the United Kingdom. The true position in such a case is that the agents of the foreign state commit acts both in this country and abroad. To distinguish between what happens abroad and what happens here, characterising the former as an act and the latter as merely the effect of the act, is artificial and unprincipled. The reality is that a foreign state which acts in this way is interfering here with the territorial sovereignty of the United Kingdom."*

I den videre analysen viser retten til at rettsanvenderen her må være varsom ved bruken av rettskildene, ettersom spørsmålet om immunitet er et eget rettslig spørsmål med eget kildemateriale i folkeretten og internretten. Rettskilder knyttet opp mot andre jurisdiksjonsspørsmål, som for eksempel utleveringsregler og prosessuelle regler om forkynning i utlandet, kan ikke uten videre legges til grunn i spørsmål om unntak fra immunitet etter SIA § 5. På den annen side viser praksis fra slike saker at hacking fra utlandet mot Storbritannia er blitt vurdert å finne sted i Storbritannia. Dette innebærer etter rettens skjønn at ordlyden i SIA § 5 rent språklig bør omfatte hacking på samme måte.

Retten legger ikke bare vekt på den rent språklige betydningen av SIA § 5 i forhold til hacking, men viser i avsnitt 40 også til det underliggende prinsippet om immunitet som hele loven bygger på. Dersom en fremmed stat utfører ulovlige handlinger innenfor en annen stats jurisdiksjon, er dette i realiteten en krenkelse av suvereniteten under folkeretten. Grunnlaget for immunitet faller da bort:

> *"That is because the hacking by a foreign state of a computer located in this jurisdiction is an interference with the territorial sovereignty of the United Kingdom, as already noted. For this purpose it makes no difference where the agents of the foreign state are located."*

Bahrains advokat i saken påberopte en ny avgjørelse fra den Europeiske Menneskerettsdomstolen (EMD) av 12. september 2023 (EMD sak 64371/16 og 64407/16, her omtalt som *Wieder*-saken) . Denne dommen hadde ikke vært tilgjengelig for underinstansen (se avsnitt 30), slik at dette var en ny anførsel i ankeomgangen. Klagerne i saken var en amerikansk statsborger bosatt i USA og en italiensk statsborger bosatt i Tyskland. Det sentrale spørsmålet til behandling var hvorvidt Storbritannia hadde gjort inngrep i den europeiske menneskerettskonvensjon (EMK) artikkel 8 ved å utføre masse-innsamling av elektronisk kommunikasjon. Det spesielle med dette tilfellet var at ingen av klagerne var bosatt i Storbritannia eller hadde sendt noen kommunikasjonen derfra. Storbritannia anførte at det ikke forelå jurisdiksjon eller ansvar under jurisdiksjonen i et tilfelle der hverken avsender eller mottaker befant seg i Storbritannia. EMD var ikke enig i dette, og skriver i avsnitt 93 i *Wieder*:

> *"Although there are important differences between electronic communications, for the purposes of Article 8 of the Convention, and possessions, for the purposes of Article 1 of Protocol No. 1, it is nevertheless the case that an interference with an individual's possessions occurs where the possession is interfered with, rather than where the owner is located […] Similarly, in the specific context of Article 8, it could not seriously be suggested that the search of a person's home within a Contracting State would fall outside that State's territorial jurisdiction if the person was abroad when the search took place."*

EMD viser også til andre saker som ikke gjelder hacking eller overvåkning, men der det samme prinsippet får anvendelse. Hannover-saken (EMD 59320/00) gjaldt publisering av bilder tatt av prinsesse Caroline av Monaco i ulike dagligdagse situasjoner. Prinsessen vant frem mot tysk presse, ettersom bildene var av privat karakter og det blant annet manglet noen offentlig interesse som kunne underbygge noe beretttiget behov for publisering. EMD viser til at flere elementer i en persons privatliv ikke lar seg skille fra den fysiske personen, for eksempel fysisk integritet. I Hannover-saken hadde EMD likevel lagt til grunn at fotografier tatt i Østerrike og publisert i tyske magasiner i Tyskland og lest av tyske lesere, gjorde inngrep i prinsessens privatliv - selv om hun var bosatt i Frankrike og med offisiell residens i Monaco.

I anvendelsen av disse prinsippene om forholdet mellom skadested og jurisdiksjon på den foreliggende saken uttalte EMD i *Wieder* avsnitt 94:

> *"Turning to the facts of the case at hand, the interception of communications and the subsequent searching,*

examination and use of those communications interferes both with the privacy of the sender and/or recipient, and with the privacy of the communications themselves. Under the section 8(4) regime the interference with the privacy of communications clearly takes place where those communications are intercepted, searched, examined and used and the resulting injury to the privacy rights of the sender and/or recipient will also take place there."

Tilbake til vår sak og den britiske ankedomstolen, så kommer det klart frem at førstvoterende ikke er overrasket over at EMD ikke lot seg overbevise av Storbritannias argumenter i Wieder-saken. Videre understreker retten at saken ikke gir noen støtte til Bahrains argumenter om manglende jurisdiksjon. I stedet fremheves avsnitt 93 fra Wieder-saken som delvis er sitert ovenfor, og konkluderer med å sammenligne hacking med et tradisjonelt innbrudd:

"In modern terms, the hacking of a person's computer is equivalent to burglars breaking in and stealing the contents of their safe."

Det var således klart at handlingen skjedde i Storbritannia i SIA § 5s forstand.

Det neste spørsmålet var da om samtlige deler av handlingen som har forårsaket skaden etter SIA § 5 må skje i Storbritannia. Underinstansen hadde her konkludert med det var tilstrekkelig at «*an* act or omission» forårsaket skaden, altså at det forelå et årsaksforhold mellom *en* handling og skaden. Denne tolkningen innebar at det ikke var nødvendig å se på hele handlingen i et større perspektiv, det vil være tilstrekkelig at det foreligger en handling som gjør skade. En mindre del av et handlingskompleks vil altså kunne være tilstrekkelig til å fjerne immunitet dersom denne anses å være utført i Storbritannia etter SIA § 5. Det har da ingen betydning for spørsmål om immunitet om ytterligere eller andre deler av handlingen i vid forstand er blitt utført i utlandet.

Retten bygger opp om den språklige tolkningen ved å vise til at denne også er i samsvar med rettstilstanden i flere andre land, og også følger av flere konvensjoner – uten at retten angir noen kilder på dette punktet. Fra dette utleder retten et generelt prinsipp om begrensningene på immunitet i avsnitt 55:

"Accordingly, if State A interferes with the territorial sovereignty of State B by doing an act in State B which is liable to cause death or personal injury to persons in State B, it takes the risk that it will be subject to civil proceedings in State B."

Deretter følger en interessant rettskildeanalyse knyttet til et argument fra Bahrain om formålet og historikken bak SIA § 5. Blant annet drøftes et internt notat som ble gjort tilgjengelig for medlemmer i overhuset i det britiske parlamentet i forbindelse med lovsaken knyttet til State Immunity Bill i 1978. Retten påpeker at notatet etter sin art er en svært spinkel rettskilde, og at mye har endret seg siden 1979 knyttet til hacking og jurisdiksjon. Retten viser også til at det underliggende argumentet om formålet med lovgivningen her ikke kun var å videreføre internasjonale konvensjoner, ettersom det ble gjort flere konkrete endringer og tilpasninger som del av det nasjonale lovarbeidet.

I den følgende drøftelsen går retten gjennom et vidt spekter av internasjonale rettskilder, herunder EMD (Al-Adsani, EMD sak 35763/97) Canadas høyesterett, FN-konvensjonen artikkel 12 og amerikansk lovgivning og rettspraksis på dette området. Retten finner imidlertid ikke grunnlag for å avvike fra ordlydsfortolkningen som innledet drøftelsen, og avviser således ankepunkt nummer 2.

Det siste spørsmålet gjaldt hvorvidt klagerne hadde lidt skade som følge av hackingen. I dette tilfellet var det snakk om psykisk skade som følge av å ha oppdaget hackingen og omfanget av personverninngrepet. Bahrain anførte at slik skade ikke var omfattet av SIA § 5 og vilkåret om «personal *injury*».

Saksøkerne hadde lagt frem bevis i form av ekspertrapporter som underbygget påstanden om psykisk skade. Dette bevistemaet var ikke i seg selv påanket til behandling. Som omtalt ovenfor omfattet ikke ankesaken det materielle spørsmålet om Bahrain rent faktisk hadde utført de aktuelle handlingene, herunder selve hackingen med tilhørende overvåking.

Bahrain anerkjente under dette punktet at britisk rett i dag har utviklet en lære som anerkjenner «personal injury», slik at begrepet omfatter både fysisk og psykisk skade. Det ble imidlertid vist til at den aktuelle bestemmelsen i engelsk rett ble introdusert i 1978, og derfor ikke omfattes av senere utvikling av begrepet. Her skjærer retten raskt gjennom og konstaterer i avsnitt 91 at engelsk rett følger et alminnelig dynamisk tolkningsprinsipp under betegnelsen «always speaking»:

"It is a general principle of statutory interpretation that a statute is not frozen in time at the date of its enactment, but should be interpreted taking into account changes that have occurred since its enactment."

Dersom det hadde foreligget en klar og etablert forståelse i internasjonal rett ville dette kunne ha påvirket dette utgangspunktet og låst fast en forståelse av innholdet i *personal injury*. Noen slik praksis finner retten ikke spor av. I stedet viser retten til en sak i overhuset fra 1998, der et spørsmål gjaldt hvorvidt «the Person Act» fra 1861 omfattet psykisk skader. Det ble lagt til grunn at nyere praksis inkluderte psykisk skade, mens den aktuelle loven kom forut for denne utvidelsen – altså et veldig relevant eksempel opp mot vår sak. Lord Steyn førte ordet i saken,

og uttalte om dette (sitert i avsnitt 93 i vår avgjørelse):

> *"Psychiatry was in its infancy in 1861. But the subjective intention of the draftsman is immaterial. The only relevant enquiry is as to the sense of the words in the context in which they are used. Moreover the Act of 1861 is a statute of the "always speaking" type: the statute must be interpreted in the light of the best current scientific appreciation of the link between the body and psychiatric injury."*

Lord Steyn gir også en god oppsummering av historikken bak «always speaking», som det er verdt å lese. For vår sak var det altså klart at utgangspunktet måtte være å legge til grunn en dynamisk tolkning av SIA § 5, som dermed også omfattet psykisk skade. Spørsmålet ble dermed om det var noe grunnlag fra å fravike dette utgangspunktet. I denne analysen ser retten på flere andre saker på området, som likevel ikke rokker på den dynamiske tolkningsmodellen.

Retten viser i tillegg til at saksøkerne uansett hadde påvist at begrepet «personal injury» allerede i 1978 og tidligere ble ansett å omfatte også psykisk skade. En rekke ulike lovbestemmelser som ble introdusert i perioden 1948 til 1980 definerer skadebegrepet slik at dette omfatter psykisk skade. Retten finner det således sannsynliggjort at dette var tilfelle allerede ved introduksjonen av SIA § 5 i 1978, og at lovgivers intensjon må ha vært at psykisk skade omfattes.

Underinstansen gjorde en analyse av flere internasjonale rettskilder, herunder Europakonvensjonen, Europarådets tolkningsuttalelser, den internasjonale spesialrapporten som la grunnlaget for FN-konvensjonen, artikkel 12 fra FN-konvensjonen og rettskilder som behandler denne bestemmelsen. Konklusjonen fra underinstansen, som ankedomstolen tiltrer fullt ut, er at det ikke foreligger holdepunkter for å anse psykisk skade for å falle utenfor skadebegrepet. Retten gjør deretter en selvstendig vurdering av en rekke andre internasjonale rettskilder, slik vi har sett på de andre punktene. I kanadisk rett dukker det opp noen rettsavgjørelser som går i motsatt retning, men retten konkluderer med at disse ikke tar utgangspunkt i internasjonal rett og spørsmålet om begrepets tolkning i spørsmålet om immunitet for nasjonalstater.

Heller ikke det tredje ankegrunnlaget kunne dermed føre frem. Det ble da ikke nødvendig å ta stilling til et siste spørsmål som lå i saken. Saksøkerne hadde fremmet en anførsel om at en avvisning av hovedkravet under henvisning til immunitet, altså at SIA § 5 ikke fjernet immuniteten til Bahrain, ville utgjøre en krenkelse av EMK artikkel 6. Denne bestemmelsen sikrer som kjent retten til rettferdig rettergang.

EMD har i en lang rekke avgjørelser slått fast at artikkel 6 må leses slik at den også gir en like sterk rett til adgang til domstolene – *access to court*. Uten en slik rett ville prinsippet om rettferdig rettergang miste mye av sin funksjon. EMD har vært klare på at artikkel 6 skal være en effektiv og slagkraftig bestemmelse, og har således slått ned på urimelig høye rettsgebyrer, krevd at saken må behandles innen rimelig tid osv.

Saksøkerne hadde anført at avvisning av saken grunnet immunitet kun var akseptabelt dersom avvisningen fullt ut var i samsvar med internasjonal rett og sedvane på dette området.

Retten trengte ikke ta stilling til dette spørsmålet, ettersom konklusjonen allerede var at Bahrain ikke hadde immunitet ettersom vilkårene i SIA § 5 om opphevelse var tilstede. Ettersom en drøftelse med motsatt utfall uansett hadde hensyntatt det internasjonale rettskildebildet, skal det nok mye til for at EMD ville ha opphevet en avgjørelse med motsatt resultat. Dette forutsatt at den nasjonale domstolen hadde hensyntatt artikkel 6 i sin vurdering, og samtidig foretatt en proporsjonalitetsvurdering mellom prinsippet om immunitet og saksøkernes behov for å prøve sin sak. Anførselen er likevel interessant, og den har en klar virkning ved at domstolen anspores til å gjøre en grundig drøftelse av det internasjonale rettskildebildet.

I en artikkel av undertegnede i *Lov & Data nr 158* (2/2024 side 36) ble det vist til hvordan EMD i saken Podchasov v Russland (EMD sak 33393/19) i avsnitt 50 og utover slår fast at alene det å kreve lagring av data som knytter seg til en enkeltpersons privatliv, utgjør et inngrep etter EMK artikkel 8, her sitert fra avsnitt 51:

> *"As regards the storage by ICOs of Internet communications and related communications data, the Court reiterates that the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding. However, in determining whether the personal information retained by the authorities involves any of the various private-life aspects, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained"*

Dette gjelder uavhengig av en eventuell etterfølgende bruk av den innsamlede informasjonen, likevel slik at blant annet konteksten for overvåkningen og hva slags data som hentes ut har betydning for vurderingen. I Podchasov-saken var det spørsmål om et påbud om utlevering av data, ikke hacking. Spørsmålet som ble drøftet var også et annet spørsmål enn hvorvidt psykisk skade omfattes av en nasjonal lovbestemmelse. Samtidig ser vi at konvensjonskravet om *access to court* inneholder en forventning om at sterke konvensjonskrenkelser medfører en sterkere prøvingsintensitet

Halvor Manshaus, AI bilde Midjourney.

fra EMD. I dette ligger at den nasjonale *margin of appreciation*, altså det slingringsmonn som den enkelte medlemsstat har sin i tolkning og anvendelse av konvensjonen i den konkrete saken, kan reduseres betraktelig. For den nasjonale domstolen innebærer dette et skjerpet krav til å følge den metodikk og de vurderingstema som EMD har foreskrevet gjennom sin praksis. Dette er nødvendig for at EMD senere skal kunne vurdere saken i en eventuell klagesak. Dersom det ikke er gjort en konkret internrettslig vurdering av om et inngrep er *necessary in a democratic society*, i praksis formulert av EMD som et krav om at det foreligger en *pressing social need*, så vil dette kunne tale for at den internretteslige proporsjonalitetsvurdering ikke holder mål. Da ser vi også at den subsidiære anførsel knyttet til artikkel 6 omtalt ovenfor antakeligvis vil stå sterkere.

Dommen er enstemmig, men med en tilleggskommentar fra Lord Justice Warby. Han påpeker først det paradoksale i at agentene som hacker og overvåker for sin del ønsker å holde dette skjult. Det er først når dette ikke slår til og at det hele blir kjent at det forårsakes skade på saksøkerne. Den skadevoldende handling skjer altså i strid med skadevolderens plan og ønsker.

Det andre synspunktet er knyttet til det første spørsmålet i saken, der han gir uttrykk for at Bahrains anførsel virker kunstig og oppkonstruert. Han viser til et spørsmål under forhandlingene, der Bahrains prosessfullmektig ga et konkret eksempel:

> *"He submitted that when a person uses a pen to create a manuscript document the marks on the page are not part of the act of writing but only the effect of that act."*

Lord Justice Warby var tydeligvis ikke imponert over svaret. Denne kommentaren viser for øvrig hvordan et uheldig eksempel kan virke

mot sin hensikt, og fremhever svakheten i en argumentasjonsrekke.

Jeg har brukt en del plass i denne artikkelen på å gå gjennom argumentasjon og rettskildebruk i denne saken. Avgjørelsen er svært godt egnet til å fremvise det internasjonale rettskildebildet og de særskilte spørsmål rundt jurisdiksjon som fort blir aktuelle når hacking skjer på tvers av landegrenser, og desto mer når det er nasjonalstater som angivelig står bak. Hvorvidt Bahrain har utført hackingen i denne saken er altså ikke avgjørende, og rettens vurderinger av samtlige tre spørsmål står ved lag uansett utfall i hovedsaken.

Når hackere opererer under statlig kontroll, minner dette mye om seiltidens kaperpirater. Det skjer en slags legitimering av en virksomhet som ellers er sterkt uønsket og forårsaker stor skade. I 1243 utstedte England det første kjente kaperkommisjon, en slags «*license to pirate*» som tillot private fartøy å angripe, borde, ransake og beslaglegge skip fra fiendtlige stater. Et privat fartøy ble umiddelbart gjort om til en militær ressurs, og fikk samtidig et økonomisk insentiv til aktivt å oppsøke fiendtlige skip. Selv nøytrale skip kunne anholdes, og lasten beslaglegges, dersom det var snakk om våpen og annet krigskontrabande. Kapere skulle i prinsippet ikke straffes som sjørøvere dersom de ble tatt til fange av fienden, de nøt en slags strafferettslig immunitet som legitime utøvere av statsmakt. I stedet for å innlede direkte krig med hverandre, er det eksempler på at skipsmaktene i stedet engasjerte hverandre i begrensede trefninger mellom kapere. Senere vokste det frem konvensjoner og internasjonale regler som i større grad formaliserte kaperrollen. Den amerikanske grunnloven fra 1787 bemyndiget kongressen til å utstede slike kaperbrev, slik det fremgår av Article 1 Legislative Branch – Section 8 Enumerated Powers – Clause 11 War Powers:

> *"To declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water…"*

I Norge kjenner vi kaperbrev både fra den store nordiske krigen (1700–1721), og krigen med Storbritannia (1807–1814).

Proceedings er et tidsskrift fra US Naval Institute. Instituttet er en privat organisasjon som har gitt ut Proceedings helt tilbake til 1874. I en kronikk publisert i oktober 2019 diskuteres the Active Cyber Defence Certainty Act[5], som i praksis ville gi private virksomheter kaperbrev. Ikke bare for rene defensive tiltak, men også mer aktiv og oppsøkende virksomhet.[6] Forfatteren beskriver et tenkt angrep mot en bank på Wall Street, som engasjerer et sikkerhetsfirma for bistand. Dette firmaet har et fått et moderne kaperbrev som tillater motangrep rettet mot hackerne. Brevet er nødvendig, ettersom slike angrep normalt ikke er tillatt ettersom dette i seg selv utgjør ulovlig hacking. Forfatteren ser for seg prosessen videre slik:

> *"If defensive measures fail and the bank is hacked, the cyber security firm would invoke its standing Cyber Letter of Marque to conduct a hack back operation against the aggressor. The goals of the hack back would be first to stop the attacker's ongoing exploits and then degrade the attacker's infrastructure. This degradation would impose a cost, to dissuade the attacker from further malicious activity. The information gleaned from the hack back operation would be reported to the Department of Homeland Security to support public-private data sharing to improve the U.S. cyber security posture."*

De rettslige spørsmålene som diskuteres her ligger i et bredt spenn mellom blant annet personvern, ytringsfrihet, datakriminalitet og folkerettens suverenitetsprinsipp.

Som vi allerede kan utlede fra Shehabi-saken som er omtalt ovenfor, vil et slikt kaperbrev innebære en rekke vanskelige avgrensninger, men debatten og lovforslaget er illustrerende for tiden vi lever i.

De rettslige spørsmålene som diskuteres her ligger i et bredt spenn mellom blant annet personvern, ytringsfrihet, datakriminalitet og folkerettens suverenitetsprinsipp. Dette er store og viktige prinsipper, samtidig som de berørte vil kunne være private virksomheter eller enkeltpersoner som i liten grad kan verne seg mot denne typen handlinger. Det blir spennende å følge rettsutviklingen på dette området, og ikke minst det endelige utfallet av denne konkrete saken.

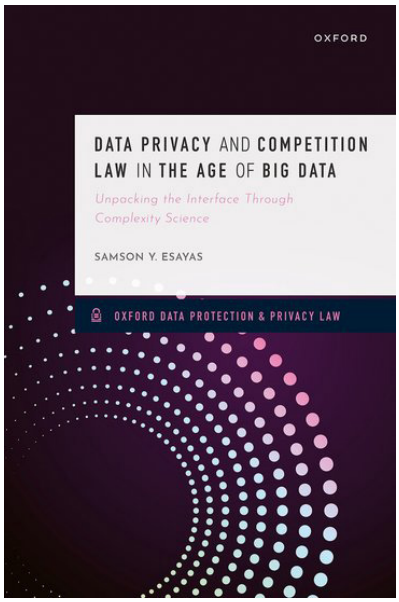
---

5 https://www.congress.gov/bill/116th-congress/house-bill/3270/text

6 https://www.usni.org/magazines/proceedings/2019/october/grant-cyber-letters-marque-manage-hack-backs

Data Privacy and Competition Law in the Age of Big Data

Unpacking the Interface Through Complexity Science



Samson Y. Esayas, Associate Professor of Law, BI Norwegian Business School

Description:

The monetization of personal data has become an increasingly common business practice, igniting global debate on the interface between data privacy law and competition law. Data Privacy and Competition Law in the Age of Big Data provides a comprehensive, novel, and interdisciplinary analysis of this nexus. Drawing insights from emergent properties and complexity science, the book exposes the commonalities and conflicts between how data privacy law and competition law address challenges resulting from the commercialization of personal data.

Samson Y. Esayas begins by identifying key shifts in big data: the growing trend of processing personal data for diverse purposes, the aggregation of data across various operations, and the shift from offering stand-alone products and services to ecosystems of several, with personal data central in connecting the different markets. These shifts engender a complex economic landscape, marked by multiple actors, a web of interactions, and non-linear, emergent outcomes. Despite this complexity, the prevailing approach to data privacy law and competition law emphasises isolated units of analysis-whether a relevant market or a distinct processing operation. This approach overlooks system-wide (emergent) risks borne of cumulative processing operations and cross-market practices. Additionally, a mindset focused on either data privacy law or competition law overlooks the increasing intersection between the two regimes, missing opportunities for synergy.

In light of these challenges, Esayas's volume calls for recalibrating data privacy law and competition law for a complex economy, emphasizing a holistic, systems-level perspective that addresses emergent harms and a polycentric strategy that leverages the strengths of each legal regime.

Overview:

- Provides a comprehensive analysis of the interface between data privacy law and competition law in addressing challenges arising from the commercialization of data
- Uses emergent properties and complexity science to deepen our understanding of the intersection between the two legal regimes
- Offers concrete policy proposals to address the challenges of big data
- Presents a detailed assessment of the role of privacy as a non-price competition parameter, including privacy issues under EU merger control, rules on anti-competitive collaboration, and abuse of dominance

Oxford Data Protection & Privacy Law

The book description is from Oxford University Press: https://global.oup.com/academic/product/data-privacy-and-competition-law-in-the-age-of-big-data-9780198891420?cc=no&lang=en&

Algoritmer, kunstig intelligens og diskriminering

En analyse av likestillings- og diskrimineringslovens muligheter og begrensninger

Vibeke Blaker Strand, professor ved Institutt for offentlig rett, Universitet i Oslo

Utredning skrevet på oppdrag fra Likestillings- og diskrimineringsombudet Levert 21. mars 2024

Rapporten som pdf: *https://ldo.no/content/uploads/2024/06/Algoritmer-kunstig-intelligens-og-diskriminering-2024.pdf*

ISBN 978-82-8320-032-4 (trykt utgave) 978-82-8320-033-1 (elektronisk utgave)

XL Nordic Conference on Law and IT – Regulating for Complexity

Join us for the 40th Nordic Conference on Law and IT, marking an incredible milestone in advancing legal scholarship and practice in the Nordic region.

XL Nordic Conference on Law and IT - Regulating for Complexity - Institutt for privatrett

UNIVERSITETET I OSLO

XL Nordic Conference on Law and IT - Regulating for Complexity - Institutt for privatrett

Join us for the 40th Nordic Conference on Law and IT, marking an incredible milestone in advancing legal scholarship and practice in the Nordic region.

www.jus.uio.no

Gizmodo

Founded in 2002 as one of the internet's very first tech news blogs, Gizmodo is dedicated to fiercely independent reporting and commentary on technology, science, and internet culture. The future is here.

GIZMODO

The Future Is Here

Delphi

Rebecka Undén, associate, Advokafirman Delphi

Regulatorisk sandlåda, föreskrifter om lagöverträdelser ny rättslig grund för kamerabevakning

Ytterligare tillståndskrav och regellättnader vad gäller kamerabevakning föreslås i av regeringen. Tidigare i år presenterades utredningen SOU 2024:27 Kamerabevakning i offentlig verksamhet. Utredningen föreslog bland annat att kamerabevakningslagens tillståndskrav för offentliga aktörer helt ska avskaffas. Regeringen bedömer att den personliga integriteten skyddas i tillräcklig utsträckning genom den generella dataskyddsregleringen.

För brottsbekämpande verksamheter föreslår utredningen dock att en särskild intresseavvägning ska tillämpas. Utredningens förslag öppnar upp för kamerabevakning på fler platser än idag. Det gäller platser där det med hänsyn till faktiska omständigheter finns risk för allvarlig eller omfattande brottslighet, eller platser som med hänsyn till faktiska omständigheter har strategisk betydelse för att motverka allvarlig brottslighet.

IMY har i ett yttrande kommenterat utredningen och framhållit riskerna med att avskaffa tillståndskravet i kamerabevakningslagen. Även om tillståndskravet tas bort måste varje enskild offentlig aktör själv bedöma om kamerabevakningen är tillåten, vilket enligt IMY innebär en större administrativ börda för aktörerna. IMY pekar särskilt på risken för mer otillåten kamerabevakning i samhället. Enligt IMY är det viktigt att tydliggöra att ett avskaffande av tillståndskravet inte innebär att bevakning blir tillåten i fler situationer än idag i offentliga verksamheter som inte är brottsbekämpande.

Parallellt med nämnda utredning har ytterligare en utredning löpt i ett så kallat ”snabbspår”. Regeringen beslutade i december förra året att tillsätta en utredning för att ge polisen och säkerhetspolisen större möjligheter att använda kameraövervakning med automatisk igenkänning av fordons registreringsnummer respektive med automatisk ansiktsigenkänning. Utredningen skulle också lämna förslag på hur polisen och säkerhetspolisen i fler fall kan ta del av kamerabevakningsmaterial från annans bevakning.

Justitiedepartementet presenterade den 3 juni betänkandet ”Förbättrade möjligheter för polisen att använda kamerabevakning”. Utredningen föreslår att polisen under vissa förutsättningar ska kunna använda kamerabevakning på allmänna trafikplatser utan att först dokumentera en intresseavvägning. Polisen ska också kunna använda sig av biometrisk fjärridentifiering i realtid på allmän plats, dock enbart efter myndighetstillstånd.

Därtill införs en ny rättslig grund i lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Den nya rättsliga grunden tar sikte på vidareanvändning av personuppgifter som samlats in genom kamerabevakning. Såväl privata som offentliga aktörer ska kunna dela uppgifter från kamerabevakning efter begäran från polisen eller säkerhetspolisen, utan att behöva beakta finalitetsprincipen som innebär att personuppgifter inte får behandlas på ett sätt som är oförenligt med det ursprungliga ändamålet för vilket de samlats in. Det gäller under förutsättning att syftet är att utreda brottslighet för vilket fängelse är föreskrivet.

Den rättsliga grunden föreslås träda i kraft den 1 januari 2025. Ett stort antal remissinstanser är dock kritiska till förslaget - dels ur integritetssynpunkt, dels för att det finns risk att förslaget inte kommer att uppfylla sitt syfte. I skrivande stund återstår att se hur regeringen väljer att gå vidare med utredningen.

Rebecka Undén, associate, Advokafirman Delphi.

Gorrissen Federspiel

Tue Goldschmieding

Datatilsynet indleder undersøgelse af Rejsekort-appen

Det danske Datatilsyn (»Datatilsynet«) besluttede den 2. juli 2024 at indlede en undersøgelse af Rejsekort-appen efter at have stillet en række overordnede spørgsmål til Rejsekort & Rejseplan A/S (»Rejseplan«) i løbet af foråret.

Spørgsmålene vedrørte appens funktionalitet og de personoplysninger, herunder lokationsdata, som indsamles gennem appen. Formålet med disse spørgsmål var at vurdere, om der var grundlag for en mere dybdegående undersøgelse af appen og den behandling af personoplysninger, som finder sted i appen; navnlig, om dette er i overensstemmelse med de databeskyttelsesretlige principper i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 5, stk. 2, litra a og c, om lovlig, gennemsigtig, rimelig og dataminimeret behandling af personoplysninger.

På baggrund af de modtagne svar og sagens karakter har Datatilsynet nu besluttet at gå videre med en nærmere undersøgelse, og har i forbindelse hermed bedt Rejsekort om en redegørelse. Det er værd at bemærke, at Datatilsynet på nuværende tidspunkt ikke har forholdt sig til andre trafikselskabers egenudviklede apps og den behandling af persondata, som finder sted ved anvendelsen af sådanne.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/jul/datatilsynet-indleder-undersoegelse-af-rejsekort-appen

Ny praksis for indsigt i logfiler

Den 22. juni 2023 tog EU-Domstolen i sag C-579/21 (Pankki S) stilling til spørgsmålet om retten til indsigt i logfiler. En »log« er en fil, hvori et it-system gemmer oplysninger om dets drift og brug, og kan efter omstændighederne indeholde personoplysninger, herunder oplysninger om, hvornår der er foretaget opslag på en given persons oplysninger og af hvem.

Dommen har medført en ændring af det danske Datatilsyn (»Datatilsynet«) praksis. Tidligere var personoplysninger i en log ikke omfattet af retten til indsigt efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 15, da Datatilsynet betragtede loggen som en systemmæssig sikkerhedsfacilitet uden selvstændig behandling af (person-)oplysninger.

EU-Domstolen fastslog dog, at GDPR artikel 15, stk. 1, skal fortolkes således, at information vedrørende søgninger i en persons personoplysninger og datoerne for og formålet med disse søgninger udgør information, som den berørte person har ret til at få fra den dataansvarlige. Dog giver bestemmelsen ikke ret til information om identiteten på den dataansvarliges ansatte, som har foretaget søgningerne, medmindre denne information er nødvendig for, at den registrerede effektivt kan udøve sine rettigheder, og under forudsætning af at de ansattes rettigheder og frihedsrettigheder kan iagttages.

Den nye praksis indebærer, at dataansvarlige skal udlevere en kopi af de personoplysninger om en registreret, som er registreret i loggen, herunder oplysninger om søgninger i vedkommendes oplysninger og datoerne for og formålet med disse søgninger. Hvis denne information er nødvendig for, at den registrerede kan udøve sine rettigheder, skal man desuden oplyse, hvem der har foretaget søgningen, medmindre det krænker sidstnævntes rettigheder.

Denne nye praksis er nu inkorporeret og tilkendegivet af Datatilsynet og vil fremadrettet udgøre grundlaget for Datatilsynets tilgang til indsigt i logfiler.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/jul/hvad-gaelder-for-indsigt-i-logfiler

Opdateret vejledning om håndtering af brud på persondatasikkerheden

Det danske Datatilsyn (»Datatilsynet«) har den 4. juli 2024 opdateret sin vejledning om håndtering af brud på persondatasikkerheden, hvorefter den er udvidet til at indeholde flere konkrete eksempler. Denne opdatering udgør en del af Datatilsynets løbende arbejde med at sikre, at dataansvarlige har de nødvendige redskaber til at håndtere brud på persondatasikkerheden korrekt.

De nye eksempler i vejledningen illustrerer de overordnede principper, der også var en del af den tidligere version, men med fornyet udgangspunkt i den praksis, der løbende er kommet på området. Indtil videre er det kun de første dele af vejledningen, der er blevet opdateret, men Datatilsynet forventer at udvide vejledningen yderligere i løbet af det fortløbende kvartal i efterår og vinter 2024.

Det bør fremhæves, at den gamle vejledning fortsat er gældende, indtil de nye opdateringer er fuldt implementeret.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/jul/opdateret-vejledning-om-haandtering-af-brud

Læs Datatilsynets opdaterede vejledning her: https://www.datatilsynet.dk/Media/637886298435856391/H%C3%A5ndtering%20af%20brud%20p%C3%A5%20persondatasikkerheden.pdf

Kommunerne efterlever Datatilsynets påbud i Chromebook-sagen

Den 10. juli 2024 konkluderede det danske Datatilsyn (»Datatilsynet«), at de af Chromebook-sagen omfattede kommuner nu efterlever det påbud, de fik udstedt tilbage i januar 2024 som del af Chromebook-sagskomplekset. Datatilsynet finder navnlig, at kommunerne ikke længere videregiver personoplysninger til uhjemlede formål.

KL meddelte på vegne af de 52 omfattede kommuner, at kommunerne fra 1. august 2024 ville ophøre med at videregive personoplysninger til Googles egne formål, som Datatilsynet i sin delafgørelse fra januar 2024 fandt uhjemlede. Datatilsynet noterer sig, at kontrakten er tilpasset, så personoplysninger nu kun behandles i overensstemmelse med den dataansvarlige kommunes instrukser med undtagelse af de tilfælde, hvor det er krævet i henhold til EU-regler eller en EU-medlemsstats nationale ret. Tilsynet påpeger dog samtidig, at der fortsat er en række udeståender i sagen.

Datatilsynet har anmodet Det Europæiske Databeskyttelsesråd om en udtalelse om bl.a. rækkevidden af den dataansvarliges dokumentationsforpligtelse for databehandlerens brug af underdatabehandlere. Når udtalelsen er modtaget, agter Datatilsynet at foretage en endelig vurdering af underdatabehandlerkæden vedrørende kommunernes anvendelse af Googles produkter.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/jul/chromebook-sagen-kommunerne-efterlever-datatilsynets-seneste-paabud-

Natklub får alvorlig kritik for håndtering af tv-overvågningsoptagelser

Den 24. juni 2024 udtalte det danske Datatilsyn (»Datatilsynet«) alvorlig kritik af Clemens Bar ApS (»Clemens Bar«) for deres håndtering af en anmodning om indsigt i tv-overvågningsoptagelser (journalnummer 2023-31-0053).

En borger klagede til Datatilsynet over, at Clemens Bar afviste at give indsigt i tv-overvågningsoptagelser, hvori borgeren fremgik. Clemens Bar begrundede afslaget med, at indsigt i optagelserne kunne kompromittere sikkerheden på natklubben og formindske den kriminalitetsbekæmpende effekt, som var formålet med tv-overvågningen. Endvidere ville det ikke være muligt at sløre de øvrige personer på optagelserne, for at undgå krænkelse af disses rettigheder, uden også at sløre klageren grundet det store antal personer, der fremgik af optagelserne.

Clemens Bar havde gemt de relevante tv-overvågningsoptagelser, men på grund af en menneskelig fejl blev optagelserne slettet, før tilsynet havde færdigbehandlet sagen.

Datatilsynet fandt, at Clemens Bar ikke kunne afvise anmodningen med henvisning til offentlige interesser, da vurderingen ikke var funderet i en erklæring fra politiet eller lignende, men derimod udelukkende var baseret på Clemens Bars egen vurdering. Dog fandt Datatilsynet, at der ikke var tilstrækkeligt grundlag for at tilsidesætte Clemens Bars vurdering af, at udlevering af optagelserne kunne krænke andres rettigheder og frihedsrettigheder, da der var ca. 150 personer på optagelserne.

Datatilsynet havde dog i lyset af den utilsigtede sletning af videomaterialet ikke mulighed for at efterprøve dette led af Clemens Bars argumentation. På den baggrund havde Clemens Bar fejlet i at håndtere klagers anmodning i overensstemmelse med princippet om lovlighed, rimelighed og gennemsigtighed efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 5, stk. 1, litra a.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/jul/natklub-faar-alvorlig-kritik-manglende-indsigt-i-og-sletning-af-tv-overvaagnings-optagelser

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jun/natklub-faar-alvorlig-kritik-manglende-indsigt-i-og-sletning-af-tv-overvaagningsoptagelser

Digitaliseringsstyrelsen ændrer kørekort-appen efter alvorlig kritik

Det danske Datatilsyn (»Datatilsynet«) afsluttede den 11. juli 2024 en sag mod den danske Digitaliseringsstyrelse (»Digitaliseringsstyrelsen«), efter at styrelsen havde ændret det digitale kørekort for at efterleve Datatilsynets forbud, og dermed overholde dataminimeringsprincippet. Sagen blev behandlet under journalnummer 2023-432-0011.

Sagen tog sit udgangspunkt i Datatilsynets brev af 8. november 2023, hvor tilsynet udtalte alvorlig kritik af Digitaliseringsstyrelsen for at behandle personoplysninger fra det danske kørekortregister om personer, som ikke selv havde tilmeldt sig muligheden for det digitale kørekort, og gav i denne forbindelse styrelsen forbud mod at behandle sådanne personoplysninger. Datatilsynet fandt, at denne behandling var i strid med dataminimeringsprincippet i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 5, stk. 1, litra c, hvorefter kun de for databehandlingen nødvendige oplysninger må behandles.

Digitaliseringsstyrelsen har nu ændret kørekort-appen, så styrelsen alene modtager oplysninger fra kørekortregisteret om de personer, der faktisk har tilmeldt sig det digitale kørekort. Datatilsynet har på den baggrund endeligt afsluttet sagen.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/jul/digitaliseringsstyrelsen-har-aendret-koerekort-appen

Læs Datatilsynets afsluttende brev her: https://www.datatilsynet.dk/Media/638562963202773201/K%C3%B8rekort-app.pdf

Udlændinge- og Integrationsministeriet får kritik for manglende kontrol med visuminformationssystemet

Det danske Datatilsyn (»Datatilsynet«) udtalte den 10. juli 2024 kritik af det danske Udlændinge- og Integrationsministerium (»Udlændige- og Integrationsministeriet«) for manglende kontrol med egne slettefrister i det nationale visuminformationssystem (VIS) og for ikke straks at slette oplysninger om visumansøgere, der opnår statsborgerskab i en EU-medlemsstat. Sagen blev behandlet under journalnummer 2023-421-0015.

Under et tilsyn hos Udlændinge – og Integrationsministeriet konstaterede Datatilsynet, at ministeriet ikke førte kontrol med, om deres automatiske sletteprakis i visuminformationssystemet fungerede korrekt. Datatilsynet vurderede, at den manglende løbende kontrol med denne sletteprakis var i strid med kravet om ansvarlighed og opbevaringsbegrænsning i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 5, stk. 2, og artikel 5, stk. 1, litra e.

Desuden konstaterede Datatilsynet, at ministeriet ikke straks slettede oplysninger om visumansøgere, der opnåede statsborgerskab i en EU-medlemsstat inden udløbet af en 5-årig periode, som påkrævet af Europa-Parlamentets og Rådets Forordning (EF) 767/2008 af 9. juli 2008 om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold (»VIS-forordningen«). I stedet blev ansøgerne vejledt til selv at kontakte Udlændingestyrelsen for at få deres oplysninger slettet. Datatilsynet vurderede, at denne fremgangsmåde ikke opfyldte VIS-forordningens krav om sletning før tid, jf. forordningens artikel 25. På denne baggrund udtalte Datatilsynet kritik af Udlændinge- og Integrationsministeriet.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/jul/udlaendinge-og-integrationsministeriet-faar-kritik-i-tilsynssag-vedroerende-visuminformationssystemet

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jul/udlaendinge-og-integrationsministeriet-faar-kritik-i-tilsynssag-vedroerende-visuminformationssystemet

Familieretshuset møder alvorlig kritik igen

Det danske Datatilsyn (»Datatilsynet«) udtalte den 2. juli 2024 endnu engang alvorlig kritik af det danske Familieretshus (»Familieretshuset«) for manglende behandlingssikkerhed resulterende i utilsigtet videregivelse af beskyttede oplysninger og oplysning om ophold på krisecentre. Sagen blev behandlet under journalnummer 2023-432-0003.

I perioden fra 6. januar 2023 til 30. juni 2024 anmeldte Familieretshuset 28 nye brud på persondatasikkerheden til Datatilsynet. Disse brud bestod i Familieretshusets uberettigede videregivelse af oplysninger om beskyttede navne og adresser eller andre oplysninger – potentielt egnet til at afsløre en persons opholdssted. Oplysningerne blev i de fleste tilfælde videregivet til den anden part i sagen, som oftest kunne være årsagen til valget om navne- og adressebeskyttelse eller ophold på et krisecenter. Den utilsigtede videregivelse skyldtes menneskelige fejl forårsaget af medarbejderes manglende opmærksomhed.

Datatilsynet har tidligere udtalt alvorlig kritik i lignende sager og påbudt Familieretshuset at foretage risikovurderinger og etablere sikkerhedsforanstaltninger. Familieretshuset arbejder fortsat på at styrke og implementere nye foranstaltninger for at mindske risikoen for lignende brud. Datatilsynet anerkendte disse bestræbelser, men fandt, at Familieretshuset fortsat ikke havde implementeret tilstrækkelige sikkerhedsforanstaltninger eller sikret, at de eksisterende foranstaltninger havde haft den ønskede effekt. Derfor udtalte Datatilsynet igen alvorlig kritik af Familieretshusets manglende overholdelse af Europa-Parlamen-

tets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 32, stk. 1, om passende behandlingssikkerhed.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/aug/familieretshuset-faar-igen-alvorlig-kritik

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jul/familieretshuset-faar-igen-alvorlig-kritik

Vejen Kommune indstillet til bøde for manglende kryptering

Det danske Datatilsyn (»Datatilsynet«) politianmeldte den 14. August 2024 Vejen Kommune for utilstrækkelige sikkerhedsforanstaltninger og indstillede i denne forbindelse til en bøde på 200.000 kroner.

Datatilsynets behandling af sagen tog sit udspring, da Vejen Kommune anmeldte et brud på persondatasikkerheden efter et tyveri af fem bærbare skolecomputere i kommunen. Disse computere indeholdt oplysninger om børn og var ikke krypterede. Datatilsynets efterfølgende undersøgelse af sagen afslørede, at op mod 300 andre computere i kommunen tilsvarende manglede kryptering.

Datatilsynet har tidligere advaret kommuner om vigtigheden af kryptering og har indstillet til bøder i lignende sager. Kryptering er ifølge Datatilsynet en basal sikkerhedsforanstaltning, som er relativt nem og ikke videre omkostningsfuld at implementere. Ud fra den betragtning bør kryptering ifølge Datatilsynet derfor som udgangspunkt også forudsættes inkorporeret i IT-sikkerheden. Datatilsynet opfordrer således kommunerne til at gennemgå deres bærbare enheder grundigt og sikre, at krypteringen er på plads.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/aug/endnu-en-kommune-indstillet-til-boede-for-manglende-kryptering

Fitnesscenters brug af ansigtsgenkendelse godkendt som gyldigt samtykke

Det danske Datatilsyn (»Datatilsynet«) har under journalnummer 2023-31-0028 den 3. juli 2024 truffet afgørelse i en sag om et fitnesscenters brug af ansigtsgenkendelse, herunder om fitnesscenterets andre adgangsmuligheder kunne udgøre tilstrækkelige alternativer. Datatilsynet vurderede, at et samtykke hos den registrerede som behandlingsgrundlag for denne praksis var gyldigt, såfremt det var informeret og korrekt indhentet.

Datatilsynet modtog en klage fra en borger over, at fitnesscentret Sporting Health Club (»SHC«) havde indført ansigtsgenkendelse som adgangskontrol. Klageren påpegede, at der ikke var tilstrækkelige alternativer til ansigtsgenkendelse. Det blev i sagen oplyst, at brugere af fitnesscentret, der ikke ønsker at give samtykke til ansigtsgenkendelse, kan blive lukket ind af receptionen i åbningstiden. Uden for de bemandede åbningstider kan brugerne kontakte døgnsupporten, som enten kan fjernåbne døren eller generere en adgangskode.

Datatilsynet har tidligere vurderet i en anden sag, at brugen af ansigtsgenkendelse som adgangskontrol til fitnesscentre ikke i sig selv overtræder Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 5 og proportionalitetsprincippet. Nærværende sag rejste derfor primært spørgsmål om samtykkekravene og muligheden for, at de eksisterende alternativer kunne betragtes som reelle.

Datatilsynet fandt, at SHC kunne indhente et gyldigt samtykke, der kunne udgøre en undtagelse til forbuddet mod behandling af særlige kategorier af oplysninger, såfremt samtykket var informeret og korrekt indhentet. Dog udtalte Datatilsynet kritik af det samtykke, som SHC konkret havde forsøgt at indhente fra klageren, da klageren var blevet oplyst om, at der ikke var alternativer til ansigtsgenkendelse.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/aug/samtykke-til-ansigtsgenkendelse-i-fitnesscenter-var-gyldigt

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jul/samtykke-til-ansigtsgenkendelse-i-fitnesscenter-var-gyldigt

Brug af kunstig intelligens i telefonsamtaler sat under lup

Det danske Datatilsyn (»Datatilsynet«) undersøgte den 27. juni 2024 IDA Forsikrings brug af kunstig intelligens til analyse af optagne telefonsamtaler. Datatilsynet fastslog, at en sådan praksis kan være lovlig, men at samtykkeprocessen skulle forbedres. Sagen blev behandlet under journalnummer 2023-431-0018.

Undersøgelsen, som Datatilsynet indledte af egen drift den 1. marts 2023 fokuserede på, hvordan IDA Forsikring anvender kunstig intelligens til at analysere selskabets telefonsamtaler med personer, der ringer til IDA Forsikrings kundeservice. IDA Forsikring optager indgående telefonopkald og sender lydfilerne til en databehandler, der transskriberer dem til tekst ved hjælp af talegenkendelse. Formålene bag indsamlingen og analysen er at forbedre IDA Forsikrings medlemsservice, sikre kvaliteten og give medarbejderne uddannelsesmæssig indsigt i samtalerne med henblik på at styrke servicen overfor medlemmerne.

Datatilsynet fandt, at IDA Forsikring kan optage og analysere samtalerne inden for rammerne af databeskyttelsesreglerne, men kritiserede imidlertid den nuværende samtykkeproces for ikke at leve op til databeskyttelsesreglerne, da samtykket ikke var tilstrækkelig granuleret. Det var dermed ikke muligt at samtykke særskilt til de enkelte formål.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/pres-

se-og-nyheder/nyhedsarkiv/2024/aug/ida-forsikrings-brug-af-kunstig-intelligens-til-analyse-af-optagne-telefonsamtaler

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jun/ida-forsikrings-brug-af-kunstig-intelligens-til-analyse-af-optagne-telefonsamtaler

Datatilsynet udgiver ny vejledning om sikkerhedsforanstaltninger mod utilsigtet offentliggørelse

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 10. september 2024 et nyt tillæg til deres vejledning over sikkerhedsforanstaltninger, der tager sigte mod at hjælpe dataansvarlige med at forhindre utilsigtet offentliggørelse af personoplysninger.

Den nye foranstaltning udgør således en del af Datatilsynets katalog over sikkerhedsforanstaltninger og fokuserer igennem konkrete tiltag på at minimere risikoen for, at personoplysninger utilsigtet bliver genstand for offentliggørelse. Foranstaltningerne indeholder både forebyggende og korrigerende tiltag, der kan hjælpe med at opdage og rette op på eventuelle sikkerhedsbrud.

Datatilsynet har forklaret i forbindelse hermed, at processen med at frasortere personoplysninger fra materiale, der skal offentliggøres, ofte resulterer i sikkerhedsbrud, som kan opdages flere år senere. Den nye foranstaltning indeholder derfor flere forslag til, hvordan man kan undgå disse sikkerhedsbrud.

Den dataansvarlige har en forpligtelse til at beskytte disse oplysninger mod utilsigtet offentliggørelse og sikre en løbende kontrol heraf. Datatilsynet har dog i deres praksis konstateret flere eksempler på brud vedrørende utilsigtet offentliggørelse af personoplysninger. Det er i lyset af Datatilsynets erfaring, at de udsteder denne udvidelse af kataloget.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/sep/ny-foranstaltning-om-styret-og-overvaaget-offentliggoerelse-af-data

Aarhus Universitet får kritik for håndtering af personoplysninger

Det danske Datatilsyn (»Datatilsynet«) har i en pressemeddelelse af 20. september 2024 informereret om udfaldet af to tilsyn med Aarhus Universitet af henholdsvis 22. maj og 11. juni i forbindelse med universitetets behandling af personoplysninger på forskningsområdet. Sagerne blev behandlet under journalnumrene 2023-421-0001 og 2023-421-0013.

I det første tilsyn blev tre forskningsprojekter udvalgt til skriftligt tilsyn med fokus på behandlingsgrundlag, ansvar og roller. Datatilsynet fandt i forbindelse med tilsynet, at der bl.a. var uklarheder om hjemmelsgrundlaget for behandlingen af personoplysninger i to af projekterne, og at der ikke var indgået en fyldestgørende databehandleraftale i et tredje projekt. Derudover blev der konstateret manglende tilsyn med universitetets databehandlere i to af projekterne.

Det andet tilsyn omfattede et fysisk besøg hos Aarhus Universitet, hvor fokus for tilsynet var en tilladelse til videregivelse af biologisk materiale fra et forskningsprojekt. Datatilsynet udvidede efterfølgende tilsynet til at omfatte alle forskningsprojekter baseret på den danske databeskyttelseslov, jf. lovbekendtgørelse nr. 289 af 9. marts 2024 (»databeskyttelsesloven«) § 10, hvor der inden for de seneste to år

Illustrasjon: Colourbox.com

var sket videregivelse omfattet af tilladelseskravet i databeskyttelseslovens § 10, stk. 3.

Datatilsynet udtalte alvorlig kritik af Aarhus Universitet for ikke at have sikret sig et overførselsgrundlag ved videregivelse af personoplysninger fra et forskningsprojekt og for ikke at have indhentet Datatilsynets tilladelse til videregivelse af personoplysninger i flere tilfælde.

Aarhus Universitet har nu i forbindelse med Datatilsynets kritik i medfør af det skriftlige tilsyn af 22. maj fået pålagt at redegøre for, hvordan de sikrer, at fremtidige forskningsprojekter overholder de databeskyttelsesretlige regler.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/sep/aarhus-universitet-faar-kritik-for-flere-forhold-i-forbindelse-med-forskning

Læs Datatilsynets afgørelser her:

https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/maj/aarhus-universitet-faar-kritik-for-haandtering-af-personoplysninger-i-tre-forskningsprojekter

https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jun/aarhus-universitet-faar-alvorlig-kritik-for-manglende-tilladelse-til-videregivelse-af-personoplysninger

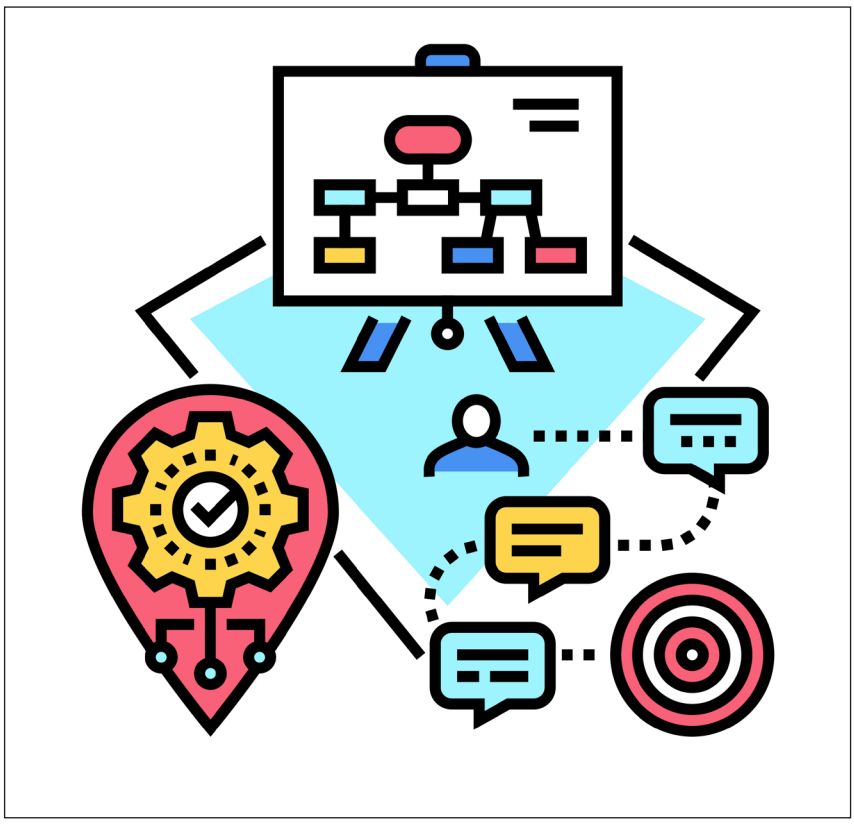
Tue Goldschmieding, partner i Gorrissen Federspiel og dansk redaktør for Lov & Data.

Wikström & PARTNERS

Karin Tilly och Anton Karlsson

Roadmap för myndigheters datahantering – En ny rapport från eSam

eSamverkansprogrammet (eSam) har i oktober 2024 publicerat rapporten ”Roadmap för myndigheters datahantering” (ES2024-15). Det sker stora förändringsarbeten på EU-nivå för datahantering och digitalisering i allmänhet, bland annat policyinitiativ och regelförändringar.



Illustrasjon: Colourbox.com

Rapporten har tagits fram i syfte att analysera och se över myndigheternas behov av att bli mer proaktiva i sin planering inför dessa förändringar. Rapporten ska även belysa och ge eSams medlemmar en bättre bild över de kommande policyinitiativ och regelförändringar som kan komma att påverka myndigheternas digitaliseringsarbete. Med anledning av detta har rapporten ”Radarbild – initiativ som påverkar myndigheternas digitaliseringsarbete” (ES2024-07) tidigare tagits fram över de olika nationella och från EU kommande policyinitiativ som av eSam anses mest väsentliga. Roadmap för datahantering tar även upp trender inom digitaliseringen, såsom generativ AI och de digitaliseringsstrategier som implementerats på nationell och europeisk nivå. Både Roadmap för datahantering och Radarbild finns att läsa på eSams webbplats.

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

Viveca Still

HD 2024/53: Upphovsrättsorganisation ansågs inte ha saklegitimation att driva ärende gällande intrång i vidaresändningsrätt

I ett av sina sällsynta upphovsrättsliga avgöranden har högsta domstolen i Finland slutit sig till att upphovsrättsorganisationen Kopiosto, som på basis av avtalslicens företräder upphovsrättsinnehavarna på området för vidaresändning av televisionsutsändningar som avses i 25 h § i upphovsrättslagen, inte har saklegitimation att i sitt eget namn driva ett civilrättsligt intrångsmål mot en part, i detta fall Telia, som inte skaffat licens för vidaresändning.

Domstolen menade att upphovsrättsorganisationen nog på basis av sin avtalslicensstatus och de fullmakter som den samlat in av rättsinnehavarna har rätt att licensiera vidaresändning av televisionsutsändningar och att driva mål som gäller indrivning av fordringar men ansåg att det skulle innebära en inskränkning i upphovsmannens rättigheter ifall upphovsrättsorganisationen i sitt eget namn skulle kunna driva ett civilrättsligt mål och där kräva sådant vederlag eller skadeståndsersättning som avses i upphovsrättslagens 57 §.

Domen var inte enhällig, utan domarrösterna föll med 3 mot 2. I sin avvikande åsikt framför Alice Guimaraes-Purokoski (med bifall av Kirsti Uusitalo) att man i förarbetena till upphovsrättslagen har betonat att avtalslicens är en sådan lagstiftningslösning om rättighetsförvaltning som tillåts i Europaparlamentets och rådets direktiv 2001/29/EG om harmonisering av vissa aspekter av upphovsrätt och närstående rättigheter i informationssamhället (*informationssamhällsdirektivet*). Domstolen har dessutom tolkat artikel 4 c i Europaparlamentets och rådets direktiv 2004/48/EG om säkerställande av skyddet av immateriella rättigheter (*enforcement-direktivet*) mot bakgrund av skäl 18 i direktivet så, att en avtalslicensorganisation ska beviljas rätt att i eget namn begära att varumärkesinnehavarnas rättigheter skyddas mot intrång, om organisationen enligt nationell rätt anses ha ett direkt intresse av att försvara dessa rättigheter och enligt nationell rätt är behörig att föra talan inför domstol i detta syfte. Unionsrätten reglerar inte villkoren för ett sådant direkt intresse (dom den 23 november 2023, *Telia Finland, C-201/22*, EU:C:2023:914, punkterna 30 och 48).

Guimaraes-Purokoski ansåg alltså att i en situation där Telia inte har skaffat avtalslicens av Kopiosto och där upphovsrättsinnehavarna till verken inte har fått ersättning för utnyttjandet av deras ensamrättigheter, har Kopiosto i egenskap av avtalslicensorganisation ett direkt intresse av att i domstol yrka på avgörande av den tvistiga frågan om Telias verksamhet är en upphovsrättsligt relevant vidaresändning av radio- och televisionsutsändningar. Samtidigt är det motiverat att anse att Kopiosto i egenskap av avtalslicensorganisation har ett direkt intresse av att yrka fastställelse av intrånget i upphovsrätten och även gottgörelse och skadestånd enligt upphovsrättslagen för intrång i ensamrätt för att försvara upphovsrättsinnehavarnas rättigheter.

Guimaeres-Purokoski ansåg alltså att det under dessa omständigheter inte kan ställas som villkor för förande av talan att det för avtalslicensorganisationens del uttryckligen föreskrivs om förande av talan i upphovsrättslagen. Inte heller domstolen har tolkat artikel 4 c i direktivet om säkerställande av immaterialrätt så, att en sådan talerätt uttryckligen ska beviljas genom en separat bestämmelse. Talerätten kan också grunda sig på allmänna processrättsliga regler, vilket EU-domstolen bekräftat i punkt 35-38 i domen *Telia Finland*. I finsk rätt finns det varken allmänna

bestämmelser om talerätt i rättegångsbalken eller i bestämmelserna i den materiella lagen, och ett sådant krav har inte heller i avgörandepraxis ställts som villkor för upphovsrättsorganisationens talan om intrång (HD 1989:87). Att ställa ett krav på uttrycklig reglering som villkor för avtalslicensorganisationens talerätt innebär således ett krav som är mer långtgående än det tidigare rättsläget och som inte har någon grund i unionsrätten.

Guimaeres-Purokoski påtalade att de exempel på fullmakt från upphovsmännen som upphovsrättsorganisationen förevisat inkluderar rättegångsfullmakt. Dessutom styr lagen om kollektiv förvaltning av upphovsrätt (1494/2016) upphovsrättsorganisationernas verksamhet, inklusive vad gäller förvaltning och fördelning av ersättningar samt tillsyn. Hon ansåg därmed att det inte fanns risk för missbruk som är förknippad med utövandet av en rättegångsfullmakt. Hon ansåg också att det med tanke på antalet upphovsmän som upphovsrättsorganisationen representerar och med tanke på att den är en i upphovsrättslagen avsedd avtalslicensorganisation gällande den användning som var föremål för tvisten, har ett klart intresse av att kunna föra talan. I praktiken är det nämligen svårt eller omöjligt att nå alla relevanta rättsinnehavare då det gäller denna typ av verk.

HD-domen undergräver den kollektiva förvaltningen av upphovsrätt

Vad är då konsekvenserna av denna dom? För upphovsrättsorganisationerna är domen synnerligen problematisk och hotar undergräva den kollektiva förvaltningen av upphovsrätt.
I praktiken är det svårt och i praktiken omöjligt för en kollektivförvaltningsorganisation att skrida till rättsliga åtgärder ifall förutsättningen är att de ska samla bakom ett käromål alla rättsinnehavarna till de berörda verken. Jag kan inte annat än instämma i Guimaeres-Purokoskis överväganden som utgår ifrån att upphovsrättsorganisationerna har ett klart intresse av att kunna driva käromål och att riskerna för missbruk av processmandat är försvinnande liten med tanke på att upphovsrättsorganisationerna är långt reglerade och har en på lag baserad skyldighet att fördela indrivna medel på ett rättvist och transparent sätt till rättsinnehavarna inklusive, då det alltså gäller rättigheter som representeras på basen av en avtalslicenskonstruktion, även till sådana rättsinnehavare som inte givit upphovsrättsorganisationen fullmakt att företräda dem. Hur ska upphovsrättsorganisationerna kunna driva upphovsmännens rättigheter och kräva att användare skaffar tillstånd till användning av upphovsrättsligt skyddade verk om de inte har någon möjlighet att skrida till åtgärder vid intrång i upphovsrätt?

Upphovsrättsorganisationerna kan inte heller kräva att upphovsmännen överlåter sin ensamrätt till organisationen, vilket troligtvis skulle möjliggöra för organisationen att driva ärenden i sitt eget namn, eftersom detta i sin tur kan anses strida mot principerna i lagen om kollektiv förvaltning av upphovsrätt. Bakgrunden till ifrågavarande lag utgår ifrån att upphovsrättsorganisationerna har en portvaktsroll vilket leder till att upphovsmännen är beroende av dem för att kunna nå ut till och kunna licensiera sina verk på marknaderna. Upphovsmännen är alltså i en utsatt ställning i förhållande till upphovsrättsorganisationerna. Att tvingas överlåta sin ensamrätt påverkar direkt upphovsmännens äganderättsliga ställning och möjligheter att i olika sammanhang disponera över sin rättighet.

Domen är ett prejudikat och måste följas i motsvarande fall. Att ändra rättsläget nu kräver alltså lagstiftningsåtgärder. Man får alltså hoppas på att undervisnings- och kulturministeriet snarast skrider till lagstiftningsåtgärder för att tillgodose upphovsrättsorganisationernas möjligheter att driva intrångsärenden å upphovsmännens vägnar. Ett sådant befullmäktigande kan säkerligen formuleras på olika sätt, och ifall man vill försäkra sig om att ett på lag baserat processmandat inte drivs i strid med upphovsmännens intressen kan man naturligtvis begränsa mandatet genom en specifik möjlighet för upphovsmän att förbjuda upphovsrättsorganisationen att i sitt eget namn driva intrångsärenden eller någon annan liknande lösning.

Fallet skjuter upp avgörandet i frågan om det är möjligt att i Finland licensiera sändning över kabelnät direkt av rättsinnehavarna

Fallet berörde i utgångspunkten frågan om det i Finland är möjligt att licensiera rättigheterna till sändning över kabelnät direkt av rättsinnehavarna och om ett kabelbolag på basen av ett underleverantörsavtal med ett sändarföretag kan anses agera för sändarbolagets räkning i en teknisk roll eller om kabelbolagets verksamhet skall anses vara sådant att sändningen sker för kabelbolagets egen räkning och att ändamålet med underleverantrösavtalet enbart är att kringgå upphovsrättsavgifter.

I fallet är det också fråga om vilka rättigheter som sändarföretaget faktiskt har skaffat och om det finns rättigheter som det inte skaffat och där det skulle behövas en kompletterande lösning. Ett problem på marknaden har redan länge varit det att sändarföretaget skaffar väldigt omfattande licenser, till och med så omfattande att det klart överskrider sändarföretagets egna behov och eventuellt också de rättigheter upphovsmännen själva kan förfoga över. Samtidigt finns det en dubbelöverlåtelseproblematik i förhållande mellan de rätter som överlåts till audiovisuella producenter och de rättigheter som överlåts till kollektivförvaltningsorganisationerna.

Tyvärr innebär HD-domen att den egentliga rättsfrågan inte kommer att behandlas eller att den åtminstone skjuts framåt på obestämd tid.

Viveca Still, juris doktor, lagstiftningsråd.

Gorrissen Federspiel

Tue Goldschmieding

Sø- og Handelsretten afgør sag om efterligning af cykelstativ

Sø- og Handelsretten afsagde den 8. juli 2024 dom i en sag om efterligning af et cykelstativ. Sagen blev behandlet under sagsnummer Sag BS-9681/2022-SHR.

I sagen havde HITSA A/S (»HITSA«) anlagt sag mod Inventarrum A/S (»Inventarrum«) med påstand om, at Inventarrums IC 10 City-cykelstativ udgjorde en nærgående efterligning af HITSA's NOLI-cykelstativ. HITSA hævdede, at Inventarrum ved at producere, markedsføre og sælge IC 10 City-cykelstativet havde krænket deres rettigheder til NOLI-cykelstativet i henhold til den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022 (»markedsføringsloven«), og derfor var berettiget til økonomisk kompensation.

Konkret fandt retten, at NOLI-stativet havde tilstrækkeligt særpræg, kommerciel adskillelsesevne samt markedsposition til at nyde beskyttelse mod nærgående eller slaviske produktefterligninger efter markedsføringslovens § 3. Denne bestemmelse pålægger erhvervsdrivende at udvise god markedsføringsskik og har et selvstændigt anvendelsesområde for nærgående efterligninger for så vidt angår udtryk, der ikke nyder tilstrækkelig beskyttelse efter immaterialretten (f.eks. design- eller ophavsretten).

I den anledning fandt Sø- og Handelsretten, at IC 10 City-cykelstativet, trods mindre forskelle, var en for nærgående efterligning af NOLI-stativet og derfor i strid med markedsføringslovens § 3. HITSA blev i lyset af efterligningen tilkendt erstatning og vederlag på 300.000 kr. Retten fandt desuden, at HITSA ikke havde udvist retsfortabende passivitet, og de var derfor afskåret fra at gøre krænkelsen gældende. Inventarrum blev herefter forbudt at fremstille, markedsføre, udbyde og sælge cykelstativet IC 10 City.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://www.domstol.dk/soeoghandelsretten/aktuelt/2024/7/efterligning-af-cykelstativ/

Læs dommen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/media/-300011/files/BS-9681-2022-SHR_Dom.pdf

En patentkrænkelse forudsætter krænkelse af alt indhold i et patentkrav

Sø- og Handelsretten afsagde den 11. juli 2024 kendelse i sagen mellem Janssen Biotech, Inc (»Janssen Biotech«) og Samsung Bioepis NL B.V. (»Samsung Bioepis«) samt AGC Biologics A/S (»AGC«). Sagen blev behandlet under sagsnummer BS-10043/2024-SHR. Janssen Biotech havde anmodet om nedlæggelse af midlertidigt forbud og påbud mod Samsung Bioepis og AGC, da de ifølge Janssen Biotech krænkede Janssen Biotechs patent på anvendelsen af aktivstoffet 'ustekinumab' til behandling af colitis ulcerosa.

Retten fandt det ikke sandsynliggjort, at AGC i Danmark realiserede eller inden for en ret snæver tidsramme ville realisere samtlige træk i stridspatentets krav. Retten bemærkede, at stridspatentets beskyttelsesmæssige udstrækning geografisk var afgrænset til dansk territorium efter den danske patentlov, jf. lovbekendtgørelse nr. 90 af 29. januar 2019. I Danmark producerer AGC som kontraktproducent stoffet ustekinumab som bulkmateriale med henblik på eksportsalg til Samsung Bioepis i udlandet. På baggrund af de af AGC's foretagne danske aktiviteter noterede retten, at bulkmateriale i form af rent aktivstof ikke som sådan kan anvendes som et lægemiddel, men at dette forudsætter en processering, og AGC er ikke involveret i sådanne nødvendige handlinger efter salget af aktivstoffet til Samsung Bioepis.

På baggrund heraf afslog retten at imødekomme de af Janssen Biotech fremsatte anmodninger om midlertidige forbud og påbud. Retten nægtede således fremme af forbudsanmodningerne mod den danske producent AGC og den udenlandske aftager af aktivstoffet, Samsung Bioepis.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://www.domstol.dk/soeoghandelsretten/aktuelt/2024/7/forbudsanmodning-naegtet-fremme/

Læs dommen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/media/-300011/files/BS-10043-2024-SHR_Kendelse.pdf

Forbud mod Steve Maddens GRAND AVE-sko

Sø- og Handelsretten nedlagde den 9. august 2024 forbud mod, at Steve Madden Ltd og Steve Madden Europe B.V (»Steve Madden«) markedsfører, udbyder, sælger, eksporterer og importerer skomodellen 'GRAND AVE' i Danmark. Sagen

blev behandlet under sagsnummer BS-25562/2024-SHR.

Sagen vedrørende Steve Maddens skomodel 'GRAND AVE' opstod da GANNI A/S (»GANNI«) anmodede Sø- og Handelsretten om et forbud. GANNI gjorde gældende, at skoen udgjorde en krænkelse af deres 'Buckle Ballerina'-sko, som er beskyttet efter både den danske ophavsretslov, jf. lovbekendtgørelse nr. 1093 af 20. august 2023 (»ophavsretsloven«), og den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022 (»markedsføringsloven«). Retten fandt, at GANNI's skomodel 'Buckle Ballerina' nød beskyttelse, og at Steve Maddens 'GRAND AVE'-sko udgjorde en krænkelse af GANNI's rettigheder efter både ophavsretsloven og markedsføringsloven, idet 'GRAND AVE'-skoen fandtes at have samme designmæssige udtryk som 'Buckle Ballerina'-skoen, ligesom skoen umiddelbart ville give forbrugeren samme helhedsindtryk.

Retten fandt det derfor usandsynligt, at Steve Maddens 'GRAND AVE' var udformet uden kendskab til skomodellen 'Buckle Ballerina'. Forbuddet blev på den baggrund nedlagt over for både det amerikanske moderselskab og det europæiske datterselskab, ansvarlig for drift og salg på det europæiske marked.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://www.domstol.dk/soeoghandelsretten/aktuelt/2024/8/forbudssag-om-sko/

Læs dommen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/media/-300011/files/Kendelse_BS-25562-2024-SHR.pdf

Ingen beskyttelse for entreprenørpumpe

Sø- og Handelsretten frifandt den 22. august 2024 Erenfred Pedersen A/S (»Erenfred Pedersen«) i en sag anlagt af Staring A/S (»Staring«), som omhandlede hvorvidt en af Starings forhandlet 'Tsurumi'-pumpe af typen HS2.4 nød markedsføringsretlig beskyttelse efter den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022 (»markedsføringsloven«), og i givet fald, om Erenfred Pedersen ved salg og markedsføring af fem dykpumper krænkede markedsføringsloven. Sagen blev behandlet under sagsnummer BS-22033/2023-SHR.

Konkret havde Staring anlagt sag mod Erenfred Pedersen med påstand om, at Erenfred Pedersens markedsføring af de førnævnte fem dykpumper krænkede Starings rettigheder.

Retten fandt imidlertid, at Staring for så vidt angik fire af pumperne havde udvist retsfortabende passivitet ved at give Erenfred Pedersen en berettiget forventning om, at de ikke ville rejse sag om disse fire dykpumper. Herved blev Erenfred Pedersen frifundet for de af Staring fremsatte påstande vedrørende de fire ud af fem dykpumper.

Da søgsmålet således var materielt afgrænset til den femte pumpe, skulle det vurderes, om denne nød markedsføringsretlig beskyttelse efter dansk ret. I den forbindelse fandt Retten det ikke godtgjort, at Tsurami-pumpen havde en sådan markedsposition for entreprenørpumper i Danmark og et sådant særpræg, at den efter en samlet vurdering havde kommerciel adskillelsesevne. Tsurami-pumpen nød derfor ikke beskyttelse efter markedsføringsloven, og Erenfred Pedersen blev derfor også frifundet for Starings påstand vedrørende den femte pumpe.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://www.domstol.dk/soeoghandelsretten/aktuelt/2024/8/entreprenoerpumpe-ej-beskyttet/

Læs dommen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-22033-2023-SHR.pdf

Google frifundet i sag om Jobindex' rettigheder

Sø- og Handelsretten frifandt den 27. august 2024 Google Ireland Ltd (»Google«) i en sag anlagt af Jobindex A/S (»Jobindex«), som omhandlede, hvorvidt Google havde krænket Jobindex' rettigheder efter den danske ophavsretslov, jf. lovbekendtgørelse nr. 1093 af 20. august 2023 (»ophavsretsloven«), den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022 (»markedsføringsloven«) og den danske varemærkelov, jf. lovbekendtgørelse nr. 88 af 29. januar 2019 (»varemærkeloven«). Sagen blev behandlet under sagsnummer BS-43304/2023-SHR.

Jobindex sagsøgte Google med påstand om, at Googles platform 'Google for Jobs' krænkede Jobindex' rettigheder ved at gøre jobannoncer kopieret fra Jobindex tilgængelige for almenheden uden Jobindex' tilladelse. Retten fandt imidlertid, at Google for Jobs alene fremsøger og lokaliserer jobannoncer, der allerede findes på internettet, idet formålet med Google for Jobs-funktionen er at få brugerne videre til de relevante hjemmesider. Som en søgemaskine, der alene fremsøger og lokaliserer information, som befinder sig andre steder, sker der således ikke en tilgængeliggørelse efter ophavsretslovens § 2. Således fandt retten, at Google ikke krænkede Jobindex' ophavsret.

Derudover fandt retten, at påstandene ét til fire var overflødige, da de alene udgjorde det retlige grundlag for Jobindex' femte og sjette påstand. Dermed måtte disse betragtes som anbringender til støtte for de to sidste påstande. Ud fra det ræsonnement tog retten således Googles påstand om afvisning af påstand ét til fire til følge. Desuden fandt retten det ikke godtgjort, at Google havde handlet i strid med hverken markedsførings- eller varemærkeloven.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://www.domstol.dk/

soeoghandelsretten/aktuelt/2024/8/jobindex-rettigheder-var-ikke-kraenket/

Læs dommen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/media/-300011/files/Dom__BS-43304-2023-SHR.pdf?rev1

NS System A/S taber varemærkesag om »Elastosoft«

Den 28. august 2024 frifandt Sø- og Handelsretten Jetsport v/Claus Bo Mørk (»Jetsport«) i en sag anlagt af NS System A/S (»NS System«) vedrørende retten til varemærket »Elastosoft«. Sagen blev behandlet under sagsnummer BS-35135/2023-SHR.

NS System nedlagde påstand om, at Jetsport uberettiget anvendte varemærket »Elastosoft« for tekstiltransfers og ønskede derfor afklaring af, hvem der havde stiftet ret til varemærket først. NS System hævdede at have stiftet varemærketten til betegnelsen i 1999. At denne ibrugtagning af NS System kunne konstituere dannelsen af en varemærket, bestred Jetsport imidlertid ved at nedlægge et modkrav om, at Jetsport havde anvendt betegnelsen siden 1995.

Sø- og Handelsretten fandt, at »Elastosoft« ikke havde en sådan beskrivende karakter for selve produktet tekstiltransfers, at det var til hinder for stiftelse af et dertilhørende varemærke, ligesom ordmærket fandtes at have det fornødne særpræg til at kunne udgøre et varemærke. Retten fastslog, at Jetsport havde dokumenteret brugen af »Elastosoft« siden 1995 ved at have markedsført tekstiltransfers under betegnelsen »Elastosoft« til kunder i hele Danmark og dermed havde stiftet varemærket til betegnelsen før NS System. Jetsport havde således ikke handlet i strid med eventuelle rettigheder tilhørende NS System ved sin brug af mærket »Elastosoft«, og Jetsport blev derfor frifundet for NS Systems påstande.

Som følge af Jetsports varemærket til mærket »Elastosoft« for tekstiltransfers var NS Systems' markedsføring på deres hjemmeside med de udsagn, som var gengivet i Jetsports selvstændige påstand, således i strid med den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022, § 3 og § 20, om pligten til at udvise god markedsføringsskik og forbuddet mod vildledende og utilbørlig handelspraksis. Betingelserne for at nedlægge forbud mod disse udsagn fandtes derfor opfyldt. Retten tog derfor Jetsports selvstændige påstand til følge.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://www.domstol.dk/alle-retsinstanser/overordnede-retter/soe-og-handelsretten/aktuelt/2024/8/varemaerket-elastosoft/

Læs dommen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-35135-2023-SHR.pdf?rev1

Retten finder Kingspan Insulation ApS skyldig i vildledende markedsføring

Sø- og Handelsretten afsagde den 10. september 2024 dom mellem Kingspan Insulation ApS (»Kingspan«) og ROCKWOOL Danmark A/S (»ROCKWOOL«) og fandt, at Kingspan havde overtrådt den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022 (»markedsføringsloven«), ved at fremsætte to vildledende udsagn i deres markedsføring af isoleringsprodukter. Dommen blev afsagt under sagsnummeret BS-23562/2021-SHR.

Sagen anlagt af ROCKWOOL mod Kingspan omhandlede, hvorvidt Kingspan ved at fremsætte en række udsagn i artikler på egen hjemmeside og på hjemmesiden byggematerialer.dk havde handlet i strid med markedsføringsloven, herunder reglerne om god markedsførings- og erhvervsskik og forbuddene mod vildledning og visse former for sammenlignende reklamer.

Retten fandt, at to af de i sagen forelagte udsagn på Kingspans hjemmeside og byggematerialer.dk var i strid med markedsføringsloven, herunder forbuddet mod vildledning og god markedsføringsskik. Retten fandt endvidere, at disse udsagn kunne give forbrugerne et fejlagtigt indtryk af produkternes egenskaber sammenlignet med konkurrerende produkter som mineraluld.

Kingspan blev dog frifundet for overtrædelse af markedsføringsloven ved anvendelse af øvrige udsagn. Derudover afviste retten flere af de af ROCKWOOL fremsatte påstande, idet påstandene var for brede og uklare til at kunne tages under påkendelse. Retten fandt afslutningsvis ikke grundlag for berigtigelse, erstatning eller bødestraf og tog derfor ikke ROCKWOOL's påstand herom til følge.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://www.domstol.dk/soeoghandelsretten/aktuelt/2024/9/markedsfoering-af-isolering/

Læs dommen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-23562-2021-SHR.pdf

Erstatning for krænkelse af ophavsretsloven og markedsføringsloven

Sø- og Handelsretten afsagde den 11. september 2024 dom i sag BS-63208/2023 vedrørende krænkelse af såvel ophavs- som markedsføringsretten.

Sagsøgte, Liewood A/S (»Liewood«), havde anerkendt, at salg og markedsføring af en futonstol krænkede sagsøgers, Karup Design A/S (»Karup Design«), rettigheder efter både den danske ophavsretslov, jf. lovbekendtgørelse nr. 1093 af 20. august 2023 (»ophavsretsloven«) og den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022 (»markedsføringsloven«). Efter, at Liewood fik kendskab til krænkelsen, kunne stolen dog stadig findes til salg online hos andre forhandlere. Sagsøger nedlagde herefter påstand om forbud mod fremstilling og påbud om

tilbagekaldelse af de pågældende stole. Hertil krævede Karup Design erstatning.

For så vidt angik påstanden om tilbagekaldelse lagde retten vægt på, at sagsøgte havde sendt en mail til en udokumenteret kundekreds med oplysning om tilbagekaldelse af futonstolen. Sagsøger havde ikke dokumenteret tilstrækkeligt, at sagsøgte herefter havde fortsat distribution af stolen til sine B2B-kunder. Således var det ikke godtgjort, at det var nødvendigt at give påbud om tilbagekaldelse, jf. markedsføringslovens § 24, stk. 1, om retsmidler efter denne lovgivning samt ophavsretsloven § 84, om tilintetgørelse af ophavsretsstridige værker.

I forhold til erstatning lagde retten til grund, at initiativet til futonstolen kom fra Liewoods leverandør, og at der i øvrigt ikke var holdepunkter for, at sagsøgte skulle have været opmærksom på, at stolen krænkende sagsøgers rettigheder, hvorfor krænkelsen ikke kunne karakteriseres som grov. Det var ikke med rimelig sikkerhed muligt at fastslå det salg, Karup Design havde mistet som følge af Liewoods salg og markedsføring, hvorfor erstatningen blev fastsat skønsmæssigt til samlet 125.000 kr.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://www.domstol.dk/soeoghandelsretten/aktuelt/2024/9/kraenkelse-futonstol/

Læs dommen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-63208-2023-SHR.2551.aspx

Sø- og handelsretten afsiger dom om ejerskabet af to patentansøgninger

Sø- og handelsretten afsagde den 13. september 2024 dom i en sag om ejerskab af to patentansøgninger vedrørende en elektrisk vinduesåbner. Sagen blev behandlet under sagsnummer BS-14416/2022-SHR, og involverede WindowMaster International A/S (»WindowMaster«) som sagsøger og Nordic Eco Vent ApS (»Nordic Eco Vent«) samt flere enkeltpersoner som sagsøgte.

Sagen drejede sig om, hvorvidt WindowMaster havde ret til (med) ejerskab af de to patentansøgninger, som Nordic Eco Vent havde indleveret til den danske Patent- og Varemærkestyrelse, samt om de sagsøgte ulovligt havde anvendt WindowMasters forretningshemmeligheder, og om de i så fald skulle betale økonomisk kompensation herfor.

WindowMaster gjorde gældende, at de to patentansøgninger var baseret på opfindelser gjort under ansættelsen af de sagsøgte hos WindowMaster, og at de derfor havde ret til (med)ejerskab af disse ansøgninger. Retten vurderede imidlertid, at dette ikke var tilfældet. Dette blev underbygget af bevismateriale, der viste, at de relevante opfindelser blev udviklet efter ansættelsens ophør.

WindowMaster anførte endvidere, at sagsøgte havde misbrugt deres forretningshemmeligheder ved at anvende fortrolig information til at udvikle opfindelserne. Retten fandt dog, at der ikke var tilstrækkeligt bevis for, at sagsøgte havde anvendt Window-Masters forretningshemmeligheder i forbindelse med indlevering af patentansøgningerne. Retten anerkendte, at leverandøroplysninger kunne udgøre forretningshemmeligheder, men at der ikke kunne påvises et økonomisk tab for brugen af oplysningerne.

Retten konkluderede, at de sagsøgte parter hverken skulle overdrage eller anerkende WindowMaster som medejer af patenterne. WindowMaster blev pålagt at betale sagsomkostninger.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://www.domstol.dk/soeoghandelsretten/aktuelt/2024/9/patentansoegninger/

Læs dommen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-14416-2022-SHR.2552.aspx

Østre Landsret stadfæster dom om krænkelse af elitesportsudøvers ret til navn og billede

Østre landsret afsagde den 8. juli 2024 dom i en ankesag om krænkelse af en elitesportsudøvers ret til eget navn og billede. Sagen blev behandlet under sagsnummer BS-23713/2023-OLR.

Ankesagen var indbragt af spilvirksomheden Hillside (New Media Malta) Plc. (»Bet365«) mod Spillerforeningen Danske Elitesportsudøveres Forening og Håndbold Spiller Foreningen som mandatarer for en række elitesportsudøvere, herunder Kasper Schmeichel og Christian Eriksen.

Sagen omhandlede, hvorvidt Bet365 havde krænket elitesportsudøverens ret til eget navn og billede ved at bruge ovenstående sportsudøveres billeder og navne i opslag på Bet365's sociale medier uden samtykke. I 1. instans havde Sø- og Handelsretten fundet, at der var tale om krænkelse. Herefter ankede Bet365 sagen til 2. instans og påstod frifindelse under påberåbelse af sin kommercielle ytringsfrihed efter Den Europæiske Konvention til Beskyttelse af Menneskerettigheder og Grundlæggende Frihedsrettigheder (»EMRK«), artikel 10 samt den tilsvarende bestemmelse i artikel 11 efter Den Europæiske Unions Charter om grundlæggende rettigheder (»Chartret«).

Østre Landsret stadfæstede Sø- og Handelsretten afgørelse efter en tiltrædelse af sidstnævntes afvejning af elitesportsudøvernes ret til privatliv og omdømme sammenholdt Bet365's kommercielle ytringsfrihed. Landsretten fastholdt således, at der var sket krænkelse. Landsretten udtalte, at det markedsføringsmæssige formål med Bet365's brug af elitesportsudøvernes navn og billede ikke kunne opveje individets ret til en beskyttelse af sit privatliv.

På den baggrund blev Bet365 til hver enkelt sportsudøver pålagt at betale både vederlag og erstatning efter den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022.

Læs pressemeddelelsen fra Østre Landsret her: https://www.domstol.dk/oestrelandsret/aktuelt/2024/7/kraenkelse-af-elitesportsudoeveres-ret-til-navn-og-billede/

Læs dommen fra Østre Landsret her: https://www.domstol.dk/media/hugjf4kv/dom-af-872024.pdf

Jysk får bøde på 200.000 kroner for vildledende prismarkedsføring

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) meddelte i en pressemeddelelse af 1. juli 2024 afslutningen på en undersøgelse af Jysk A/S (»Jysk«). Jysk blev politianmeldt og indstillet til en bøde på 200.000 kr. for at have anvendt vildledende priser i sin markedsføring af en dyne og en seng i henholdsvis 2017 og 2021. Jysk vedtog den indstillede bøde.

Jysk havde markedsført en dyne på tilbud til 350 kr. og 300 kr. med en normalpris på 599 kr. Dynen havde imidlertid i dele af perioden haft en lavere normalpris, hvorfor der var tale om vildledning i strid med den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022, § 5, stk. 1. Ydermere havde Jysk udbudt en seng til 14.000 kroner med en overstreget førpris på 27.999 kr. Da sengen i 38 af de 83 forudgående dage også havde været til salg for 14.000 kr., var tilbuddet vildledende og gav forbrugerne et fejlagtigt indtryk af et særligt godt tilbud.

Læs pressemeddelelsen fra Forbrugerombudsmanden her:https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2024/20240701-boede-paa-200000-kroner-for-vildledende-prismarkedsfoering/

Ny samarbejdsaftale skal skærpe kontrol med ulovlig markedsføring af spil i Danmark

Den danske Forbrugerombudsmand, den danske Spillemyndighed og det danske Spilreklamenævn har i en pressemeddelelse af 11. juli 2024 udmeldt, at parterne har indgået en aftale for at styrke indsatsen mod ulovlig markedsføring af spil. Formålet med aftalen er at koordinere myndighedernes arbejde med henblik på bedre deling af viden om og hurtigere reaktion på lovovertrædelser. Særligt fokus rettes på tilfælde, hvor reklamer er målrettet sårbare grupper, herunder unge og personer med spilafhængighed.

Indsatsen skal ses i lyset af, at de respektive institutioner håndterer spilvirksomheders markedsføring på tværs af forskellige regelsæt og retsområder.

I praksis indebærer det, at myndighederne tilsigtes at koordinere deres tilsyn og indsatser, så spilvirksomheder ikke tjekkes flere gange for samme overtrædelse af forskellige institutioner. Hvis en virksomhed eksempelvis anmeldes for ulovlig reklame hos én myndighed, skal oplysningerne ifølge den nye aftale hurtigt deles med de øvrigt relevante parter. Intentionen herfor er ikke kun at spare ressourcer, men også sikre en i højere grad ensartet og konsekvent håndtering af overtrædelser inden for ulovlig markedsføring af spil på det danske marked på tværs af gældende regelsæt.

Læs pressemeddelelsen fra forbrugerombudsmanden her: https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2024/20240711-ny-aftale-skal-styrke-indsatsen-mod-spilvirksomheders-markedsfoering/

Forbrugerombudsmanden politianmelder selskabet GOR-Toms ApS for ulovlig markedsføring af alkohol til unge

Den 17. juli 2024 indgav den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) en politianmeldelse mod selskabet GOR-Toms ApS (»GOR-Toms«) for i 59 tilfælde at have markedsført begivenheder på Facebook, hvor der blev omtalt, vist billeder af eller henvist til alkohol. Indholdet var rettet mod skoleelever i alderen 16-17 år. GOR-Toms driver diskotekerne »Kalas Club« og »Club Zanzi Event & Nightclub«, og står ligeledes bag natklubbernes facebooksider.

Forbrugerombudsmanden understregede, at det ifølge den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022 (»markedsføringsloven«), § 11, stk. 2, er forbudt at omtale, vise billeder af eller referere til alkohol i markedsføring, der er rettet mod børn og unge. Dette forbud gælder uanset, om der reelt serveres alkohol til personer under 18 år. Forbrugerombudsmanden vurderede på denne baggrund, at GOR-Toms havde overtrådt markedsføringsloven.

Læs pressemeddelelsen fra forbrugerombudsmanden her:https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2024/20240717-selskab-politianmeldt-for-omfattende-markedsfoering-af-alkohol-over-for-boern-og-unge-paa-facebook/

Forbrugerombudsmanden finder flere klimaudsagn vildledende

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) fastslog den 12. juli 2024, at det var i strid med den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022 (»markedsføringsloven«), at en virksomhed, der leverede CO2-beregninger, havde kåret Danmarks mest klimavenlige hotel og markedsført sig på denne baggrund. Dette udmøntede sig i to afgørelser med sagsnumrene 24/06919 og 24/05255, hvoraf den første vedrørte forbrugere og den anden erhvervsdrivende.

Virksomheden overtrådte bl.a. markedsføringslovens § 20 ved at

kåre Danmarks mest klimavenlige hotel. Dokumentationen for klimaudsagnet levede op til relevante ISO-standarder, men omfattede kun de hoteller, der deltog i konkurrencen og repræsenterede således ikke alle danske hoteller, hvorfor virksomheden på den baggrund ikke kunne kåre det mest klimavenlige hotel.

Ydermere markedsførte virksomheden sig med udsagn om, at ophold på specifikke hoteller var mere klimavenligt end hos en gennemsnitlig dansker. Dette var vildledende, da sammenligningen ikke tog højde for klimapåvirkningen af forbrugeres private boliger, og da det desuden var en irrelevant sammenligning.

Det var også vildledende, at virksomheden markedsførte sig med udsagn om miljøvenlige og bæredygtige rejsedestinationer, når der alene var tale om tiltag, som forbrugere selv kunne foretage, f.eks. at besøge færre attraktioner, spise vegansk mv. Virksomhedens markedsføring var derfor i strid med dokumentationskravet i markedsføringslovens § 13 samt forbuddet mod vildledning mellem erhvervsdrivende i § 20.

Læs pressemeddelelsen fra forbrugerombudsmanden her: https://forbrugerombudsmanden.dk/find-sager/sager/markedsfoeringsloven/sager-efter-markedsfoeringsloven/miljoeogetik/en-virksomhed-der-leverede-co2-beregninger-til-brug-for-andre-virksomheder-kunne-ikke-dokumentere-sine-udsagn-om-at-have-kaaret-danmarks-mest-klimavenlige-hoteller/

Forbrugerombudsmanden politianmelder to personer for at markedsføre alkohol målrettet børn og unge

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) politianmeldte den 25. juli 2024 to personer for markedsføring af alkohol målrettet børn og unge på Instagram og Facebook. De to personer havde reklameret for fester med billeder af bl.a. drinks og vodkaflasker med teksten 16+ i hjørnet.

Forbrugerombudsmanden fandt, at de to personers profiler rettede deres markedsføring af alkohol mod børn og unge under 18 år. Hertil fastslog Forbrugerombudsmanden, at markedsføring af alkohol rettet mod børn og unge er i strid med den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022, § 11, stk. 2, og at dette er tilfældet uanset, om der er tale om mindre fester eller andre arrangementer, der ikke afholdes på diskoteker.

Læs pressemeddelelsen fra forbrugerombudsmanden her: https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2024/20240725-forbrugerombudsmanden-politianmelder-personer-for-alkoholreklamer-rettet-mod-boern-og-unge/

Udsagnet »vandfast« må kun bruges om smykker med reel vandmodstand

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) vurderede den 16. august 2024, at det ikke er i strid med vildledningsforbuddet i den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022, at benytte udsagnet »vandfast« om smykker behandlet med belægningsprocessen PVD (Physical Vapor Deposition), hvis belægningsprocessen faktisk gør smykket mere modstandsdygtigt. Det er dog ikke tilstrækkeligt, hvis smykket blot er mere modstandsdygtigt over for vand end andre smykker, hvis det reelt ikke er vandfast.

De særlige aspekter ved et produkt, der fremhæves i markedsføringen, må ses i forhold til udbuddet af tilsvarende produkter på markedet. Er det almindeligt forekommende for smykker at være mere vandfaste, vil det kunne være vildledende at fremhæve det som et særligt aspekt ved produktet.

Forbrugerombudsmanden henledte også opmærksomheden på, at det kan være vildledende at benytte udsagnet »vandfast« om smykker med en PVD-belægning, hvis smykket sammenlignes med bestemte typer af smykker, der også er modstandsdygtige over for vand, eksempelvis massivt guld.

Læs pressemeddelelsen fra forbrugerombudsmanden her: https://forbrugerombudsmanden.dk/find-sager/sager/markedsfoeringsloven/2407901-forbrugerombudsmandens-vurdering-af-udsagnet-vandfaste-smykker/

Tagging uden samtykke er i strid med spamforbuddet

En virksomhed, som sælger fodboldtrøjer, ønskede en vurdering fra den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) angående af en række eksempler på deltagerkrav, som virksomheden påtænkte at anvende på sociale medier til giveaways/konkurrencer.

Forbrugerombudsmanden vurderede den 20. august 2024, at det ikke er omfattet af spamforbuddet i den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022, § 10, stk. 1, at stille krav om, at deltageren skal like opslaget eller følge virksomheden på sociale medier. Det skyldes, at indholdet alene vises i deltagerens venners newsfeed og derfor ikke karakteriseres som elektronisk post. Det er – af samme årsager – ej heller omfattet af spamforbuddet at oplyse, at deltagerens chancer for at vinde øges ved at dele konkurrencen på Story.

For så vidt angår deltagerkravet »Fortæl 2 venner i kommentaren som også skal have chancen for at vinde« udtalte Forbrugerombudsmanden, at en forudsætning for anvendelse af kravet var, at deltageren anvendte tag-funktionen. Hvis en virksomhed eller en bruger tagger en anden bruger i et opslag, der er en erhvervsmæssig aktivitet og indeholder markedsføring, og den taggede bruger modtager notifikati-

on herom, er tagget omfattet af spamforbuddet. Deltagerkravet er herefter i strid med spamforbuddet, medmindre den, som tagges, har samtykket hertil.

Tilsvarende fandt Forbrugerombudsmandens, at virksomhedens tre resterende eksempler på deltagerkrav skabte incitament til, at deltageren skulle »tippe« sine venner om konkurrencen, hvilket ofte vil foranledige et tag, selvom ordet »tag« ikke er anvendt. Da virksomheden måtte anse det for sandsynligt, at deltagere tagger andre brugere i kommentarfeltet og derfor deler markedsføringen på en ulovlig måde, fandt Forbrugerombudsmanden, at virksomheden var ansvarlig for den ulovlige markedsføring.

Læs pressemeddelelsen fra forbrugerombudsmanden her: https://forbrugerombudsmanden.dk/find-sager/sager/markedsfoeringsloven/sager-efter-markedsfoeringsloven/spam/deltagerkrav-i-konkurrencer-paa-sociale-medier-i-strid-med-spamforbuddet/

Illustrasjon: Colourbox.com

Forbrugerombudsmanden indskærper vildledningsforbud over for en rengøringsvirksomheds brug af Fødevarestyrelsens elitesmiley

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) har i en afgørelse af 21. august 2024 indskærpet et vildledningsforbud overfor en rengøringsvirksomhed under sagsnummer 24/05966.

Forbrugerombudsmanden havde fået oversendt en klage fra den danske Fødevarestyrelse (»Fødevarestyrelsen«) vedrørende rengøringsvirksomhedens brug af Fødevarestyrelsens elitesmiley til markedsføring på et køretøj. Senere fandt Forbrugerombudsmanden, at Elitesmileyen også blev anvendt på rengøringsvirksomhedens hjemmeside. Markedsføringen var rettet mod andre erhvervsdrivende.

Forbrugerombudsmanden fandt, at markedsføringen var vildledende og i strid med den danske markedsføringslov, jf. lovbekendtgørelse nr. 866 af 15. juni 2022, § 20, stk. 1, om vildledende handelspraksis, da rengøringsvirksomheden gav andre erhvervsdrivende og konkurrenter indtryk af, at rengøringsvirksomheden i sin helhed efterlevede Fødevarestyrelsens kvalitetsmæssige krav eller var kvalitetskontrolleret hos Fødevarestyrelsen. Endvidere var det Forbrugerombudsmandens opfattelse, at elitesmileyen anses som et kvalitetsmærke, der generelt giver et positivt indtryk af en virksomhed i forbindelse med håndteringen af fødevarer.

Forbrugerombudsmanden bemærkede, at rengøringsvirksomheden ikke kunne tildeles en elitesmiley, da rengøringsvirksomheden hverken var en fødevarevirksomhed eller forhandler af fødevarer.

Læs pressemeddelelsen fra Forbrugerombudsmanden her: https://forbrugerombudsmanden.dk/find-sager/sager/markedsfoeringsloven/sager-efter-markedsfoeringsloven/miljoeogetik/2405966-et-rengoeringsfirma-fik-indskaerpet-forbuddet-mod-vildledende-markedsfoering-mellem-erhvervsdrivende-for-uberettiget-brug-af-foedevarestyrelsens-elitesmiley/

Tue Goldschmieding, partner i Gorrissen Federspiel og dansk redaktør for Lov & Data.

Bird & Bird

Gunnar Hjalt

Upphävd varumärkesregistrering på grund av otillbörlig avsikt

Patent- och marknadsöverdomstolen (PMÖD) har bekräftat ett upphävande i lägre instans av en varumärkesregistrering på grunden att varumärkesansökan gjorts i ond tro.

Enligt 2 kap. 7 § varumärkeslagen får ett varumärke inte registreras om ansökan gjorts i ond tro men lagtexten utvecklar inte vad som menas med ond tro vilket medför att domstolspraxis får stor betydelse för förståelse av begreppet.

Illustrasjon: Colourbox.com

Vid bedömningen av om sökanden agerat i ond tro konstaterade PMÖD att enbart vetskap om att en tidigare samarbetspartner hade använt ett varumärke (i det här fallet GULDRUTAN för kaffe) under lång tid i sig inte utgjorde ond tro. Sökandens avsikt måste också utredas. PMÖD konstaterade i det här målet bland annat att ansökan om varumärkesregistrering hade gjorts kort efter att sökandens tidigare samarbetspartner, som sedan länge använt sig av kännetecknet för sina egna produkter, gått i konkurs. PMÖD ansåg att sökanden genom sin ansökan hade agerat illojalt gentemot sin tidigare samarbetspartner och mot en eventuell förvärvare av varumärket från konkursboet eftersom en varumärkesansökan syftar till att förhindra för andra. Domstolens bedömning var alltså att ansökan hade skett med en otillbörlig avsikt och därmed i ond tro.

Se avgörandet i dess helhet här: https://www.domstol.se/globalassets/filer/domstol/patentochmarknadsoverdomstolen/avgoranden/2024/pma-4662-24.pdf

Gunnar Hjalt, Senior Counsel, Bird & Bird Advokat.


Selmer
Thea Kjølø og Øystein Kolstad Kvalø

Nye dommer om IT-kontrakter

De siste månedene er det avsagt to nye dommer om IT-kontrakter. I denne artikkelen redegjør vi kort for saksforholdene og resultatene i disse to dommene. Avslutningsvis gir vi en kommentar om hva man kan ta med seg fra disse for å unngå å havne i tilsvarende tvister.

Fell mot Geta

25. juni 2024 avsa Buskerud tingrett dom i saken mellom Fell Technology AS («Fell») og Geta AS («Geta»). Saken gjaldt krav fra Fell om rettmessig heving av kontrakt og restitusjon/erstatning, og motkrav fra Geta om betaling av ubetalte fakturaer og avtalt lisens.

Fell utvikler teknologi for maritime og landbaserte tjenester. Selskapet engasjerte IT-konsulentselskapet Geta for å etablere en e-handelsløsning for sin virksomhet. Det ble inngått en rammeavtale og gjennomført en innsiktsstudie, og deretter inngått arbeidsordrer for de ulike systemene i Fells ønskede e-handelsløsning. Leveransene skulle baseres på Getas «out of the box» e-handelsløsning, men måtte tilpasses Fells behov. Hoveddelen av løsningen var ferdigutviklet før partene inngikk avtale, og andre kunder av Geta brukte allerede systemet. Avtalen skisserte levering ved starten av tredje kvartal 2022, og arbeidet ble påbegynt i september 2021.

Det ble inngått totalt åtte arbeidsordrer under rammeavtalen. De seks første gjaldt arbeid med oppstart i september 2021, og for disse var det estimert at Geta skulle fakturere rundt kr 2,6 millioner. Per februar 2022 hadde Geta fakturert om lag kr 2,8 millioner, per april 2022 var beløpet steget til om lag kr 3,2 millioner, og i oktober 2022 hadde Geta fakturert for om lag kr 6,8 millioner. Totalsummen gikk altså langt utover det som var estimert.

Store deler av uenigheten mellom partene knyttet seg til de to siste arbeidsordrene som ble inngått våren 2022. Den første av disse arbeidsordrene, inngått mars 2022, gjaldt innleie av én konsulent fra Geta i 95 % stilling. For denne arbeidsordren ble det fakturert om lag kr 1,3 millioner for arbeid utført fra mars til oktober 2022. Den andre arbeidsordren, inngått i juni 2022, gjaldt et kjerneteam Geta stilte til Fells disposisjon med en arbeidsinnsats opptil 250 %. For denne arbeidsordren ble det fakturert om lag kr 1,7 millioner for arbeid fra juni til oktober 2022.

I juni 2022 nedjusterte Fell ressursbruken fra Geta. Fell sa opp arbeidsordre åtte om kjerneteam, og i oktober 2022 varslet Fell at Geta måtte stanse alt arbeid.

Fell mente at Geta hadde misligholdt avtalen ved å ikke levere komplette systemer innen avtalte frister, levere mangelfulle systemer og overskride kostnadsestimater. Fell mente at de hadde hevet alle avtaler med Geta høsten 2022, og krevde erstatning for både betalte og ubetalte fakturaer, lisenskostnader og eget arbeid.

Geta på sin side anførte for retten at de hadde utført arbeid som avtalt og løpende levert sine leveranser høsten 2021 og våren 2022. Ifølge Geta gjaldt de to siste arbeidsordrene ikke arbeid på prosjektet som opprinnelig var avtalt høsten 2021, men arbeidsordre som ble inngått fordi Fell ikke hadde kompetanse til å gjøre sin del av leveransen. Geta mente det ikke var noen forsinkelse, at en eventuell forsinkelse skyldtes Fell, og at Fell i alle tilfeller ikke hadde hevet avtalen innen rimelig tid. Geta fremmet motkrav på betaling for utført arbeid og betaling av avtalte lisenskostnader.

Retten kom til at Geta hadde levert et komplett system til Fell innen en rimelig tidsramme, gitt omstendighetene. Retten fant at Fell ikke hadde medvirket tilstrekkelig: Det var en felles forventning om at Fell hadde kompetanse til å utføre sin del av avtalen ved avtaleinngåelsen i september 2021, og gjennom innsiktsrapporten i 2021 hadde Fell også fått informasjon om hva dette bestod i. Det viste seg at Fell ikke hadde den riktige kompetansen til å oppfylle sine forpliktelser under avtalen. I tillegg hadde Fell også meldt inn endrede behov og prioriteringer underveis i utviklingsperioden, og dette tilsa også Fell hadde medvirket til forsinkelsen. Retten konkluderte

med at Fell ikke hadde sannsynliggjort at Geta hadde brutt sine plikter etter avtalen, og at det ikke forelå mislighold. På denne bakgrunn ble Geta frifunnet for hovedkravet.

Når det gjaldt Getas motkrav, ga retten delvis medhold. Fell ble dømt til å betale for tilnærmet alt arbeid utført og lisenskostnader, med unntak for en liten del av arbeidet som ikke var godkjent av Fell.

Ycom mot Kirkvaag

3. oktober 2024 avsa Oslo tingrett dom i saken mellom Ycom Norway AS («Ycom») og Alexander Nord Kirkvaag/Kirkvaag Venture ENK («Kirkvaag»). Saken gjaldt oppgjør etter kontraktsforhold om utvikling av en nettside/mobilapp. Ycom fremmet krav om betaling av vederlag for IT-løsningen, og Kirkvaag fremmet motkrav som i hovedsak gjaldt erstatning grunnet mislighold fra Ycoms side.

Ycom og Kirkvaag inngikk 22. oktober 2021 avtale om et forprosjekt for utvikling av en nettside, www.festportalen.no. I tillegg til avtalen om forprosjektet, inngikk partene en samarbeidsavtale, en databehandleravtale og en avtale om hosting og vedlikehold. Etter forprosjektet fikk Kirkvaag tilbud fra tre ulike leverandører på utvikling av løsningen. Ycom var ikke billigst, men valgte å matche det laveste tilbudet og fikk kontrakten. En ny oppdragsavtale ble inngått 21. desember 2021. De øvrige avtalene, nevnt ovenfor, ble videreført. For retten var sentrale temaer hva Ycom skulle levere, til hvilken tid, og når betaling kunne kreves.

I oppdragsavtalen var varighet angitt fra 15. desember 2021 til 31. mars 2022. Når det gjelder hva som skulle leveres fulgte det av pkt. 5 i avtalen at «Endelig produkt regnes som en Beta versjon og vil være gjenstand for Bugfix en gitt periode etter overlevering/implementering». Ved oppstart av prosjektet skulle Kirkvaag betale en fastpris på kr 250 000. De første seks månedene etter «lansering» skulle Kirkvaag betale kr 1200 per måned, og de neste 30 månedene kr 8640 per måned.

Arbeidet startet opp, og pågikk utover vinteren 2022. I mars ble det klart at løsningen ikke ville være klar innen utløpet av måneden, og 15. mars varslet Kirkvaag at han ville få noen andre til å ta over oppdraget. A2N Digitalbyrå ble engasjert. Selskapet ønsket tilgang til Ycoms kildekode, noe de ikke ønsket å gi fra seg før oppdraget var fullført og betalt.

Kirkvaag engasjerte advokat, og sendte så søksmålsvarsel til Ycom 7. april. Brevet ble besvart 12. april hvor Ycom estimerte at de kunne levere prosjektet 22. april, med den presisering at dette ville være en betaversjon, med henvisning til avtalen. Prosjektet ble levert 22. april, og i den påfølgende perioden, april til juni, var det en del korrespondanse mellom partene. Den 10. august 2022 skrev Ycom at de anså «alle punkter [som] korrigert og venter på bekreftelse fra Kirkvaag». Kirkvaag var derimot ikke enig i at løsningen var klar til bruk, og det var også uenighet om betaling av resten av vederlaget til Ycom. Kirkvaag hadde også overlatt ferdigstillelsen av portalen til A2N Digitalbyrå, og han mente løsningen ikke var klar for lansering. Av det som er opplyst om i saken fremgår det at Kirkvaag startet salg i januar 2023, som antageligvis innebærer at løsningen var lansert omkring samme tidspunkt.

Retten tok først stilling til hovedkravet. Ycom krevde betaling for resten av vederlaget i henhold til oppdragsavtalen, som totalt beløp seg til om lag kr 289 000 inkludert renter. Kirkvaag mente på sin side at det ikke var grunnlag for betaling utover det allerede betalte forskuddet på kr 250 000.

Retten gjorde en vurdering av avtalebestemmelsene i oppdragsavtalen supplert med det alminnelige kontraktsrettslige prinsippet om krav til «alminnelig god vare», og konkludere med at Kirkvaag skulle frifinnes for Ycoms krav om betaling av det resterende vederlaget. Retten fant ikke at Ycom ikke hadde sannsynliggjort at de hadde levert en løsning som Kirkvaag var forpliktet til å akseptere. Retten fant at Ycom var forpliktet til å levere en løsning som var klar til «lansering», slik ordlyden i bestemmelsen om betaling i avtalen lød, og at dette var noe annet enn levering. Ettersom Ycom aldri leverte en løsning som kunne lanseres offentlig hadde det ikke skjedd noen «lansering» i avtalens forstand. Det var derfor ikke grunnlag for å tilkjenne Ycom betaling utover det allerede betalte forskuddet.

I motkravet ble Ycom frifunnet for Kirkvaags erstatningskrav, da det ikke var sannsynliggjort at Kirkvaag hadde lidt et økonomisk tap. Retten vurderte at Kirkvaags utgifter til A2N Designbyrå ikke kunne anses som et tap, ettersom han ble fri for betalingsforpliktelsen overfor Ycom og utgiftene til A2N ikke oversteg det han ellers skulle betalt til Ycom.

Samlede sakskostnadskrav i saken var på rundt kr 1 250 000 inkl. MVA, og etter dommens resultat måtte hver av partene bære sine egne kostnader.

Hva kan vi lære av disse dommene?

Begge dommene gir verdifulle innsikter i hvordan kontraktsforhold og tvister ikke skal håndteres for å ende i retten. For ved tvister som disse kan det være fornuftig å vurdere minnelige løsninger fremfor langvarige og kostbare rettsprosesser.

Dommene understreker viktigheten av klare avtaler mellom kunder og leverandører av IT-tjenester, herunder bør det entydig spesifiseres hva som skal leveres, når det skal leveres og hvilke betingelser som utløser betaling i de enkelte

tilfellene. Som vi kan lese ut av dommen mellom Ycom og Kirkvaag ville dette redusert risikoen for misforståelser partene imellom, og uenighetene ville antageligvis ikke endt i retten.

I tillegg må begge parter være aktive og bidra til fremdriften i prosjektet. Manglende medvirkning kan føre til forsinkelser og utfordringer med leveransen, hvor dette, som vist i dommen mellom Fell og Geta, kan skyldes begge parter. I dette ligger det også forventningsstyring; fra tidspunkt for oppstart bør det være tydelig regulert hva som er inkludert i avtalen, hva som er tilleggstjenester og hva som forventes av den ene eller andre parten selv. Dommen mellom Fell og Geta viser også viktigheten av at kunden har et tilstrekkelig kompetent mottaksprosjekt på egen side som kan gjøre kundens del av arbeidet når slik medvirkning er avtalt.

Sentralt for reklamasjon og forsinkelse er også nødvendigheten av å sette realistiske frister som er dokumentert skriftlig og som begge parter er enige om. Partene bør også være forberedt på å justere tidslinjen ved behov, som for eksempel i dommen mellom Fell og Geta der Fell meldte flere endrede behov og prioriteringer som resulterte i misnøye og uenigheter. Kunden bør ha en bevissthet om at endrede behov og prioriteringer både kan føre til kostnadsoverskridelser og utsatt leveringstidspunkt.

Bevissthet om disse forholdene kan bidra til å redusere risikoen for tvister og sikre at kunden får riktig løsning til riktig tid. Dyre domstolsprosesser ender aldri godt for samarbeidet mellom partene, og i tvisten mellom Ycom og Kirkvaag endte sakskostnadene på et beløp godt over den samlede tvistesummen. Tydeligere avtaler mellom partene og en villighet til å komme til en minnelig løsning ville trolig gitt et mer fordelaktig resultat for begge parter.

Forfatterne er ikke kjent med hvorvidt dommene er rettskraftige.

Thea Kjølø. Advokatfullmektig. Thea bistår klienter med regulatoriske spørsmål innenfor blant annet teknologi, IP, digitalisering og personvern.

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

Illustrasjon: Colourbox.com

Gorrissen Federspiel

Tue Goldschmieding

To lovforslag i høring skal styrke det danske cybersikkerhedsniveau

Det danske Forsvarsministerium har sendt to lovforslag i høring, der implementerer to EU-direktiver. Forslagene er ikke i skrivende stund fremsat i det danske Folketing. Det foreslås, at begge love skal træde i kraft 1. marts 2025.

Det første lovforslag i høring er forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, som implementerer Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (»NIS 2-direktivet«). NIS2-direktivet har til formål at styrke cybersikkerheden og skabe et mere ensartet cybersikkerhedsniveau på tværs af medlemsstaterne ved eksempelvis at stille cybersikkerhedskrav til virksomheder, myndigheder og organisationer på tværs af samfundskritiske sektorer.

Den andet forslag i høring er forslag til lov om kritiske enheders modstandsdygtighed, som implementerer Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 af 14. december 2022 om kritiske enheders modstandsdygtighed og om ophævelse af Rådets direktiv 2008/114/EF (»CER-direktivet«). CER-direktivet supplerer NIS2-direktivet og gælder ikke forhold omfattet af NIS2-direktivet. CER-direktivet har til formål at styrke kritiske enheders modstandsdygtighed i samfundsvigtige sektorer. Hvis en enhed identificeres som kritisk efter CER-direktivet, er enheden også omfattet af NIS2-direktivet.

CER-direktivet pålægger medlemsstaterne at udarbejde nationale strategier til styrkelse af kritiske enheders modstandsdygtighed. Lovforslaget pålægger de relevante danske ressortministerier at identificere kritiske enheder, sikre modstandsdygtighed og tilsyn i de forskellige sektorer. Den danske Beredskabsstyrelse får dog en tværgående rolle til at facilitere et samarbejde på tværs af sektorerne.

Lovforslagene til implementering af henholdsvis NIS 2-direktivet og CER-direktivet sendt til høring kan findes her:

https://hoeringsportalen.dk/Hearing/Details/68921

https://hoeringsportalen.dk/Hearing/Details/68920

Tue Goldschmieding, partner i Gorrissen Federspiel og dansk redaktør for Lov & Data.

Illustrasjon: Colourbox.com

LOVDATA

Produksjon: Aksell AS