

# Lov & Data

September 2024

Nr. 159 3/2024



## Innhold

Leder .....	2
Viveca Still	
Lov & Data breder ut sig till Finland	

## Artikler

Jaakko Lindgren og Sohrab Känkänen A brief history of data breaches in Finland from Vastaamo to City of Helsinki. ....	4
Nicholas Foss Barbantonis, Fabian Bjørnstad og Camilla Hagelien Norsk rett møter Baby Reindeer .....	6
Boris Melvås En definition av ett AI-system utifrån matematiska modeller av inlärning. ....	12
Lars Arnesen Harmoniserte standarder: En ny sentral rettskilde i kommende regulering av kunstig intelligens .....	16
Veronika Lundqvist og Haakon Føyen Fra åndsverk til algoritme: Navigering av oppavsrett i KI-alderen .....	21
Gaëlle Bjurström Mot ett starkare skydd för den enskildes integritet ..	27
Julia D. Fuglestad Brodshaug og Simen Hafstad-Moi Pasientens rett til informasjon ved bruk og utvikling av kunstig intelligens i helsehjelp .....	30
Ida Thorsrud Innsyn i klasselister er i strid med GDPR .....	33
Stein Schjøberg FN-konvensjon om cyberkriminalitet .....	38
JusNytt .....	41
Halvor Manshaus:	
Rettsinformatisk litteratur .....	44
Nytt om personvern .....	46
Nytt om immaterialrett .....	51
Nytt om IT-kontrakter .....	59
Annet nytt .....	61

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

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

**Ansvarlig redaktør** er Sara Habberstad  
**Medredaktør** er Trine Shil Kristiansen,  
Lovdata.

**Redaktør** for Danmark er  
Tue Goldschmieding, partner i firmaet  
Gorriksen Federspiel, København.

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

**Redaktør** for Finland er Viveca Still,  
Ministry of Education and Culture

**Fast spaltist** er Halvor Manshaus,  
partner i advokatfirmaet Schjødt.

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



# Leder

## Lov & Data breder ut sig till Finland

Den finske IT-rettslige foreningen (IT-oikeuden yhdistys) har besluttet å anta Lov & Data som medlems-tidning från och med detta år. Det kan dermed vara på sin plass å kort presentere foreningen.

Startskottet for det som idag heter IT-rettslige foreningen lades då Ritva Juntunen, som var både jurist og informatiker, samman-kallade ett antal personer som var interesserte av rettslige spørsmål og samman-kopplade med automatisk databehandling til ett møte. Den ADB-rettslige foreningen (ATK-oikeudellinen yhdistys) grundades år 1985, og firar alltså sitt fyrtynde jubileumsår inkommande år, 2025. Foreningens første ordförande var Jukka Liedes, sedermera direktör og långvarig tjänsteman på Undervisning- og kulturministeriet ansvarig for opphovsrätt. Ända sedan start kom foreningen att formas av behovet bland framför allt praktiserande jurister og tjenstemän att diskutera IT-rettslige spørsmål og framställningar.

Inom den akademiska världen var interessen blant de etablerte forskarna svalt for dessa nye spørsmål, forutom vid Lapplands universitet, där professor Ahti Saarenpää gikk i bräsch for forskningen i rettsinformatikk. Idag finns det en allstärkere IT-rettslig forskning inom de finske universitetene.

Efter att ha fört en tynande tillvaro några år på 1990-talet återuppväcktes verksamheten og fikk sig en rivstart i og med den begynnan-



Viveca Still

de boomen inom IT-industrin. I början av 2000-talet moderniserade man navnet, så att foreningen idag heter IT-rettslige foreningen (IT-oikeuden yhdistys).

Foreningen är idag en mycket aktiv forening med over 700 medlemmer. Foreningens verksamhet består i hovedsak av diskussionstillfällen kring IT-rettslige spørsmål og foretogsbesök. Forutom jurister är foreningen også öppen for enhver som interesserer sig for IT-rettslige spørsmål.

Samtidig som Lov & Data antas som medlemstidning for IT-rettslige foreningen börjar underteknet som redaktör for Finland, varfor det säkert är på sin plass med en kort introduktion.

Hela min yrkesverksamma tid har kretsat kring informationsretten. Redan år 1997 deltog jag under ledning av professor Ahti Saarenpää i skrivandet av en utredning for



Illustration: Colourbox.com

finansministeriet om behovet av datasäkerhetslagstiftning. Jag kom därefter att fundera vidare kring vad datasäkerhet betyder inom upphovsrätten, vilket ledde till en doktorsavhandling år 2007 kring elektronisk rättighetshantering, DRM, och dess inverkan på upphovsrättens balans.

Faktiskt hade IT-rätten betydelse redan under studietiden, eftersom jag skrev min pro gradu-avhandling om polisens undercovermetoder, inklusive teknisk övervakning (1997). Jag deltog också som troligtvis den första juridikstuderanden i Finland i en webbkurs. Det var en webbkurs i rättsinformatik som ordnades av Saarbrücke universitet år 1995.

År 1999–2003 fungerade jag som ansvarsperson för rättsinformatik

vid Helsingfors universitet. Praktisk erfarenhet av IT-rätten fick jag då jag arbetade med kommersialisering av innovationer för ett konsortium av sex universitet inom konst-, medie- och tekniksektorn under åren 2003–2008. Från och med 2008 arbetade jag på undervisnings- och kulturministeriet med upphovsrättsliga frågor fram till år 2022, då jag övergick i finansministeriets tjänst, där jag numera verkar som lagstiftningsråd på enheten för informationspolitik och i första hand är sysselsatt med frågor kring digitalisering av myndighetsverksamhet.

Lov & Datas läsare kommer alltså så småningom att få en allt bättre inblick i vad som sker även i Finland. I detta nummer publiceras en

intressant artikel av en av Finlands främsta IT-rättsliga experter, advokat Jaakko Lindgren, om det sk. Vastaamo-fallet, där man lugnt kan säga att datasäkerheten fallerade med katastrofala följder för psyko-terapicentralen Vastaamos patienter.

*Namn:* Viveca Still

*Titel:* Juris doktor, lagstiftningsråd

*Arbetsplats:* Finansministeriet / enheten för informationspolitik

*Doktorsavhandling:* DRM och upphovsrättens obalans (2007)

Viveca Still

# A brief history of data breaches in Finland from Vastaamo to City of Helsinki

Av Jaakko Lindgren og Sohrab Känkänen

Data breaches have been a hot topic in Finland recently, with the data breach suffered by the City of Helsinki on April 30th being the largest in Finland's history according to current information. Additionally, the Vastaamo case, previously the largest data breach in Finland, received its first court ruling from the District Court of Western Uusimaa on the same day as the City of Helsinki breach. It is evident that in an increasingly digital world, the volume of cybercrime is rising. The fact that two of the largest data breaches in Finland occurred so close to each other is certainly noteworthy. The timing of these breaches suggests a pattern of negligence in the data security field in Finland. The big question is what circumstances create such vulnerabilities, and what can we learn from them to prevent future breaches. As the City of Helsinki data breach is still under investigation, this article will cover only the details of the Vastaamo case.

” The big question is what circumstances create such vulnerabilities, and what can we learn from them to prevent future breaches.

The Vastaamo case involved the data breach of over 30,000 psychotherapy patients admitted to Vas-



*Jaakko Lindgren*

taamo Psychotherapy Center. Cybersecurity-wise, the Vastaamo case was essentially a catastrophe waiting to happen. The baseline protection for the Vastaamo database was virtually non-existent. On top of this, the company was revealed to have wildly disregarded their obligations to ensure adequate levels of data protection under the GDPR. According to the court ruling, the patient database was public and accessible by anyone for at least 17 months, from November 2017 to March 2019. During this time, access to the database was possible without a password. Additionally, Vastaamo did not become aware of the breach until September 2020, when the attacker made contact with them. This demonstrates that very little was done in terms of internal cybersecurity audits, and the non-actions were grossly negligent. The forensic investigation revealed that the data breach most likely occurred within a four-minute window. It took just four minutes



*Sohrab Känkänen*

for what was then the largest data breach in Finland to happen, resulting in 30,000 people losing their sensitive patient histories and other personal data.

Even in light of these major deficiencies, it is hard to grasp how much of a disaster the entire case truly was, with the complete lack of cybersecurity measures, audits and procedures being the catalyst for a plethora of problems. Preceding the police investigations, but after the data breach, Vastaamo was sold to a Intera Partners holding company. After the police investigations began, the holding company commenced legal proceedings against Vastaamo on the grounds that the acquisition would not have taken place if they had known about the breach. During the trial, the CEO denied knowing about the breach and even tried to shift the blame from himself to his employees, claiming that the employees withheld the information about the breach. A total of nearly 10 million

euros of assets of the then-CEO of Vastaamo were seized as part of the legal action. The actual termination of the acquisition was settled through arbitration, resulting in the defendant having to pay 8 million euros in damages to the holding company. The CEO of Vastaamo was charged with three months of probation from a data protection offence. Also, the business of Vastaamo was later sold to another company, and Vastaamo itself declared bankrupt.

The magnitude and rapidity of the Vastaamo case could be partly attributed to the centralized information system on which the database was based. Centralized information systems are arguably more susceptible to cybercrime than their decentralized counterparts. As societies become increasingly digital and global data masses increase in volume and speed of flow, it is logical that data breaches will also grow directly proportional to the sizes of databases. Centralized information systems face significant difficulties when dealing with security issues.

The Vastaamo ruling was given solely on the criminal procedure related to the case, as the related civil claims were so massive that they re-

quire their own trial. While the civil side of the case is still pending a court date, the criminal ruling is also still unsolved as it has yet to reach force of law due to the defendant expressing his discontent on the District Court judgment. Getting a second ruling from the Court of Appeals may take another few years, and even then, force of law may not yet be achieved, as a possibility for the case to be brought before the Supreme Court of Finland remains. As a landmark case in Finland, the possibility for a Supreme Court ruling is more likely than generally. In any case, it will still be another four to five years before we get a final say on the matter.

” In essence, a major shift in attitudes towards cybersecurity and data protection is necessary to prevent large-scale breaches.

The growth of data centrism presents other challenges as well, such as the increasing impact of human error. The Vastaamo case

was one of negligence, just like the recent case with the City of Helsinki, both resulting from human error. Moreover, the current political landscape provides fertile ground for foreign cyber operations, evidenced by the palpable increase in denial-of-service attacks and other interference. Hackers are also becoming increasingly talented, with younger generations surpassing older ones in efficiency at exploiting available technology.

In essence, a major shift in attitudes towards cybersecurity and data protection is necessary to prevent large-scale breaches. It is no longer feasible for organizations to compartmentalize or outsource IT matters with the expectation that cybersecurity can be ensured, fixed, or implemented as a “one-off” solution. Proper IT management requires constant attention on both an individual and collective level. Today, cybersecurity is no longer an issue solely for experts but a consideration for everyone.

*Jaakko Lindgren, Partner, Dottir Attorneys*

*Sohrab Känkänen, Associate, Dottir Attorneys*



Illustration: Colarbox.com

# Norsk rett møter Baby Reindeer

Av Nicholas Foss Barbantonis, Fabian Bjørnstad og Camilla Hagelien



Nicholas Foss Barbantonis



Fabian Bjørnstad



Camilla Hagelien

## 1. Innledning

Netflix-serien Baby Reindeer følger hovedpersonen Richard Gadd i en fiktiv utgave av seg selv og personforfølgeren «Martha» i hva Netflix hevder å være en «true story». Gjennom seriens syv episoder skildres «Martha» som en tidligere straffedømt «stalker»,<sup>1</sup> og serien viser hvordan hun skal ha personforfulget Gadd gjennom blant annet e-poster, tekstmeldinger og fysisk forfølgning. Serien har hatt over 88,4 millioner visninger og har generert over 9,5 milliarder dollar i inntekter for Netflix.<sup>2</sup> Serien har imidlertid blitt gjenstand for stor debatt.<sup>3</sup>

Kort tid etter utgivelsen ble «Martha» identifisert som skotske

Fiona Harvey.<sup>4</sup> Harvey tok ut søksmål mot Netflix i juni 2024, med krav om erstatning, «punitive damages», menerstatning, og oppreisning på totalt flere hundre millioner dollar.<sup>5</sup> De aktuelle ansvarsgrunnlagene er æreskrenkelse, forsettlig skade av psykologisk art, uaktsomhet, grov uaktsomhet og retten til personlig særpreg i henhold til kalifornisk lov og rettspraksis.

I denne artikkelen analyserer vi hvordan denne saken kunne utspilt seg i et norskrettslig perspektiv. Vi har tatt utgangspunkt i reglene om æreskrenkelse, krenkelse av privatlivets fred og prinsipper for vurdering og utmåling av erstatnings- og oppreisningskrav. Saken aktualiserer for øvrig spørsmål tilknyttet personvernreglene og journalistfritaket i personopplysningsloven § 3, samt reglene om villedende markedsføring. Dette er imidlertid spørsmål

som ikke vil bli behandlet i denne artikkelen.

” I denne artikkelen analyserer vi hvordan denne saken kunne utspilt seg i et norskrettslig perspektiv. Vi har tatt utgangspunkt i reglene om æreskrenkelse, krenkelse av privatlivets fred og prinsipper for vurdering og utmåling av erstatnings- og oppreisningskrav.

1 Stalker og personforfølger brukes synonymt i denne artikkelen.

2 Se: [https://s22.q4cdn.com/959853165/files/doc\\_financials/2024/q2/FINAL-Q2-24-Shareholder-Letter.pdf](https://s22.q4cdn.com/959853165/files/doc_financials/2024/q2/FINAL-Q2-24-Shareholder-Letter.pdf) (nedlastet 16.08.2024).

3 Se: <https://www.nrk.no/kultur/kvinnesom-bevder-a-vaere-virkeligbetens-martha-i-baby-reindeer-saksoker-netflix-for-1-8-milliarder-1.16915765> (nedlastet 16.08.2024) og <https://d18rn0p25nvr6d.cloudfront.net/CIK-0001065280/d9ac401f-6967-4a26-868c-710952e5f3e0.pdf> (nedlastet 16.08.2024).

4 Se: <https://www.theguardian.com/tv-and-radio/article/2024/may/10/piers-morgans-baby-reindeer-interview-fiona-harvey-reeked-grubby-exploitation> (nedlastet 16.08.2024).

5 Stevningen er tilgjengelig her: <https://fingfx.thomsonreuters.com/gfx/legal-docs/zjpaqyemhpx/Baby%20reindeer%20complaint.pdf> (nedlastet 16.08.2024).

Gadd.<sup>6</sup> Påstandene blir tydelig presentert og gjentatt flere ganger i serien, og det etterlates ingen tvil om deres innhold. Et annet sentralt aspekt i saken er at seriens første episode innledes med setningen «*[t] his is a true story*». Mye av seriens markedsføring har også sentrert seg rundt nettopp denne formuleringen.

Netflix og Gadd har bekreftet at den virkelige inspirasjonen bak «Martha» aldri ble dømt for straffbare forhold.<sup>7</sup> Hun var imidlertid underlagt et trakasseringsvarsel, eller såkalt «*first instance harassment warning*».<sup>8</sup> Selv om Netflix har erkjent at Harvey var inspirasjonen bak «Martha»,<sup>9</sup> har Gadd opprettholdt anførselen om at serien er basert på hans egne følelser og minner, og at den ikke er ment å fremstille noen virkelige personer.<sup>10</sup> Serien har ifølge Gadd som formål å vise hans utfordringer med seksuelt misbruk, manipulasjon, utnyttelse, besettelse, seksuell identitet, selvforakt, selvdestruksjon og selvpoppdagelse.<sup>11</sup> Allikevel bruker han nærmere 20 sider på å forsvare at historien er basert på faktiske for-

hold Gadd ble utsatt for av Harvey i 2015.<sup>12</sup> Gadd forteller om voldshendelser og seksuelt misbruk og har lagt frem tusenvis av e-poster og telefonbeskjeder med seksuelt eksplisitt, voldelig og nedsettende innhold, hatytringer og trusler, som er blitt overgitt til politiet.<sup>13</sup> Han har også lagt ved bevis på dialog med politiet og trakasseringsvarselet mot Harvey, samt bevis på tidligere forfølgelse av andre.<sup>14</sup>

Det er imidlertid ikke lagt frem bevis på verken det seksuelle overgrepet som vises i serien, eller at Harvey har forfulgt en politimann.

### 3. Ærekrenkelser etter norsk rett

#### 3.1 Oversikt

Forutsatt at en domstol fastslår at Harvey kan identifiseres som «Martha» oppstår spørsmålet om serien medfører at Harvey ærekrenkes. Å introdusere Baby Reindeer som en «*sann historie*» skaper en viss forventning hos seeren om at forholdene er representativt for forholdet mellom Gadd og Harvey. Dette vil også kunne ha en side mot markedsføringslovens bestemmelser om urimelig handelspraksis og villedende handlinger, jf. markedsføringsloven §§ 6 og 7. Dette er imidlertid utenfor rammen for denne artikkelen.

#### 3.2 Skadeserstatningsloven § 3-6 a

Etter skadeserstatningsloven § 3-6 a er den som «*uaktsomt*» har satt frem en «*ytring som er egnet til å krenke en annens ærefølelse eller omdømme*» erstatningsansvarlig for «*den lidte skade og slik erstatning for tap i fremtidig erverv som retten ut fra den utviste skyld og forholdene ellers finner rimelig*». Ærekrenkelse var tidligere regulert i straffeloven av 1902 kapittel 23. Når bestemmelsen ble flyttet til skadeserstatningsloven ble skyldkravet også nedjustert til uaktsomhet,

12 Ibid.

13 Ibid.

14 Ibid side 17 og 18.

både for fremsettelsen av ytringen og ved vurderingen av om innholdet er ærekrenkende.

Etter bestemmelsens annet ledd kan det gjøres unntak for ærekrenkende ytring som anses «*berettiget etter en avveining av de hensyn som begrunner ytringsfrihet*». Unntaket viser hvordan bestemmelsen er en balanse mellom grunnleggende rettigheter.

Skadeserstatningsloven § 3-6 a bygger på veletablert praksis fra Høyesterett og EMD, og reflekterer i all hovedsak de momenter som er blitt lagt til grunn her. Det klare utgangspunkt etter norsk rett er ytringsfrihet etter Grunnloven § 100, og vurderingen av om det foreligger en ulovlig ærekrenkelse beror på tre primære spørsmål, nemlig «*hvordan det aktuelle utsagnet skal tolkes, om utsagnet er ærekrenkende og om det er rettsstridig*».<sup>15</sup>

#### 3.3 Tolkningen av ytringene

En ytring skal tolkes i lys av hvordan den ville blitt oppfattet av en ordinær person, hvor det sentrale er ytringens innhold og kontekst.<sup>16</sup> Det må både ses hen til det enkelte utsagn og, dersom flere, hvilken betydning disse må tillegges sett i sammenheng.<sup>17</sup> Når det gjelder innholdet, skal det mer til for at verdipregede ytringer er rettsstridige enn ytringer om et faktisk forhold. Riktignok forutsetter dette at det

15 Rt-2014-1170 (avsnitt 90). Se også Rt-2015-746 (avsnitt 52 flg.) og LE-2019-190039.

16 Rt-2014-1170 (avsnitt 92), Rt-2014-152 (avsnitt 115) og Rt-2015-746 (avsnitt 48). Se også Ovchinnikov mot Russland, 16. desember 2010 (avsnitt 53) EMD-2004-24061, Tønsberg Blad AS mfl. mot Norge, 1. mars 2007 EMD-2004-510 (avsnitt 90), samt Erla Hlynsdóttir mot Island 10. juli 2012 EMD-2010-43380 (avsnitt 62).

17 Rt-2014-1170 (avsnitt 92),

6 Harvey v Netflix (avsnitt 28).

7 Se: <https://www.hollywoodreporter.com/tv/tv-news/netflix-letter-baby-reindeer-stalker-fiona-harvey-richard-gadd-1235962991/> (nedlastet 16.08.2024) og <https://s3.documentcloud.org/documents/25020581/gadd-declaration-harvey-lawsuit.pdf> (nedlastet 16.08.2024).

8 Såkalte first instance harassment warnings ble tidligere brukt av britisk politi som et administrativt middel for å håndtere trakasseringsanklager, se for øvrig <https://s3.documentcloud.org/documents/25020581/gadd-declaration-harvey-lawsuit.pdf> side 17 (nedlastet 16.08.2024).

9 Se: <https://www.hollywoodreporter.com/tv/tv-news/netflix-letter-baby-reindeer-stalker-fiona-harvey-richard-gadd-1235962991/> (nedlastet 16.08.2024).

10 Se: <https://s3.documentcloud.org/documents/25020581/gadd-declaration-harvey-lawsuit.pdf> side 2 flg. (nedlastet 16.08.2024).

11 Ibid side 3 flg.

ikke foreligger tilstrekkelige holdpunkter for det faktiske forholdet.<sup>18</sup>

Serien er fremstilt som en «*sammehistorie*». Flere vesentlige deler av serieinnholdet er også dokumentert uriktig, og kan heller ikke bortforklares av Gadd/Netflix. Vår vurdering er derfor at en alminnelig seer sannsynligvis vil tolke innholdet i serien slik at Harvey faktisk har begått disse handlingene.

### 3.4 Om ytringen er egnet til å krenke en annens æresfølelse og omdømme

Begrepet «*æresfølelse*» tilsier en persons selvrespekt og opplevelse av verdighet, mens omdømme handler om andres oppfatning og personrykte. Som utgangspunkt vil en ytring i strid med § 246 («*krenker en annens æresfølelse*») eller § 247 («*skade en annens gode navn og rykte eller til å utsette ham for hat, ringeakt eller tap av den for hans stilling eller næring fornødne tillit*») av straffelovens av 1902 gi klar indikasjon på at det foreligger en ærekrenkende ytring.<sup>19</sup> Likevel understrekes det i forarbeidene at det er rettsgodene som er vernet, altså æresfølelse og omdømme, og det kan neppe oppstilles et faktisk krav om overskridelse av gjerningsbeskrivelsene.<sup>20</sup>

Anklager om lovbrudd er egnet til å skade ens æresfølelse og omdømme, men ikke alltid.<sup>21</sup> Det er imidlertid lite tvil om at slike beskyldninger som lagt frem i serien, om alvorlige lovbrudd som grov forfølgning og seksuelt overgrep, vil kunne skade en persons æresfølelse og omdømme.<sup>22</sup>

### 3.5 Om den krenkende ytringen

#### er rettsstridig

Spørsmålet om ytringen er rettsstridig etter skadeserstatningsloven § 3-6 a annet ledd handler om ytringen likevel er rettmessig etter en avveining av de hensynene som begrunner ytringsfriheten. Det kreves en helhetlig balansering av de motstridende rettighetene for å sikre en rettferdig avveining.<sup>23</sup>

I vurderingen av rettsstrid skal det etter skadeserstatningsloven § 3-6 a annet ledd andre punktum særlig legges vekt på «*om ytringen hviler på et fyldestgjørende faktisk grunnlag, på ytringens grad av krenkelse, og om hensynet til den krenkede er tilfredstillende ivare tatt ved for eksempel adgang til imotegåelse, om allmenne interesser eller andre gode grunner tilsa at den ble satt frem, og om ytreren har vært i aktsom god tro med hensyn til de momenter som kan gjøre ytringen berettiget*». Bestemmelsen er langt på vei en kodifisering av Høyesteretts praksis til bestemmelsene i den gamle straffeloven.<sup>24</sup>

Hvorvidt ytringen bygger på «*fyldestgjørende faktisk grunnlag*», tar utgangspunkt i om det på tidspunktet for ytringen var sannsynlighetsovervekt for at forholdet var sant.<sup>25</sup> Unntak gjøres dersom ytringen på dette tidspunktet var tilstrekkelig begrunnet, og om det var sterke hensyn som talte for rask offentliggjøring for å ivareta ytringsfrihetens formål.<sup>26</sup>

Det klare utgangspunktet er at sanne ytringer ikke er rettsstridige med mindre tunge argumenter tilsier at det vil medføre et uforholdsmessig inngrep i den omtaltes rettigheter.<sup>27</sup> Dette gjelder hovedsakelig for ytringer med et faktisk innhold, men også mer verdipregede ytringer.<sup>28</sup> Ifølge EMD er verdibaserte ytringer en fundamen-

tal del av ytringsfriheten og baserer seg på tanken om at alle innehar en rett til å ha en mening.<sup>29</sup> Høyesterett har uttalt at usanne ærekrenkende uttalelser om faktiske forhold som klar hovedregel ikke er beskyttet etter ytringsfriheten.<sup>30</sup>

Allmenn interesse vil være det sentrale momentet for å beskytte en æreskrenkelse på bekostning av rettigheter som retten til privatliv etter Grunnloven § 102 og EMK art. 8.<sup>31</sup> Særlig gjelder dette ytringer som berører sosialt viktige forhold, som politikk eller maktkritikk, men også ytringer om straffbare forhold kan anses som av allmenn interesse.<sup>32</sup>

Dette momentet vil stå sentralt i saken mellom Harvey og Netflix dersom skadeserstatningsloven § 3-6 a skulle komme til anvendelse. Som nevnt innledningsvis, har ikke Netflix fremlagt faktiske grunnlag for de tre påstandene i serien som er løftet frem i søksmålet. Et sentralt spørsmål vil trolig være om de hendelsene Harvey faktisk har begått, selv om de fant sted under andre omstendigheter enn de fremstilt i serien, kan forsvare ytringene.

På den ene siden kan det hevdes at hvis serien skildrer faktiske hendelser, har den en viss berettigelse og offentlig interesse. Offentligheten kan ha rett til å bli informert om slike handlinger, spesielt dersom de utgjør en fare for andre eller representerer en form for samfunnsskadelig atferd. På den andre siden må man vurdere om serien gir en sannferdig og balansert fremstilling, eller om den overdriver og fordreier virkeligheten på en måte som medfører urettmessig skade på Harveys omdømme og rykte. Selv om Harvey har begått handlinger som kan anses klanderverdige, innebærer ikke det at hun skal måtte godta

18 Ibid (avsnitt 105 flg) og Bjørnar Borvik, Personvern og ytringsfrihet, 2011 side 270.

19 Rt-2014-152 (avsnitt 99) og Ot.prp. nr.22 (2008-2009) side 488.

20 Ot.prp. nr.22 (2008-2009) side 488.

21 Ibid.

22 Ibid.

23 Se blant annet Rt-2014-152 (avsnitt 101 flg).

24 Se særlig Rt-2003-928 (avsnitt 44) og Rt-2015-152 (avsnitt 104).

25 Rt-2014-152 (avsnitt 110).

26 Ot.prp. nr.22 (2008-2009) side 489.

27 Ibid.

28 Ibid.

29 Lingens v. Austria fra 1986 (avsnitt 46).

30 Rt-2005-1677 (avsnitt 74) jf. Rt-2003-928 (avsnittene 41 og 57).

31 Ot.prp. nr.22 (2008-2009) side 489.

32 Ibid.



urettmessige ærekrenkelser. Dersom serien vesentlig overdriver eller legger til fiktive elementer som ikke reflekterer virkeligheten, kan dette utgjøre en krenkelse som ikke kan forsvares med henvisning til ytringsfriheten.

Videre bør det vurderes om ytringene primært tjener et underholdningsformål på bekostning av Harvey, eller om de bidrar til en samfunnsdebatt. Her er valget av medium av betydning og vil påvirke hvilke forventinger som kan stilles til sannferdigheten av ytringene.<sup>33</sup> Baby Reindeer er en dramaserie, ikke en dokumentar. Selve valget av medium tar et forbehold om historiens faktiske sannhet. Skuespillere fremfører en manusbasert historie, og det faktum at innholdet er dramatisert fjerner det et stykke fra en objektiv sannhet. Serien er fortellerens subjektive sannhet og hendelsesforløpet må først tolkes av fortelleren, deretter av skuespillerne, og til slutt av seeren. Seeren må derfor ha en viss forventning om at sannheten er noe fjern, selv om det påstås å være en sann historie.

Et annet viktig moment etter skadeserstatningsloven § 3-6 a annet ledd annet punktum, er om «*hensynet til den krenkede er tilfredsstillende ivare tatt ved for eksempel adgang til imøtegåelse*». Forarbeidene understreker at den som rammes av beskyldninger skal ha rimelig anledning til å korrigere eller imøtegå disse.<sup>34</sup> Imøtekommelsesplikten kan avhenge av den samlede virkningen av flere ytringer. For pressen er det også særlig viktig å sikre en balansert fremstilling, da ubalanserte reportasjer kan mangle tilstrekkelig faktisk grunnlag.<sup>35</sup> Det er uklart hvorvidt det kan stilles tilsvarende krav for innholdsprodusenter, som i tillegg til underholdning også sender faktaorientert materiale i form av serier

og dokumentarer. At serien ikke har noen isolert nyhetsverdi slik at det haster å publisere, noe som ofte vil prege journalistikk, kan være et argument for at Harvey skulle vært gitt adgang til imøtegåelse.

Endelig følger det av EMD-praksis at retten til privatliv kun kan forsvare inngrep i ytringsfriheten i tilfeller der angrep på en persons omdømme når en viss minsterskel. Man kan ikke vise til retten til privatliv for å klage over skade på omdømmet hvis denne skaden er en forutsigbar konsekvens av ens egne handlinger.<sup>36</sup> Dette kan også bli et relevant spørsmål i saken, da Netflix anfører at Harvey ikke kan påvise skade på sitt omdømme, da hennes omdømme allerede var skadet av tidligere nyhetsartikler om hennes tidligere personforfølgning av offentlige personer.<sup>37</sup>

Det endelige resultatet vil avhenge av en vurdering av hvorvidt seriens dramatiserte fremstilling, som Gadd og Netflix har innrømmet, respekterer grensen mellom ytringsfriheten og rettsstridig ærekrenkelse i lys av momentene behandlet over. I lys av det faktum som er kjent, mener vi at ærekrenkelsen trolig må anses rettstridig.

## 4. Om krenkelser av privatlivets fred

### 4.1 Oversikt

Søksmålet aktualiserer også problemstillinger tilknyttet det norske regelverket om krenkelse av privatlivets fred og retten til privatliv. Verket om privatlivets fred etter skadeserstatningsloven § 3-6 er nært tilknyttet retten til respekt for

privatliv som er grunnlovfestet i Grunnloven § 102 og inntatt i EMK artikkel 8.

## 4.2 Skadeserstatningsloven § 3-6

I henhold til skadeserstatningsloven § 3-6, skal den som «*uaktsomt har krenket privatlivets fred*» yte erstatning. Selv om erstatningskrav etter skadeserstatningsloven ikke anses som ileggelse av straff, er det lagt til grunn i rettspraksis at skadeserstatningsloven § 3-6 skal tolkes i lys av straffeloven § 267, hvis ordlyd er mer eller mindre sammenfallende.<sup>38</sup>

Hvorvidt det foreligger opplysninger som angår «*privatlivets fred*», vil være et spørsmål om hvorvidt «*det er tale om opplysninger med en viss grad av sensitivitet*».<sup>39</sup> En sak som kan gi en viss veiledning om dette spørsmålet er Rt-2010-258. Saken gjaldt spørsmål om krenkelse av privatlivets fred ved utgivelse av en lokalhistorisk bok om forfatterens eget småbruk. Deler av boken inneholdt opplysninger om forfatterens samliv med tidligere ektefelle, deres separasjon og øvrige opplysninger om «*ekteskapskrisen*». Den tidligere ektefellen mente at boken utgjorde en krenkelse av privatlivets fred. Retten kom til at det ikke var «*særlig tvilsomt*» at disse opplysningene omhandlet privatlivet, og selv om ikke alle opplysningene hadde personlig karakter, var «*helhetsinntrykket*» at det omhandlet tilstrekkelig personlige og sensitive forhold.<sup>40</sup>

## 4.3 Ville Baby Reindeer medført krenkelse?

I Baby Reindeer fremkommer det en rekke opplysninger som kan knyttes til Harvey og hennes forhold til Gadd, inkludert en del opplysninger som trolig kan belyse Har-

33 Rt-2014-152 (avsnitt 115).

34 Ot.prp. nr.22 (2008-2009) side 489.

35 Ibid. Se også Rt-2002-764 og Rt-2003-1190 (avsnitt 81).

36 EMDs dom av 7. februar 2012 Axell Springer AG mot Tyskland [EMD-2008-39954], Sidabras and Džiautas v. Lithuania, nos. 55480/00 and 59330/00, § 49, ECHR 2004-VIII) og Rt-2015-746 (avsnitt 72).

37 Se: <https://www.hollywoodreporter.com/tv/tv-news/netflix-letter-baby-reindeer-stalker-fiona-harvey-richard-gadd-1235962991/> (nedlastet 16.08.2024).

38 Se eksempelvis Rt-2007-687 (avsnitt 56), Rt-2010-258 (avsnitt 43), som begge er sivilrettslige saker, men anvender straffelovens forbud mot krenkelse av privatlivets fred.

39 Ot.prp. nr. 22 (2008-2009) side 150.

40 Rt-2010-258 (avsnitt 51).

veys psykiske helse. Selv om ikke alle opplysningene i serien kan anses å være sensitive, vil helhetsinntrykket trolig være at disse samlet omfattes av begrepet «*privatlivets fred*». Neste spørsmål blir da om det foreligger en krenkelse.

I begrepet «*krenkelse*» ligger det et krav om rettsstrid, som «*inneber at det må skje ei totalvurdering av formidlinga i lys av kontekst og situasjon, der omsynet til personvernet samtidig blir avvege mot yttringsfriheten*». <sup>41</sup> I denne avveiningen må det anvendes en objektiv norm, der personlige opplevelser til vedkommende er av mindre betydning. <sup>42</sup> Det skal vektlegges «*hvor nærgående og intim opplysningen er*», og «*om opplysningen er negativ eller positiv for den som omtales, om den er riktig, eventuelt om den fremtrer som sjikanøs*». <sup>43</sup>

Man kan identifisere argumenter på begge sider av vektskålen. På den ene siden danner opplysningene en negativ fremstilling av Harvey og belyser potensielt straffbare forhold. Det er også uklart hvorvidt samtlige av opplysningene som kobles til Harvey er sanne. Videre reises det spørsmål om serien kan forsvares ut fra allmenne og offentlige interesser, ettersom det dreier seg om en underholdningsserie. Samtidig er ikke serien bare underholdende. Serien berører flere alvorlige spørsmål tilknyttet personforfølgning og overgrep og kan bidra til å skape debatt og belyse større samfunnsproblemer.

Som ledd i denne vurderingen er det relevant å vurdere om Netflix kunne gjort mer for å undersøke om opplysningene de oppgir i serien ville krenke Harveys rettigheter. For det tilfellet Netflix var kjent med likhetene mellom Harvey og «*Martha*», bør det også vurderes om Netflix kunne og burde gjennomført ytterligere tiltak som grun-

digere anonymisering av personlige meldinger, handlinger og relasjonen til hovedkarakteren. Kort tid etter seriens debut ble Harvey identifisert av seerne på bakgrunn av en tweet rettet mot Gadd i 2014 identisk til et utsagn i serien. <sup>44</sup> Akkurat som «*Martha*» er Harvey en skotsk advokat som bor i London, tjuve år eldre enn Gadd, anklaget for tidligere forfølgelse som er offentlig kjent. Videre er det ubestridelig likhet mellom Harvey og «*Martha*» i utseende og talemåte. <sup>45</sup> Gitt den raske identifiseringen av Harvey, burde det ha vært gjort mer for å beskytte hennes anonymitet.

Dersom man legger til grunn at distribusjonen av Baby Reindeer utgjør en krenkelse av Harveys rett til vern om privatlivets fred, er neste spørsmål om krenkelsen er erstatningsbetingende.

## 5. Erstatnings- og oppreisningsvurderingen

Erstatning for krenking av privatlivets fred og ærekrenkelser reguleres i hhv. skadeserstatningsloven §§ 3-6 og 3-6 a. I begge bestemmelser er det et vilkår om at skadevolderen eller krenkeren må ha utvist uaktsomhet. Videre følger det av bestemmelsene at den forulempede kan kreve «*erstatning for den lidte skade og slik erstatning for tap i fremtidig erverv som retten ut fra den utviste skyld og forholdene ellers finner rimelig*». Bestemmelsene hjelmer også oppreisningskrav «*for skade av ikke-økonomisk art som retten finner rimelig*». <sup>46</sup>

<sup>44</sup> Harvey v Netflix side 10 flg. og 29 flg.

<sup>45</sup> Ibid.

<sup>46</sup> I saken som verserer for domstolene i California er det også fremmet krav om erstatning for skade på person (psykologisk skade), menerstatning og erstatning for personlige krenkelser, og skade av ikke-økonomisk art. Disse reguleres tilsvarende etter hhv. skadeserstatningsloven §§ 3-1, 3-2, 3-3 og 3-5. Disse faller utenfor omfanget av denne artikkelen etter plassshensyn.

Etter skadeserstatningsloven § 3-6 det et vilkår om at skadevolderen må ha utvist uaktsomhet. Ifølge forarbeidene er det tale om et «*rent uaktsombetsansvar, tilsvarende det som framgår av § 3-6 a om ærekrenkelser*». Uaktsomhetskravet knytter seg primært seg til selve ytringen og at denne ville krenke privatlivets fred eller den forulempedes æresfølelse. Uaktsomheten kan også knytte seg til krenkerens mangelfulle forarbeid forut for ytringen. <sup>47</sup>

Legger man til grunn at vilkårene her er oppfylt blir spørsmålet hvordan erstatningen og/eller oppreisningen skal utmåles. Harvey spesifiserer ikke den anført lidte skaden, foruten at serien har skadet hennes omdømme, og forårsaket skam, latterliggjøring, ydmykelse og sårede følelser. Hun anfører også at hun har lidt alvorlig emosjonell- og mental skade. For dette krever hun minimum 50 millioner dollar. Dette beløpet er tilsynelatende tilknyttet påstanden om at de uriktige påstandene skal ha vært vist mer enn 50 millioner ganger. Etter skadeserstatningsloven §§ 3-6 og 3-6 a ville Harvey først og fremst hatt krav på erstatning for lidt skade. Det ville blitt fastslått etter en ordinær vurdering av dokumentert lidt økonomisk tap som har adekvat årsakssammenheng med krenkelsen. Et relevant eksempel her kunne vært utgifter til psykolog. Det er ikke kjent om Harvey var i arbeid, men om hun var det og ytringene medføre at hun enten mistet jobben eller ble forbigått, så ville hun dessuten hatt krav på tapt erverv.

Kort fortalt er det lite sannsynlig at Harvey hatt noe erstatningskrav i størrelsesorden mangfoldige millioner dollar mot Netflix etter norsk rett. Etter vårt syn blir det mer interessant å vurdere en eventuell oppreisningsutmåling. Dette omfatter erstatning for ikke-økonomisk skade, og har gjennom rettshistorien vært pønalt motivert – man skulle

<sup>47</sup> Se for eksempel LB.2013-180678.

<sup>41</sup> Rt-2010-258 (avsnitt 54), sitert fra Rt-2007-687 (avsnitt 57 og 58).

<sup>42</sup> Rt-2010-258 (avsnitt 58).

<sup>43</sup> Rt-2010-258 (avsnitt 56).

straffe skadevolder og dermed bidra til å skape en preventiv effekt.<sup>48</sup> I denne sammenheng er det noen likhetstegn mellom dette ansvaret og såkalte «*punitive damage*» som Harvey krever i California. I senere tid har motivasjonen forflyttet seg mot oppreisningens betydning som kompensasjon for den forulempede.<sup>49</sup>

Som ved ordinært erstatningskrav er det for oppreisning en forutsetning at kravet må stå i årsaks-sammenheng med ytringen som danner grunnlaget for oppreisningen. Skaden må også være en adekvat følge av handlingen. Dersom dette legges til grunn, skal utmålingen fastsettes «*som retten finner rimelig ut fra den utviste skyld og forholdene ellers*». Dette legger opp til en sakspesifikk og skjønsmessig vurdering. Det er flere relevante momenter, særlig om den forurettede var sårbar for de aktuelle beskyldningene, og hvor utbredte uttalelsene har vært.<sup>50</sup> I Rt-2014-152 og Rt-2014-1170 ble det eksempelvis vektlagt at ytringen var landsdekkende. I Harveys sak er ytringene godt kjent over hele verden. I de omtalte sakene ble forulempede tilkjent henholdsvis kr 200 000 og kr 400 000.

I Rt-2014-1170 vektla førstvoterende at «*beskyldningene var alvorlige, klart ufullstendige og misvisende og i strid med informasjon avisen hadde i hende. Mediedekningen fikk store konsekvenser for A både profesjonelt og personlig. Den førte blant annet til at A ble satt under tilsyn, at det ble opplyst offentlig at politiettersforskning ble satt i verk mot ham, og at han ble nektet å operere. A oppfattet beskyldningen, som også ble kjent i fagmiljøet internasjonalt, som så belastende at han sa fra seg internasjonale vern. Han og konen følte seg sosialt isolert og fikk store psykiske problemer. Etter en tid sa han opp stillingen sin og flyttet med fami-*

*lien til Danmark.*» I Rt-1994-174 ble spredningsomfanget også vurdert i lys av at den forulempede ikke selv hadde søkt offentlighetens lys. I LB-2013-67432 omhandlet ytringene private forhold uten «*offentlig interesse*», som medføre at den krenkede hadde «*krav på at rettsordenen gir effektiv beskyttelse mot å bli hengt ut i media*». Tilsvarende momenter gjør seg gjeldende i Harveys sak.



Med forutsetning om at det foreligger urettmessig æreskrenkelse og/eller krenkelse av privatlivets fred er det ikke usannsynlig at man i Norge ville kunne blitt tilkjent et millionbeløp som vesentlig overstiger tidligere norsk rettspraksis.

Et ytterligere og sentralt moment er at Netflix hittil skal ha tjent over 9,5 milliarder dollar på serien. Til sammenligning er det ikke kjent hva krenkeren (regional avis) hadde generert av inntekter i Rt-2014-1170, men trolig vil ikke de aktuelle ytringene hatt målbar påvirkning på avissalget. I Rt-2009-265 og LA-2021-155004 ble inntektene uttrykkelig vektlagt til fordel for et høyere beløp. Motsatt eksempel er TOSLO-2017-151387 hvor tingretten la til grunn et lavere beløp grunnet krenkerens økonomiske situasjon, hvis hensynet var at vedkommende ikke skulle rammes urimelig hardt. Krenkerens økonomi er dermed relevant i begge retninger. Et argument som tilsier at Harveys oppreisning kunne blitt redusert er at hun selv gjentatte ganger har uttalt seg offentlig om saken, som også var tilfellet i LB-2020-64670. Et slikt hensyn skal imidlertid vektlegges med forsiktighet, ettersom

man som hovedregel har rett til å imøtegå ytringer. I Harveys sak kan det argumenteres for at hun har gått for langt, ved å blant annet delta på «*Piers Morgan Uncensored*».<sup>51</sup>

Med forutsetning om at det foreligger urettmessig æreskrenkelse og/eller krenkelse av privatlivets fred er det ikke usannsynlig at man i Norge ville kunne blitt tilkjent et millionbeløp som vesentlig overstiger tidligere norsk rettspraksis. Dette gjelder særlig gitt Harveysakens til dels høyest urovekkende skildringer og at Netflix har generert betydelige inntekter som angivelig direkte følge av krenkelsen.

*Nicholas Foss Barbantonis, assosiert partner, Advokatfirmaet Simonsen Vogt Wiig AS. Nicholas arbeider i firmaets prosedyreavdeling, med fokus på teknologi, media, telekom og immaterialrett.*

*Fabian Bjørnstad, advokatfullmektig, Advokatfirmaet Simonsen Vogt Wiig AS. Fabian arbeider i firmaets teknologi- og medieavdeling, med fokus på kommersiell kontraktsrett.*

*Camilla Hagelien er fast advokat i Simonsen Vogt Wiig AS. Camilla arbeider i prosedyreavdelingen og har erfaring fra arbeid med teknologi- og medie relaterte problemstillinger.*

48 Hagstrøm, Erstatningsrett, 2. utg., s. 582.

49 Rt-2011-769.

50 Se eksempelvis LB-2013-67432.

51 Intervjuet er allerede sett over 14 millioner ganger. Intervjuet er tilgjengelig her [https://youtu.be/mK-isQXd\\_Qw?si=bM6II\\_2pTU4VMVbR](https://youtu.be/mK-isQXd_Qw?si=bM6II_2pTU4VMVbR).

# En definition av ett AI-system utifrån matematiska modeller av inlärning

Av Boris Melvås

Definitionen av ett AI-system enligt 3.1 rättsakten om AI är:<sup>1</sup>

*AI-system: ett maskinbaserat system som är utformat för att fungera med varierande grad av autonomi, som kan uppvisa anpassningsförmåga efter införande och som, för uttryckliga eller underförstådda mål, på grundval av de indata det tar emot, drar slutsatser om hur utdata såsom förutsägelser, innehåll, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer ska genereras.*



Boris Melvås

Definitionen är formulerad med hjälp av ett vardagligt språk så att även de som helt saknar fackkunskaper ska kunna förstå vad som menas. Men en sådan målsättning är på det aktuella rättsområdet i varje fall till viss del illusorisk, eftersom en definition utifrån vardagsspråket i praktiken ändå måste översättas till ett på IT-marknaden gångbart fackspråk innan definitionen kan appliceras på en verklig situation. Skälet till detta är att IT-system benämns utifrån de namn man har gett olika datavetenskapliga lösningar och inte med hjälp av de väldigt oprecisa beskrivningar, av hur dessa lösningar fungerar, som kan genereras med hjälp av vardagsspråket. Att i väldigt allmänna ordalag beskriva hur t.ex. ett datorprogram fungerar är ju trots allt något helt annat än att referera till etablerade konstruktioner såsom subprogram, algoritmer eller matematiska modeller. Således finns det ett behov av en översättning av definitionen av ett

AI-system i rättsakten om AI till ett fackspråk. I det följande redogör jag för ett försök att ge en sådan gångbar definition, utifrån ett modellteoretiskt tankesätt, som ändå är förhållandevis lätt att förstå för lekmän.

” I det följande redogör jag för ett försök att ge en sådan gångbar definition, utifrån ett modellteoretiskt tankesätt, som ändå är förhållandevis lätt att förstå för lekmän.

En modellteoretisk definition bygger på termen *modell*, med vilken avses ett förenklat sätt att återge en del av verkligheten med hjälp av någon form av medium. En fysisk modell av ett hus eller ett skepp kan t.ex. vara konstruerat av trä medan en modell av ett trafikflöde bättre återges med en matematisk

funktion.<sup>2</sup> Även andra symbolspråk än matematiska används. Lambda-kalkyl kan t.ex. användas för att modellera en av flera möjliga metoder för hur en dator utför beräkningar och en predikatlogisk modell kan användas för att beskriva ett språks semantik.<sup>3</sup> Men vilken typ av modell bör man använda för att definiera ett AI-system? Jag hävdar i denna artikel att definitionen av ett AI-system i rättsakten om AI är logiskt ekvivalent med följande definition utifrån matematiska modeller av inlärning:

*Ett AI-system är en fysisk maskin som implementerar minst en matematisk modell av inlärning eller minst en matematisk modell av kunskap som har genererats med hjälp av en matematisk modell av inlärning.*

Med frasen *en fysisk maskin som implementerar minst en matematisk modell* menas varje lyckat försök att skapa en fysisk maskin som utför den uppgift, närmare bestämt den beräkning, som den matematiska modellen anger.<sup>4</sup> Med frasen *en ma-*

<sup>1</sup> [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138\\_SV.html](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_SV.html) [Besökt 2024-08-17]

<sup>2</sup> Edwards D. & Hamson M. (2007) Guide to Mathematical Modelling, 2 ed. Industrial Press Inc och OECD:s Explanatory Memorandum från mars 2024 som finns här: [https://www.oecd-ilibrary.org/science-and-technology/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system\\_623da898-en](https://www.oecd-ilibrary.org/science-and-technology/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_623da898-en)

<sup>3</sup> Fernández M. (2009) Models of Computation – An Introduction to Computability Theory. Springer samt Portner P.H. (2005) What is Meaning? – Fundamentals of Formal Semantics. Blackwell

<sup>4</sup> Gabbrielli M. & Martini S. (2010) Programming Languages: Principles and Paradigms. Springer

*tematisk modell* menas här varje matematiskt baserad definition av ett fenomen i världen, t.ex. inläring eller kunskap.<sup>5</sup> Med frasen *en matematisk modell av kunskap som har genererats med hjälp av en matematisk modell av inläring* menas en matematisk modell av kunskap som framgår av en programkod som har genererats av ett annat program, som i sin tur är en implementering av en matematisk modell av inläring. En implementering av en modell av kunskap som i denna mening inte har genererats med hjälp av en matematisk modell av inläring, utan har skapats manuellt, utgör därmed inte ett AI-system. Det ska avslutningsvis noteras att jag med kunskap här menar såväl praktisk kunskap om hur man gör något (eng. knowledge how) som kunskap om hur något förhåller sig (eng. knowledge that).<sup>6</sup>

För att visa att definitionen ovan av ett AI-system kan härledas från definitionen i rättsakten om AI går jag igenom den senare definitionen fras för fras.

Ett *maskinbaserat system* är en *agent*, d.v.s. något som agerar. En sådan agent kan besitta ett antal förmågor så som förmågan att i någon mening veta något eller kunna uppfatta sin omvärld, kommunicera med andra, röra sig i världen, utföra rörelser med extremiteter etc.<sup>7</sup> Att agenten är maskinbaserad betyder i detta sammanhang att agentens förmågor i grunden härrör från en *beräkningsmaskin*.<sup>8</sup> Visserligen är även en bensindriven gräsklippare av äldre

modell en maskin, men det är i sammanhanget förhållandevis klart att man, liksom inom datavetenskapen i övrigt, avser en beräkningsmaskin när man talar om en maskin.<sup>9</sup> En modern beräkningsmaskin kallas för en dator. Ett maskinbaserat system är således *en dator med ett antal anslutna enheter (som kan vara ytterligare datorer)* som förser datorn med t.ex. ljud, bild, text m.m. och ser till så att den kan kommunicera och eventuellt också förflytta sig etc. Ett sådant AI-system kan vara fristående, normalt med en bildskärm och ett tangentbord etc. för kommunikation, eller utgöra en komponent i en större produkt och då antingen vara fysiskt inbyggt eller vara sådant att det på annat sätt ”tjänar produktens funktioner”.<sup>10</sup> Av det faktum att systemet är maskinbaserat, d.v.s. körs på en maskin, drar jag dock slutsatsen att det krävs *en fast kommunikationsväg mellan datorn och enheterna* för att de ska utgöra delar av samma AI-system. Bara det faktum att en dator och ett program har använts för att en gång i tiden generera ett program som används på en annan dator bör därför inte innebära att de är en del av samma AI-system, d.v.s. en del av samma maskin.

Att systemet ska fungera med *varierande grad av autonomi* betyder att programmet är konstruerat för att självständigt dra vissa betydelsefulla slutsatser, även om dessa slutsatser inte behöver utgöra beslut i en mer strikt mening.<sup>11</sup> Därmed blir också frågan om t.ex. en knapptryckning i enlighet med en dators förslag från en livrädd stridsvagnsförare med en beslutstid som understiger en sekund räknas som ett ej automati-

serat beslut mindre relevant.<sup>12</sup> Det räcker med att systemet är konstruerat för att självständigt lämna åtgärdsförslag för att autonomikravet ska vara uppfyllt.

Att systemet *kan uppvisa anpassningsförmåga* innebär att systemets programkod kan utvecklas under driftstiden genom att det finns en förmåga till självlärande. Dock verkar detta, speciellt inte enligt OECD, vara ett nödvändigt villkor för att något ska vara ett AI-system, utan mer en egenskap som många AI-system har. Frasen ”kan uppvisa” verkar således betyda just en möjlig förmåga hos ett AI-system. Detta följer också av att t.ex. program för bildigenkänning kan sakna inlärningsförmåga även om det är uppenbart att även sådana program är tänkta att regleras av rättsakten om AI.<sup>13</sup> Frasen får därmed anses utgöra ett förtydligande av att inlärningsförmåga är något som gör något till ett AI-system, men att det även finns andra typer av AI-system.

Att systemet är *konstruerat för att uppnå uttryckliga eller underförstådda mål* betyder att målen antingen kan vara hårdkodade, d.v.s. permanent definierade mål som inte kan ändras, eller sådana mål som systemet kan lära sig efterhand utifrån regler som den tillämpar, t.ex. genom att läsa av trafikskyltar.<sup>14</sup>

Avslutningsvis kan tyckas att frasen ”*drar slutsatser om hur utdata [...] ska genereras*” borde betyda att systemet kan lära sig hur utdata ska genereras. Men speciellt OECD

5 Guttag J.V. (2016) Introduction to Computation and Programming Using Python – With Application to Understanding Data. MIT

6 <https://plato.stanford.edu/entries/knowledge-how/> [Besökt 2024-06-10.]

7 Russel S. & Norvig P. (2016) Artificial Intelligence – A Modern Approach. Pearson

8 Gabbrielli M. & Martini S. (2010) Programming Languages: Principles and Paradigms. Springer

9 Se preamble 12 till rättsakten om AI enligt denna text: [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138\\_SV.html](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_SV.html) [besökt 2024-05-31]

10 Se preamble 12 till rättsakten om AI.

11 Se preamble 12 till rättsakten om AI.

12 Liljefors M., Noll G. & Steuer D. (2019) War and Algorithm. Rowman & Littlefield samt Hänold S. Profiling and Automated Decision-Making: Legal Implications and Shortcomings i Corrales, Fenwick & Forgó (ed) (2018) Robotics, AI and the future of Law. Springer

13 Se preamble 12 till rättsakten om AI och <https://www.oecd.org/digital/artificial-intelligence/>.

14 Se OECD:s hemsida <https://oecd.ai/en/work/ai-system-definition-update>. [besökt 2024-05-31]

verkar istället mena att även en klassificeringsmodell, t.ex. ett vanligt bildigenkänningsprogram, som saknar inlärningsförmåga drar slutsatser om hur utdata ska genereras. Detta följer av att OECD beaktar såväl AI-systems "build phase" som dess "use phase" när man bedömer om det deduktiva kravet ovan är uppfyllt.<sup>15</sup> Även i preamble 12 rättsakten om AI verkar man mena att maskininlärning antingen ska ha varit en del av systemets "build phase" eller vara en del av systemets "use phase" för att systemet ska vara ett AI-system. Däremot utgör rena s.k. logiska agenter, d.v.s. agenter vars programkod enbart bygger på grundläggande logiska samband och ingen mer avancerad matematik, inte AI-system.<sup>16</sup> Att AI-system delvis kan baseras på "logik- och kunskapsbaserade strategier" är en annan sak.<sup>17</sup>

Sammanfattningsvis är ett AI-system således:

- a) En beräkningsmaskin, till vilken ett antal assisterande enheter (t.ex. ytterligare en dator) har anslutits,
- b) som har en förmåga att lära sig ett beteende eller uppvisar ett inlärt beteende
- c) som innebär att systemet, för uttryckliga eller underförstådda mål, från indata genererar utdata, oavsett om denna utdata kan påverka en fysisk eller en virtuell miljö.

Från dessa premisser kan man nu härleda den modellteoretiska definition som jag nämnde i inledningen. Av a-b ovan följer att ett AI-system till att börja med är en viss typ av fysisk maskin med förmågan att lära sig ett beteende eller att följa ett

inlärt beteende. Det är dock irrelevant hur maskinen är uppbyggd så länge den har någon av de förmågor som nämns i b, eftersom den då också måste bestå av en beräkningsmaskin med assisterande enheter. En sådan fysisk maskin är en fysisk implementering av en matematisk modell av inlärning eller en fysisk implementering av en matematisk modell av kunskap som har genererats med hjälp av en sådan matematisk modell av inlärning. Del c av definitionen tillför i min mening däremot ingenting ytterligare av följande skäl. Att indata ska medföra utdata är en del av definitionen av ett datorprogram, vars existens är en förutsättning för en fysisk implementering av en matematisk modell.<sup>18</sup> Vidare innebär det faktum att målet med detta program antingen kan vara uttryckligt definierat eller underförstått, samt att utdata ska kunna påverka en fysisk eller en virtuell miljö, inte mer än att beräkningsmaskinen är konstruerad för att på något sätt kunna ha en betydelsefull effekt på sin omgivning. Varje implementering av en modell av inlärning eller en modell av kunskap kan dock ha en sådan effekt utifrån uttryckliga eller underförstådda mål. Därmed följer det att kriteriet c är uppfyllt om kriterierna a-b är uppfyllda. Definitionen av ett AI-system kan då förkortas till:

1. En fysisk maskin
2. som implementerar minst en matematisk modell av inlärning eller minst en matematisk modell av kunskap som har genererats med hjälp av en matematisk modell av inlärning.

Definitionen i rättsakten om AI kan således översättas till en modellteo-

retisk definition enligt 1 och 2 ovan utifrån matematiska modeller av inlärning. Att denna definition inte bara är möjlig, utan även är lätt att förstå och använda, förklaras dock bäst med ett exempel.

Anta att följande, påhittade, matematiska modell av förmågan att kunna skilja falska hyreskontrakt från äkta hyreskontrakt är genererad genom maskininlärning:

- I.  $f(x_1, x_2) = 1$ , om  $x_2 < (x_1 - 2) * 3$
- II. annars  $f(x_1, x_2) = 0$

Modellen för inlärning antas vara en s.k. SVM (Support Vector Machine). Jag förklarar inte här hur en sådan modell fungerar men ger en länk till en grafisk beskrivning för den intresserade.<sup>19</sup> Den SVM som i detta fall har använts för att generera modellen av kunskap är därmed en matematisk modell av inlärning. Vad gäller modellen av kunskap behöver den bara två mätvärden,  $x_1$  och  $x_2$ , vilket är helt orealistiskt men pedagogiskt. Modellen ska läsas så att ett hyreskontrakt bedöms som äkta om  $f(x_1, x_2) = 1$ . Detta gäller t.ex. om mätvärdena är  $x_1 = 5$  och  $x_2 = 6$ , eftersom  $(5 - 2) * 3 = 9$ , vilket är större än 6. Den matematiska modellen ovan är därmed en matematisk modell av kunskap som har genererats med hjälp av en matematisk modell av inlärning. Således är varje implementering, i form av en fysisk maskin, av den modell av kunskap som definieras genom I och II ett AI-system. Även varje implementering, i form av en fysisk maskin, av den SVM som har använts för att generera denna modell av kunskap är ett AI-system.

I min mening visar detta att det utifrån den definition av ett AI-system som jag här har föreslagit är gan-

15 <https://oecd.ai/en/nonk/ai-system-definition-update> och OECD:s Explanatory Memorandum från mars 2024

16 Russel S. & Norvig P. (2016) Artificial Intelligence – A Modern Approach. Pearson

17 Se preamble 12 till rättsakten om AI

18 Med "program" menar jag här såväl en implementering genom "hardware", "firmware" som "software", jfr Gabbrielli M. & Martini S. (2010) Programming Languages: Principles and Paradigms. Springer. I praktiken är det dock "software" som det handlar om.

19 Bilden används i enlighet med Creative Commons Attribution-Share Alike 3.0 Unported license, se [https://commons.wikimedia.org/wiki/File:Svm\\_separating\\_hyperplanes\\_\(SVG\).svg](https://commons.wikimedia.org/wiki/File:Svm_separating_hyperplanes_(SVG).svg). (I och II motsvaras av den röda linjen i denna bild.)

ska enkelt att avgöra om en fysisk maskin är ett AI-system eller inte. Detta beror i sin tur på att det finns klara matematiska definitioner av vad som menas med en matematisk modell av inlärning. Exempel på sådana modeller är förutom SVM, Linear Regression, Random Forest Classifier, CNN (Convolutional Neural Network), GAN (Generative Adversarial Network) etc. Vad som menas med en modell av kunskap som har genererats med hjälp av en modell av inlärning samt vad som menas med en fysisk implementering av någon av dessa modeller är också glasklart. Definitionen som jag här har föreslagit är

därmed mycket lättare att förstå och använda än den definition i rättsakten om AI från vilken jag har härlett den.

” Sammanfattningsvis anser jag mig ha goda grunder för att definitionen i rättsakten om AI är logiskt ekvivalent med den definition utifrån matematiska modeller av inlärning som jag här har givit.

Sammanfattningsvis anser jag mig ha goda grunder för att definitionen i rättsakten om AI är logiskt ekvivalent med den definition utifrån matematiska modeller av inlärning som jag här har givit. Jag anser mig även ha visat att den härledda definitionen är mycket lätt att förstå och använda. Men jag överlämnar till läsaren att avgöra om detta stämmer även efter närmare granskning.

*Boris Melväs arbetar som jurist på Pensionsmyndigheten men har även en bakgrund inom teoretisk filosofi, logik och klassiska språk.*

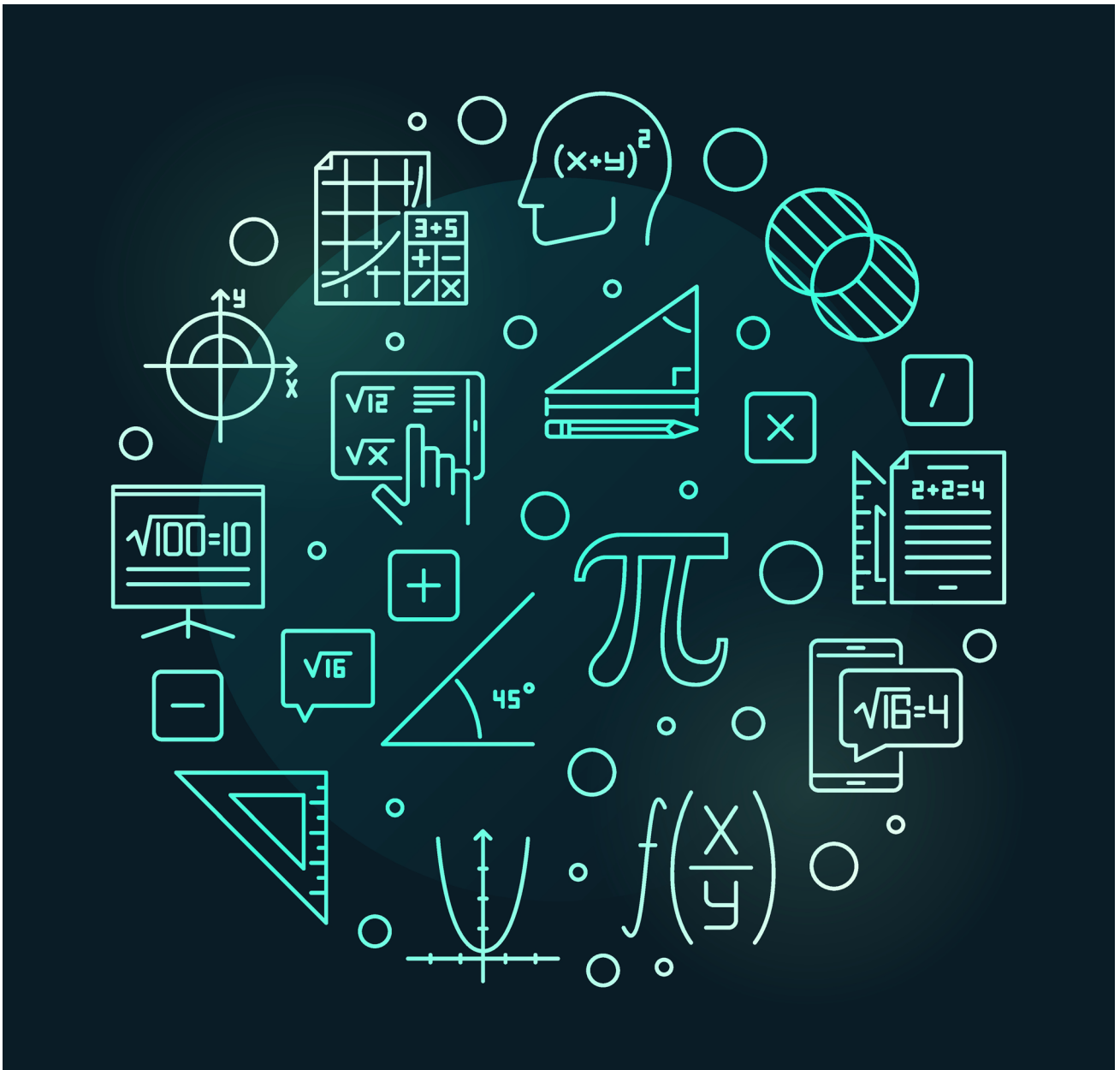


Illustration: Colorbox.com

# Harmoniserte standarder: En ny sentral rettskilde i kommende regulering av kunstig intelligens

Av Lars Arnesen

Harmoniserte standarder har lenge vært et viktig verktøy i EUs produktlovgivning, og vil komme til å spille en sentral rolle med innføringen av KI-forordningen.<sup>1</sup> Europeiske standarder utvikles av europeiske standardiseringsorganisasjoner, og blir «harmonisert» gjennom en godkjeningsprosess administrert av EU-kommisjonen.<sup>2</sup> Denne artikkelen forklarer hva harmoniserte standarder er, og peker på noen utfordringer knyttet til bruken av dem som rettskilde, med særlig vekt på regulering av kunstig intelligens.

Harmoniserte standarder er et privat supplement til ordinær lovgivning. Lovgivning fra demokratisk valgte representanter, slik som EU-parlamentet, blir i økende grad supplert av private initiativer.<sup>3</sup> Privatproduserte supplementer til offisielle rettskilder kommer i ulike former.<sup>4</sup> Et eksempel er etiske retningslinjer for bruk av kunstig intelligens som



Lars Arnesen

private selskaper selv har utarbeidet.<sup>5</sup> Et annet eksempel er standarder utviklet av interessegrupper, bransjeorganisasjoner eller standardiseringsorganisasjoner.

” Denne artikkelen forklarer hva harmoniserte standarder er, og peker på noen utfordringer knyttet til bruken av dem som rettskilde, med særlig vekt på regulering av kunstig intelligens.

Personvernforordningen er et fremtredende eksempel, der forordningen fungerer som et regulatorisk rammeverk som åpner for supplering og spesifisering gjennom atferdsnormer,<sup>6</sup> sertifisering,<sup>7</sup> samt anbefalinger og retningslinjer fra blant annet Personvernrådet.<sup>8</sup> Kravene i personvernforordningen kan derfor formuleres nokså generelt, slik som for eksempel forpliktelsene i artikkel 24, der det følger at behandlingsansvarlig skal «gjennomføre egnede tekniske og organisatoriske tiltak.» Hva «egnete» tiltak innebærer beror på en helhetlig risikovurdering.<sup>9</sup> Støtte til hvordan denne risikovurderingen skal gjøres, og hvilke tiltak som er relevante, finnes i blant annet standarder.

Standarder spiller allerede en viktig rolle i å utfylle de generelle forpliktelsene i personvernforordningen. ISO 27001:2017 er for eksempel en mye brukt standard, som et verktøy for å oppfylle informasjons sikkerhetskravene som følger av personvernforordningen artikkel 32.<sup>10</sup>

Det er imidlertid en sentral forskjell mellom standarder og *harmoniserte* standarder. Det er ingen harmoniserte standarder knyttet direkte til personvernforordningen, men det vil komme en rekke nye harmo-

1 Forordning 2024/1689 av 13. juni 2024 (Engelsk: Artificial Intelligence Act, Norsk: KI-forordningen).

2 Forordning 1025/2012 (standardiseringsforordningen).

3 van Gestel, R., & van Lochem, P. J. P. M. (2020). Private standards as a replacement for public lawmaking? DOI: <https://doi.org/10.4337/9781788118415.00009>.

4 Cafaggi, F. (2011). New Foundations of Transnational Private Regulation. DOI: <https://doi.org/10.1111/j.1467-6478.2011.00533.x>.

5 For eksempel Microsoft Responsible AI Standard (juni 2022), besøkt 13. juni 2024. URL: <https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2022/06/Microsoft-Responsible-AI-Standard-v2-General-Requirements-3.pdf>.

6 Personvernforordningen art. 40

7 Personvernforordningen art. 42

8 Personvernforordningen art. 70

9 C-340/21 VB v *Natsionalna agentsia za prihodite*, avsnitt 42.

10 Denne standarden etterspørres for eksempel i offentlige anbud i tilknytning til personvernforordningen artikkel 32.



niserte standarder til den nye KI-forordningen.<sup>11</sup>

Harmoniserte standarder er direkte knyttet til EUs rettsystem ved at de publiseres av EU-kommisjonen i Den europeiske unions tidende (*Official Journal of the European Union*).<sup>12</sup> EU-domstolen har derfor avklart, først i 2016 og på nytt i en avgjørelse fra 5. mars 2024, at harmoniserte standarder er en del av EU-retten.<sup>13</sup>

Dette reiser flere prinsipielle rettslige spørsmål.<sup>14</sup> Ett spørsmål er om harmoniserte standarder i realiteten er ufravikelig og obligatorisk tvingende rett, noe som reiser spørsmålet om alle bør ha fri tilgang til standarden, på lik linje med ordinære, formelle EU-rettskilder. Tilgang til harmoniserte standarder selges i dag av standardiseringsorganisasjonene, typisk til priser som varierer fra noen hundre til flere hundre euro.<sup>15</sup>

Det er ikke bare tilgang til de endelige standardene som koster. Deltakelse i standardiseringsarbeidet er også avgiftsbelagt, der de som ønsker å bidra til å utvikle standardene må betale for en plass rundt bordet. Det finnes visse krav fra EU-kom-

misjonen for å sikre tilgang og deltakelse fra små og mellomstore bedrifter, og fra sivilsamfunnsorganisasjoner. Kravene er likevel formulert som myke juridiske krav, uten sanksjoner. For eksempel skal europeiske standardiseringsorganisasjoner «oppmuntre» små og mellomstore bedrifter til å delta, «for eksempel» ved å gi gratis eller redusert tilgang og deltakelse.<sup>16</sup> Satsene fastsettes imidlertid av dem selv.

Et tredje spørsmål, som særlig knytter seg til regulering av KI-systemer, er de samfunnsmessige problemstillingene som oppstår når KI-systemer tas i bruk. Design, utvikling og bruk av KI-systemer reiser en rekke grunnleggende og komplekse samfunnsproblemer. Dette kan stille seg annerledes enn for eksempel tekniske krav til heiser, bygningstutstyr eller leker, der harmoniserte standarder har vært fremtredende i en årrekke allerede.

Denne artikkelen vil fortsette med en kort forklaring av hvordan standarder blir harmonisert, etterfulgt av en redegjørelse for to avgjørelser fra EU-domstolen som bekrefter at harmoniserte standarder er en del av EU-retten. Artikkelen avslutter med noen betraktninger rundt implikasjonene av at harmoniserte standarder er innlemmet som en del av EUs rettsystem.

## 1. Hva er en standard, og hva gjør den harmonisert?

De første standardiseringsorganisasjonene i Europa ble dannet i forbindelse med industrialiseringen på 1800-tallet. Standardisering var nødvendig for produksjon i industriell skala, noe som førte til dannelsen av nasjonale standardiseringsorganisasjoner og senere internasjonale standardiseringsorganisasjoner på 1900-tallet.<sup>17</sup>

16 Forordning 1025/2012 (standardiseringsforordningen), artikkel 5 og 6.

17 Standardisering, Wikipedia, besøkt 13.06.2024. URL: <https://en.wikipedia.org/wiki/Standardization>.

Harmoniserte standarder omhandler typisk svært tekniske emner, som for eksempel grenseverdier for ulike typer kjemiske stoffer som kan brukes i et bestemt produkt. For eksempel avgjørelsen *James Elliot v Irish Asphalt* (C-613/14), som er nærmere omtalt nedenfor, gjaldt spesifisering av hvor mye svovel som skal inngå i asfalt. Spesifikasjonene endres kontinuerlig, basert på den nyeste kunnskapen i bransjen og nye vitenskapelige funn, noe som gjør det utfordrende å gi detaljerte spesifikasjoner gjennom ordinære lovgivningsprosesser.

I dag er det tre europeiske standardiseringsorganisasjoner som har ansvaret for å utarbeide harmoniserte standarder. Disse er European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), og European Telecommunications Standards Institute (ETSI). De tre organisasjonene er anerkjent som «europeiske standardiseringsorganisasjoner» etter forordning 1025/2012 (standardiseringsforordningen).

Samordningen mellom standardiseringsorganisasjonene ble først regulert på EU-nivå i 1983.<sup>18</sup> Rådsdirektivet fra 1983 fastsatte en prosedyre for utveksling av informasjon om standardiseringsprosjekter, noe som sørget for at de ulike nasjonale standardiseringsorganisasjonene ble bedre koordinert.<sup>19</sup> Direktivet sørget også for at det ikke ble utarbeidet nasjonale standarder der det allerede fantes en europeisk standard.<sup>20</sup> På denne tiden fantes det ingen *harmoniserte*

18 Pelkmans, J. (1987). The New Approach to Technical Harmonization and Standardization. *Journal of Common Market Studies* Volume XXV, No. 3 March 1987 002 1-9886.

19 Rådsdirektiv av 28. mars 1983 om fastsettelse av en informasjonsprosedyre med hensyn til tekniske standarder og forskrifter (83/189/EØF), artikkel 2.

20 Ibid. artikkel 7.

11 EU-kommisjonen har en oppdatert oversikt over gjeldende harmoniserte standarder, se «Harmonised Standards», besøkt 13. juni 2024. URL: [https://single-market-economy.ec.europa.eu/single-market/european-standards/harmonised-standards\\_en](https://single-market-economy.ec.europa.eu/single-market/european-standards/harmonised-standards_en).

12 Forordning 1025/2012 (standardiseringsforordningen) art. 10(6).

13 C-613/14 *James Elliot Construction Limited mot Irish Asphalt Limited*, avsnitt 40, og C-588/21 *Public.Resource.Org Inc & Right to Know CLG mot Europakommisjonen*, avsnitt 70-80.

14 Se blant annet Traktaten om Den europeiske unions virkemåte (TFEU), artikkel 15(3) og Pakten om grunnleggende rettigheter («Pakten»), artikkel 20, 42 og 47.

15 Prisene varierer betydelig, fra noen hundre til flere hundre euro per standard. Prisene er oppgitt i nettbutikkene til de nasjonale standardiseringsorganisasjonene. Det kan være nødvendig med et sett med standarder for å overholde alle gjeldende produktforskrifter i EU, for eksempel for leketøy, medisinsk utstyr eller KI-systemer.

standarder, kun europeiske standarder. De europeiske standardene ble utarbeidet av de europeiske standardiseringsorganisasjonene, men uten at de ble harmonisert og innlemmet i formell EU-lovgivning.

Ideen om harmoniserte standarder ble formelt introdusert to år senere, i 1985, med rådsresolusjonen «on a new approach to technical harmonisation and standards.»<sup>21</sup> Den nye tilnærmingen innebærer et system der EU-kommisjonen gir de europeiske standardiseringsorganisasjonene mandat til å utarbeide egnede standarder, som deretter vedtas av EU-kommisjonen, forutsatt at standarden oppfyller kravene i mandatet. Vedtatte standarder publiseres som harmoniserte standarder i Den europeiske unions tidende.

Det følger av rådsresolusjonen fra 1985 at standardene vil «maintain their status as voluntary standards.»<sup>22</sup> Den nye metoden med harmonisering av standarder hadde altså ikke til hensikt å gjøre standardene obligatoriske, noe som fortsatt er et grunnleggende prinsipp i europeisk standardisering, nedfelt i fortalepunkt to i standardiseringsforordningen.<sup>23</sup>

Standardiseringsforordningen fastsetter den gjeldende prosedyren for harmonisering av standarder. EU-kommisjonen kan, i henhold til artikkel 10, anmode en eller flere europeiske standardiseringsorganisasjoner om å utarbeide standarder som skal harmoniseres med en eller flere produktreguleringer. Harmoniserte standarder kan for eksempel brukes i forbindelse med regulering av leketøy, medisinsk utstyr, og nå også snart KI-systemer. Kommisjonen vil offentliggjøre standarder som oppfyller kravene i mandatet i Den eu-

ropeiske unions tidende.<sup>24</sup> Europa-parlamentet eller medlemslandene kan protestere mot harmoniserte standarder, med den begrunnelse at standardene ikke oppfyller kravene i mandatet. Standardene kan da enten trekkes tilbake eller opprettholdes med begrensninger.<sup>25</sup>

## 2. Kan harmoniserte standarder være både frivillige og obligatoriske på samme tid?

EU-domstolen har i nyere tid behandlet to saker om harmoniserte standarders rettslige og frivillige karakter. I den første saken, *James Elliot v Irish Asphalt (C-613/14)*, kom EU-domstolen til at harmoniserte standarder utgjør en del av EU-retten, når harmoniserte standarder er brukt på en måte som skaper bindende rettsvirkninger.<sup>26</sup> Saken gjaldt en kontraktsmessig tvist om den avtalte kvaliteten på asfalt. Asfalten oppfylte ikke de tekniske spesifikasjonene i standarden EN 1342:2002, særlig med hensyn til svovelinnholdet. Irlands høyesterett anmodet EU-domstolen om en prejudisiell avgjørelse for å avklare om EU-domstolen har kompetanse til å tolke den harmoniserte standarden i henhold til TFEU artikkel 267.

EU-domstolen kom til at den aktuelle harmoniserte standarden er en del av EU-retten fordi overholdelse av den skaper en presumsjon for overholdelse av byggeveredirektivet (direktiv 89/106).<sup>27</sup> Det er dermed en direkte forbindelse mellom den harmoniserte standarden og de ufravikelige lovkravene i byggeveredirektivet. For å utfordre presumsjonen må standarden tolkes av EU-domstolen, og følgelig utgjør standarden en del av EU-retten.

I den andre saken, *Public.Resource.Org and Right to Know v. European Commission*, gjentar domstolen at

harmoniserte standarder som har rettsvirkninger, er en del av EU-retten.<sup>28</sup> Saken gjaldt fri tilgang til fire harmoniserte standarder for leketøy. De fire aktuelle standardene har rettsvirkninger, ettersom overholdelse av de fire standardene forutsetter overholdelse av leketøysdirektivet (direktiv 2009/48).<sup>29</sup>

I sin begrunnelse i *Public.Resource.Org-saken* påpekte domstolen at det ikke finnes noen realistiske alternativer til bruk av harmoniserte standarder. Domstolen mente at «it may prove difficult, or even impossible, for economic operators to have recourse to a procedure other than that of compliance with such standards, such as an individual expert report, in the light of the administrative difficulties and additional costs arising therefrom.»<sup>30</sup> På dette grunnlaget konkluderte domstolen med at selv om de fire standardene i saken formelt sett var frivillige, var standardene i realiteten «manifestly mandatory» for å overholde regelverket om leketøysikkerhet.<sup>31</sup>

Domstolen påpekte at enhver person som ønsker å utfordre presumsjonen om at lovkravene er oppfylt må ha tilgang til de aktuelle harmoniserte standardene. Domstolen la til grunn at en «harmonised standard may specify the rights conferred on individuals as well as their obligations and those specifications may be necessary for them to verify whether a given product or service actually complies with the requirements of such legislation»<sup>32</sup> Det er ikke bare virksomheter som er underlagt lovkrav som kan ha en interesse, men også privatpersoner kan ha en legitim interesse i å utfordre presumsjonen om at lovkravene er oppfylt. For eksempel kan en familie som har blitt eksponert for farlige leker ønske å konsultere

21 Rådets resolusjon av 7. mai 1985 om en ny tilnærming til teknisk harmonisering og standarder (85/C/136/01).

22 Ibid, vedlegg II.

23 Pelkman (se n. 20) gir en utførlig redegjørelse for den nye tilnærmingen som ble vedtatt i 1985.

24 Standardiseringsforordningen, art. 10(6).

25 Ibid, art. 11(1).

26 *James Elliot*, avsnitt 40-42.

27 Ibid.

28 *Public.Resource.Org.*, avsnitt 70.

29 Ibid., avsnitt 70-80.

30 Ibid., avsnitt 75.

31 Ibid., avsnitt 79.

32 Ibid., avsnitt 82.

standardene, for å vurdere om produsenten faktisk har overholdt de relevante lovkravene.<sup>33</sup>

EU-domstolen bekrefter gjennom de to sakene at harmoniserte standarder er gjenstand for obligatorisk håndhevelse, ettersom domstolene kan anvende dem for å avgjøre om EU-retten er overholdt.

Til tross for disse avklaringene er det fortsatt flere uavklarte spørsmål, knyttet til statusen harmoniserte standarder har som rettskilde sammenlignet med konvensjonelle EU-rettskilder. EU-domstolen har kun løst spørsmålet om tilgang til standardene basert på et spesifikt rettslig grunnlag, som de europeiske standardiseringsorganisasjonene ikke er underlagt. Det rettslige grunnlaget for innsyn, som brukes i *Public.Resource.Org*, er forordning 1049/2001, som omhandler offentlighet i dokumenter fra Europaparlamentet, Rådet og Kommisjonen. Enhver kan be om innsyn i harmoniserte standarder fra EU-institusjonene, men ikke fra de europeiske standardiseringsorganisasjonene.

Opphavsretten til de harmoniserte standardene er ikke opphevet. De europeiske standardiseringsorganisasjonene kan fortsatt påberope seg opphavsrett og begrense tilgangen i henhold til sine egne vilkår og betingelser. Harmoniserte standarder, inkludert de fire standardene som behandles i *Public.Resource.Org*, tilbys fortsatt for salg til en pris på 250 til 380 euro per stykk, noe som utgjør mer enn 1000 euro for å få tilgang til alle standardene.

EU-domstolen gir gjennom sin avgjørelse i *Public.Resource.Org* en mulighet til å omgå betalingsmuren til de europeiske standardiseringsorganisasjonene, ved å få gratis tilgang til standardene direkte fra EU-institu-

33 Et annet eksempel er standardenes rolle i den franske brystimplantatsaken, forklart i van Gestel, R., & van Lochem, P. J. P. M. (2020). Private standarder som erstatning for offentlig lovgivning? DOI: <https://doi.org/10.4337/9781788118415.00009>.

sjonene. Veien til tilgang kan likevel være lang og byrdefull. *Public.Resource.Org* presiserer kun at det var en «overriding public interest» i å gi tilgang til de fire harmoniserte standardene om leker. Dette reiser spørsmålet om hvorvidt en slik «overriding public interest» gjelder generelt for alle harmoniserte standarder, noe som foreløpig ikke er avklart.

Et spesielt og begrensende faktum i *Public.Resource.Org* er at det i forordning 1907/2006, spesifikt fremgår at bruken av nikkel i leketøy er regulert av en av standardene, og at det følger av dette at «the standards adopted by CEN are to be used as test methods for demonstrating the conformity of the products»<sup>34</sup> For å verifisere samsvar er det derfor ikke noe annet valg enn å gå til den relevante standarden, noe som gjør det åpenbart at standarden er obligatorisk. Det er ikke alle harmoniserte standarder som det henvises til i EU-regelverket på denne måten. Men bortsett fra standarden om terskelverdier for nikkel, la EU-domstolen til grunn at alle harmoniserte standarder som brukes for å skape en presumsjon om etterlevelse, i realiteten er en del av EU-retten, noe som i utgangspunktet skulle kunne gi en «overriding public interest» til fri tilgang til den aktuelle standarden.

Likevel, EU-domstolen har, gjennom *Public.Resource.Org*, opprettholdt en todelt tilnærming der harmoniserte standarder delvis er tilgjengelige på grunn av tvingende allmenne hensyn, og delvis begrenset på bakgrunn av opphavsrettslig beskyttelse. Dette sprikende resultatet er et tydelig symptom på implikasjonene ved å innlemme privatproduserte og opphavsbeskyttede kilder i EUs formelle lovgivning.

Konvensjonelle rettskilder, som ordinære lover og rettspraksis, er fritt tilgjengelige på nettet, uten at det er nødvendig å be om tilgang. Etter EU-domstolens avgjørelser er

34 *Public.Resource.Org*, avsnitt 79.

harmoniserte standarder formelt sett tilgjengelige, men ikke like enkelt som andre rettskilder. Dette reiser spørsmålet om det er lovlig, i henhold til de grunnleggende rettighetene som er nedfelt i TFEU og Charteret,<sup>35</sup> å begrense tilgangen til harmoniserte standarder, slik EU-kommisjonens praksis er i dag.

Det reiser også spørsmålet om begrensede rettskilder, som harmoniserte standarder, er egnet til å regulere svært komplekse områder som reiser flere grunnleggende samfunnsproblemer, slik som regulering av KI-systemer.

### 3. Bruk av harmoniserte standarder for å regulere KI-systemer

Ti standarder er under utvikling for å gi detaljerte regler for design, utvikling og bruk av KI-systemer. Standardene handler ikke bare om produkt-sikkerhet, men også om overholdelse av grunnleggende rettigheter. KI-systemer er i høyeste grad tekniske, men bruken av KI-systemer reiser samtidig en rekke samfunnsmessige spørsmål om personvern, diskriminering, sikkerhet med mer. I EU-kommisjonens anmodning om standardisering i tilknytning til KI-forordningen, som ble utstedt av 22. mai 2023, fremkommer det at «standards are important instruments to support the implementation of Union policies and legislation and to ensure a high level of protection of safety and fundamental rights for all persons in the Union.»<sup>36</sup>

Hensynet til grunnleggende rettigheter var ikke til stede da den nye tilnærmingen til harmonisering av standarder ble innført i 1985. Den gang var det utelukkende produktsikkerhet som sto i fokus. Så langt

35 Traktaten om Den europeiske unions virkemåte (TFEU), artikkel 15(3) og Pakten om grunnleggende rettigheter («Pakten»), artikkel 20, 42 og 47 (på engelsk «Charter of Fundamental Rights»).

36 EU-kommisjonens gjennomføringsbeslutning (Commission Implementing Decision), 22. mai 2023, C(2023)3215 final, fortalepunkt nr. 3

finnes det ingen harmoniserte standarder der hensynet til grunnleggende rettigheter spiller en dominerende rolle. De ti standardene som skal innføres for KI-systemer, vil derimot alle ha grunnleggende rettigheter som et vesentlig og overordnet hensyn. Standardene forventes å foreligge innen 30. april 2025.<sup>37</sup>

KI-forordningen trådte i kraft 1. august 2024. KI-forordningen definerer tre produkter som skal være underlagt harmoniserte standarder: høyrisiko-KI-systemer, generative KI-modeller og generative KI-modeller med systemisk risiko. Mandatet som ble gitt til de europeiske standardiseringsorganisasjonene 22. mai 2023, gjelder bare høyrisikosystemer for kunstig intelligens, fordi de to sistnevnte kategoriene ble inkludert i KI-forordningen på et senere tidspunkt.<sup>38</sup>

Det er ti krav til høyrisiko-KI-systemer, og det forventes mer detaljerte spesifikasjoner i standardene. De ti kravene er risikostyring, data og datastyring, åpenhet, menneskelig tilsyn, nøyaktighet, robusthet, cybersikkerhet, kvalitetsstyringssystem og samsvarsvurdering. Hensynet til grunnleggende rettigheter er nedfelt i alle kravene. For eksempel, fra kravet om risikohåndtering følger det at risiko skal identifiseres, inkludert risikoer som KI-systemet «can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose.»<sup>39</sup>

Et vanlig argument for tekniske standarder som supplement til lovgivning er behovet for den nyeste tekniske ekspertisen. Når det gjelder KI-systemer, er det imidlertid også et behov for samfunnsmessig bevissthet, ikke bare teknologiske ferdigheter, men også kunnskap om hvordan te-

knologien påvirker og påvirker samfunnet. Overholdelse av grunnleggende rettigheter krever nøye avveininger mellom til tider motstridende rettigheter og interesser.

Som påpekt av Martin Ebers,<sup>40</sup> er ikke harmoniserte standarder gjennomgått av offentlige organer. I «Blue Guide» om produktregulering utarbeidet av EU-kommisjonen i 2016 følger det at: «Union harmonisation legislation for products do not foresee a procedure under which public authorities would systematically verify or approve either at Union or national level the contents of harmonised standards».<sup>41</sup>

Det er uklart hvorfor offentlige myndigheter ikke kunne vært mer involvert. Sterkere involvering fra offentlige organer kan bidra til å skape større bevissthet rundt hvor grensen mellom formell lovgivning og standarder bør trekkes. Harmoniserte standarder bør i utgangspunktet angi konkrete og tekniske spesifikasjoner som knytter seg til krav angitt i formell lov. Bredere involvering vil også bidra til at avveingen av grunnleggende rettigheter blir bedre forankret. Disse avveiningene bør ikke ligge til standardiseringsorganisasjonene alene.

#### 4. Harmoniserte standarder kan være nyttig, så lenge alle har tilgang til dem

Uten harmoniserte standarder ville det fortsatt eksistert standarder. Det finnes mange standarder som virksomheter velger å følge frivillig, uten at det er lovpålagt.

Integrasjon mellom det private initiativer og formell lovgivning har flere fordeler. Harmonisering sikrer enhetlige europeiske standarder som er direkte knyttet til lovkrav. Ved å følge loven, inkludert de harmoniserte standardene, får virksomheter smidig tilgang til hele det indre markedet. I tillegg gir harmoniseringssystemet obligatorisk håndheving gjennom EU-domstolen og nasjonale domstoler. Dette kan være en bedre løsning enn å basere seg på frivillige, private standarder som lever sitt eget liv utenfor EUs offisielle rettsystem.

Personvernforordningen er et fremtredende eksempel på dette. Ingen harmoniserte standarder er knyttet til sikkerhetskravene i artikkel 32 i personvernforordningen, men det er vanlig å bruke ikke-harmoniserte standarder for å overholde kravene, slik som ISO27001:2017. Denne standarden etterspørres ofte i offentlige anbud.

Fortsatt bruk av harmoniserte standarder krever imidlertid visse forbedringer av den nåværende praksisen. For det første bør det gjøres helt klart at grunnleggende rettsstatsprinsipper trumfer opphavsretten. Tilgang til loven er en grunnleggende og absolutt rettighet som må respekteres, uavhengig av kommersielle interesser. For det andre bør det åpnes for deltakelse i private lovgivningsprosedyrer, med obligatorisk deltakelse fra offentlige organer. Selv om private organisasjoner er involvert, bør det aldri være tvil om at det er de offentlige EU-institusjonene og medlemslandene som er ansvarlige for å sikre at grunnleggende rettigheter blir respektert.

*Av Lars Arnesen, stipendiat ved Senter for rettsinformatikk (SERI), Universitetet i Oslo.*

37 Ibid. artikkel 1.

38 EU-kommisjonens gjennomføringsbeslutning (Commission Implementing Decision), 22. mai 2023, C(2023)3215 final.

39 KI-forordningen, artikkel 9(2)a).

40 Martin Ebers, Standardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act, i: Larry A. DiMatteo/Michel Cannarsa/Cristina Poncibò (red.), The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, under utgivelse, 22 sider, Cambridge University Press 2022.

41 Europakommisjonen, «The 'Blue Guide' on the implementation of EU products rules 2016.» EUT 2016 C 272/1, 41, 45.

# Fra åndsverk til algoritme: Navigering av opphavsrett i KI-alderen

Av Veronika Lundqvist og Haakon Føyen

## 1. Innledning

Et tema som fortsetter å være aktuelt er diskusjonene rundt rettighetene til data som de nye kunstig intelligens (KI) modellene er trent på. KI-tjenester som ChatGPT, Midjourney, Sora og Suno kan etter noen enkle ledetekster, gjerne omtalt som «prompts», generere større mengder nytt innhold av tekst, bilder, video og lyd. Dette er muliggjort ved at KI-modeller har blitt trent på enorme mengder data, som i mange tilfeller inneholder opphavsrettsbeskyttede verk som ligger offentlig tilgjengelig på internett.

Bruk av slike verk har startet en rekke søksmål fra rettighetshavere mot teknologiselskaper bak KI-tjenester over hele verden. Et illustrativt eksempel er den pågående tvisten mellom New York Times, OpenAI og Microsoft som angår hvorvidt OpenAI hadde rett til å trene KI-modellene sine på innholdet i artiklene til New York Times, og deretter selge KI-tjenester basert på disse.

I denne artikkelen vil vi først gi et kort innblikk i diskusjonen mellom KI-selskaper og rettighetshavere internasjonalt. Deretter vil vi vurdere hvorvidt norsk opphavsrett tillater bruk av beskyttede verk i opptreningen av KI-modeller. Rettsområdet vil bli preget av ny lovgivning, noe vi også vil gå inn på før vi ser på det «opphavsrettslige markedet» og kommer med noen avsluttende refleksjoner.

## 2. Det internasjonale bildet

### 2.1 Overordnet

Det pågår i dag en rekke større tvister internasjonalt mellom rettighets-



Veronika Lundqvist

havere og KI-selskaper.<sup>1</sup> Et av de største og mest kjente søksmålene, er tvisten som pågår i USA mellom The New York Times (NYT) og OpenAI samt Microsoft. I begynnelsen av 2023 klagde NYT på at deres innhold ble brukt i KI-trening uten godkjenning eller kompensasjon. Etter mislykkede forhandlinger saksøkte NYT begge selskapene for opphavsrettskrenkelser, med påstander om tap på milliarder av dollar. NYT krever at KI-selskapene stenger sine chatbot-tilbud og destruerer treningsdata som bruker deres opphavsrettsbeskyttede materiale. Saken symboliserer spenningen mellom rettighetshavere og KI-utviklere, og kan sette en viktig presedens i det juridiske landskapet fremover.

Etter at NYT saksøkte OpenAI, fulgte i april 2024 åtte andre større avisforlag eid av investeringsgiganten Alden Global Capital etter, med søksmål mot Microsoft og OpenAI



Haakon Føyen

for krenkelse av deres rettigheter. I motsetning til NYT, prøvde avisene eid av Alden Global Capital ikke å forhandle med OpenAI og Microsoft før søksmål ble inngitt.<sup>2</sup> Andre rettighetshavere, som Financial Times, Associated Press og Axel Springer, har i stedet gått veien om forhandlinger og inngått lisensieringsavtaler med KI-selskaper for noen millioner av dollar årlig. Lisensverdien står i kontrast til NYT's påstand om tap på milliarder av dollar.<sup>3</sup> Om det lønner seg for rettighetshavere å velge forhandlingsveien eller søksmålsveien, gjenstår å se.

Spørsmålet som kan få store økonomiske konsekvenser for både teknologiselskaper og rettighetshavere er: Hvordan reguleres bruk av åndsverk til KI-utvikling?

1 <https://chatgptiseatingtheworld.com/2023/12/27/master-list-of-lawsuits-v-ai-chatgpt-openai-microsoft-meta-midjourney-other-ai-cos/>

2 [https://www.axios.com/2024/04/30/microsoft-openai-lawsuit-copyright-newspapers-alden-global?utm\\_source=tldrui](https://www.axios.com/2024/04/30/microsoft-openai-lawsuit-copyright-newspapers-alden-global?utm_source=tldrui)

3 <https://www.ft.com/content/33328743-ba3b-470f-a2e3-f41c3a366613>

## 2.2 Internasjonale forskjeller

Opphavsretten i Norge, USA og flertallet av andre land i verden er bygget på felles internasjonale avtaler som Bernkonvensjonen om vern av litterære og kunstneriske verk (1886), og andre komplementerende konvensjoner. Et felles utgangspunkt internasjonalt, er at rettighetshavere har eksklusive rettigheter til sine åndsverk med mindre det foreligger unntak eller andre begrensninger i rettigheten. Det eksisterer imidlertid en rekke større forskjeller i opphavsrettslovgivingen mellom de ulike landene.

I USA finnes det et «*fair use*»-unntak, som begrenser opphavsretten og åpner for fri bruk til blant annet kommentar, kritikk, nyhetsformidling, undervisning og forskning. Unntaket har historisk gitt en del spillerom for utviklere av ny teknologi i USA.<sup>4</sup> Tilsvarende generelt unntak finnes ikke i Norge eller i EU. OpenAI og Microsoft vil under amerikansk rett kunne argumentere for at transformasjon av innhold gjort av KI-modeller som ChatGPT er «*fair use*».

Følgene av søksmålet anlagt av NYT kan få større praktiske konsekvenser. En avgjørelse til fordel for NYT vil kunne utløse en bølge av lignende søksmål i USA. Dette kan medføre at KI-selskaper undersøker kildene til sine treningsdata nærmere og mer aktivt søker lisenser for bruk av treningsdata. Dette kan bremse tempoet i KI-utviklingen og skifte fokus mot modeller trent på andre datasett. Saken kan også påvirke hvordan KI oppfattes i samfunnet. Hvis KI anses som et verktøy som krenker rettighetene til innholdsskapere, kan det føre til strengere reguleringer og en mer forsiktig tilnærming fra investorer og interessenter i KI-industrien. Nye lisensmodeller er også en sannsynlig konsekvens.

4 [https://southerncalifornialawreview.com/wp-content/uploads/2018/01/83\\_797.pdf](https://southerncalifornialawreview.com/wp-content/uploads/2018/01/83_797.pdf)

Søksmålet mellom NYT, OpenAI og Microsoft blir derfor en lakmustest for fremtiden til KI-utvikling og sameksistens med rettighetshaverne. De største KI-selskapene er i dag basert i USA, og en rettsavklaring der vil følgelig kunne få betydning for hvordan KI tilbys i resten av verden.

## 3. Relevante regler for bruk av verk i opptreningen av KI-modeller i Norge

### 3.1. Åndsverkloven

I Norge reguleres opphavsretten av åndsverkloven, som gjennomfører EUs direktiver om opphavsrett, herunder Infosoc-direktivet. Spørsmålet om bruk av åndsverk i opptreningen av generative KI-modeller er tillatt, vil derfor langt på vei måtte løses likt i Norge og i EU.

Det er kun åndsverk som er beskyttet av opphavsrett, jf. åvl. § 2. Utviklingen av generative KI-modeller som f.eks. språkmodeller og bildegenereringsprogrammer, krever prosessering av enorme mengder relevante data (tekst, bilde, video og lyd). Innholdet skrapes gjerne opp fra internett via automatiserte prosesser kalt «*crawling*»<sup>5</sup>, hvilket betyr at KI-modeller kan være trent på åndsverk fra hele verden som ligger offentlig tilgjengelige på internett.<sup>6</sup>

Videre må det vurderes om KI-selskapene bruker åndsverkene på en måte som faller innenfor rettighetshaverens enerett. Det følger av åvl. § 3 at *eksemplarframstilling* og *tilgjengeliggjøring for allmennheten* av verk som faller innenfor eneretten. Prosessen med å skrape opp verk fra internett og behandle disse til

5 <https://anifitai.medium.com/overview-of-web-crawling-technologies-for-generative-ai-2315953c2b0c>

6 OpenAI hevder f.eks. at det ville være umulig å trene KI uten bruk av opphavsrettslig beskyttet materiale: <https://www.euronews.com/next/2024/01/09/openai-says-its-impossible-to-train-ai-without-copyrighted-materials>

å trene opp algoritmer, innebærer som hovedregel at det på et tidspunkt tas en kopi av verket. I så fall vil det foreligge en eksemplarframstilling i lovens forstand.

” Innholdet skrapes gjerne opp fra internett via automatiserte prosesser kalt «*crawling*», hvilket betyr at KI-modeller kan være trent på åndsverk fra hele verden som ligger offentlig tilgjengelige på internett.

Til slutt må det vurderes om bruken likevel kan være tillatt iht. en av unntaksbestemmelsene i åndsverkloven. Det finnes ingen unntaksbestemmelser som eksplisitt hjemler bruk av åndsverk til opptrening av generative KI-modeller, og hvert tilfelle må vurderes konkret. For eksempel kan det tenkes at unntaket for midlertidige kopier kan være relevant i forbindelse med denne typen bruk. Med mindre bruken er dekket av en unntaksbestemmelse, må i utgangspunktet utviklere av generative KI-modeller innhente forhåndssamtykke fra rettighetshaverne. Det har imidlertid kommet nytt regelverk fra EU som gjør rettskildesituasjonen mer sammensatt.

### 3.2. Digitalmarkedsdirektivet

Digitalmarkedsdirektivet fra EU (2019/790) («*DSM-direktivet*») er i ferd med å bli gjennomført i norsk rett. Direktivet inneholder to opphavsrettslige unntak for tekst- og datautvinning, som har blitt mye diskutert etter utviklingen av de store generative KI-modellene i 2022. Den mest omdiskuterte bestemmelsen er DSM-direktivets art. 4, som foreslås innført av KUD i ny §§ 50 e) i åndsverkloven. I innhold til den nye bestemmelsen er

det tillatt å bruke verk i tekst- og datautvinning, så lenge rettighetshaveren ikke eksplisitt reserverer seg mot dette.

” Med mindre bruken er dekket av en unntaksbestemmelse, må i utgangspunktet utviklere av generative KI-modeller innhente forhåndssamtykke fra rettighetshaverne.

«Tekst- og datautvinning» (ofte omtalt som Text and Data Mining eller «TDM») betegner den tekniske prosessen med å samle inn og analysere store mengder data, for å fremskaffe informasjon. Teknologien gjør det mulig å analysere større mengder data, mer effektivt enn et menneske hadde kunnet gjøre. Derfor spiller tekst- og datautvinning en viktig rolle innenfor blant annet forskning og innovasjon.<sup>7</sup>

Overordnet innebærer reguleringen i DSM-direktivet en anerkjennelse av at det burde være forholdsmessig enkelt å gjennomføre tekst- og datautvinning, da det er en viktig teknisk komponent for kunnskapsutvikling og innovasjon. Samtidig legger regelverket opp til at de rettighetshaverne som ønsker det, kan unnta verkene sine fra slik bruk.

### 3.3. Om trening av KI-modeller omfattes av unntakene for tekst- og datautvinning

Definisjonen av tekst- og datautvinning omfatter etter sin ordlyd innsamling og analysering av data til også å utvikle generative KI-modeller. I norsk sammenheng ser det også ut til at departementet legger til grunn en tolkning om at art.

4 regulerer generativ KI.<sup>8</sup> Standpunktet er forståelig, da EU-lovgiver selv anerkjenner tilknytningen mellom tekst- og datautvinning og KI i KI-forordningen (mer om dette senere). Standpunktet har samtidig vist seg å være kontroversielt, da bestemmelsen har blitt kritisert særlig av representanter for rettighetshavere.<sup>9</sup>

Det mest omdiskuterte aspektet ved art. 4 er *hvordan* rettighetshaverne skal kunne reservere seg iht. bestemmelsens tredje ledd. Reservasjonen skal iht. direktivteksten gjøres «*in an appropriate manner, such as machine-readable means in the case of content made publicly available online*». Slik begrenses rettighetshavernes valgfrihet når det gjelder metode å reservere seg på, men i mangel av en felles standard er det flere ulike oppfatninger om hvilke metoder som er tilstrekkelig for å ha oppnådd en gyldig reservasjon iht. direktivet.<sup>10</sup>

Fra teknologiselskapenes side er det viktig at reservasjonene er maskinleselige og kan gjenkjennes automatisk. En måte å reservere seg på er ved bruk av robots.txt (robots exclusion standard) i nettsidens kode. En slik løsning tilbys av de fleste teknologiselskaper, og innebærer at de automatiserte web-crawlerne ikke skrapet opp innholdet på den aktuelle nettsiden. Andre måter innebærer tekniske tilgangssperrer på nettsider, vannmerking av filer, o.l.<sup>11</sup> Fordelen med disse metodene, og særlig robots.txt, er at de kan gjenkjennes av maskiner og dermed automatisk hindrer at nett-

siden blir kopiert og brukt til trening av KI. Disse metodene har imidlertid blitt kritisert av rettighetshavere, fordi vedkommende må ha kontroll over samtlige nettsider som inneholder verket og samtlige verkskopier som finnes tilgjengelig på nett.

” Fra teknologiselskapenes side er det viktig at reservasjonene er maskinleselige og kan gjenkjennes automatisk.

En annen utfordring er at en stor mengde bruk skjer utenfor rettighetshavernes kontroll, for eksempel lovlige parodier eller sitater. Noen KI-selskaper har tilgjengeliggjort en såkalt «opt-out»-funksjon som gjør det mulig for rettighetshaveren å melde ifra om verk som de ikke ønsker at skal brukes i fremtidige oppdateringer av KI-modellen.<sup>12</sup> Spesifikke verk kan dermed lukes ut av treningsmaterialet, uavhengig av hvilken nettside det kommer fra. Også denne funksjonen har blitt kritisert av rettighetshavere for å være lite brukervennlige, da rettighetshaverne må laste opp ett og ett verk om gangen, og prosessen må gjentas for hver KI-modell som til enhver tid finnes.<sup>13</sup>

Rettighetshavere er på sin side opptatt av at de på en enkel måte skal kunne formidle til KI-selskaperne hvilke verk de ønsker å reservere mot bruk til tekst- og datautvinning. De ønsker brukervennlige reservasjonsmetoder som vil fungere for samtlige verk, herunder mer generelle reservasjoner via nettsiders

7 Se DSM-direktivets forale pkt. 8 og 18

8 Se KUD sitt høringsnotat s. 37: <https://www.regjeringen.no/contentassets/449f5b4495644c2af1df7680d1649e5/horingsnotat-221123.pdf>

9 Se f.eks. høringsvaret til Kunstnernettverket s. 1

10 [https://openfuture.eu/wp-content/uploads/2023/09/Best\\_practices\\_for\\_optout\\_ML\\_training.pdf](https://openfuture.eu/wp-content/uploads/2023/09/Best_practices_for_optout_ML_training.pdf)

11 Les mer om ulike metoder <https://www.theverge.com/24063327/ai-art-protect-images-copyright-generators>

12 F.eks. OpenAI, se <https://techcrunch.com/2024/05/07/openai-says-its-building-a-tool-to-let-content-creators-opt-out-of-ai-training/>

13 <https://www.businessinsider.com/openai-dalle-opt-out-process-artists-enraging-2023-9?amp>

brukervilkår,<sup>14</sup> eller i form av erklæring til omverdenen om at «ingen verk av rettighetshaver X skal brukes». Flere kollektive forvaltningsorganisasjoner har derfor publisert såkalte «kollektive reservasjoner» på sine nettsider, som er ment å dekke alle verkene de forvalter opphavsretten til.<sup>15</sup> Utfordringen med denne typen reservasjoner er at de ikke nødvendigvis gjenkjennes av maskiner.

Fordi det råder usikkerhet og uenighet om hvordan det kan være mulig å reservere verkene sine iht. art. 4 - og dermed hvilke verk som kan brukes - er det vanskelig for både KI-selskaper og rettighetshavere å innrette seg på måter som ivaretar de motstridende interessene. Tekst- og datautvinnings-sunn-takene ble vedtatt i EU før utviklingen av generative KI-modeller slik vi kjenner dem i dag. Det ser ikke ut til at lovgiver i tilstrekkelig grad har vurdert hvordan interessene knyttet til utviklingen av KI og opphavsrett skal balanseres opp mot hverandre i denne konteksten. Som følge av dette foreligger det for øyeblikket usikkerhet rundt hva som utgjør - og bør utgjøre - gjeldende rett.

#### 4. Den kommende KI-forordningen

Den kommende forordningen for kunstig intelligens (KI-forordningen, også kjent som EU AI Act) skal adressere utfordringene og mulighetene som følger med utvikling og bruk av KI-teknologier. Den endelige teksten er vedtatt og forordningen vil etter all sannsynlighet komme til å bli innlemmet i EØS-avtalen og bli en del av norsk rett.

Overordnet adresserer forordningen risikostyring, transparens og

etiske hensyn rundt KI, og stiller særlig strenge krav til høyrisiko KI-systemer. KI-forordningen vil imidlertid også få følger for såkalte «general-purpose» (heretter ‘generelle’) KI-modeller slik disse er definert i artikkel 3(1) avsnitt 63. Definisjonen omfatter modellene som populære KI-tjenester som ChatGPT, Gemini og Copilot er trent på. Selv om det står eksplisitt i KI-forordningen at den ikke påvirker håndhevelsen av opphavsrettsreglene fastsatt i Unionsretten<sup>16</sup>, så vil særlig transparensreglene ha relevans for rettighetshavere.

” Fordi det råder usikkerhet og uenighet om hvordan det kan være mulig å reservere verkene sine iht. art. 4 – og dermed hvilke verk som kan brukes - er det vanskelig for både KI-selskaper og rettighetshavere å innrette seg på måter som ivaretar de motstridende interessene.

Under den kommende KI-forordningen kan ikke KI-selskaper lenger nekte å informere om treningsdata er opphavsbeskyttet eller ikke. KI-forordningen artikkel 53(1) (d) pålegger tilbydere av generelle KI-systemer å utarbeide og gjøre offentlig tilgjengelig et tilstrekkelig detaljert sammendrag om innholdet som blir brukt til opplæring av KI-modeller for generell bruk. Sammenbraget av innholdet skal skje i henhold til en standard som skal utarbeides og håndheves av AI Office.

KI-forordningens bestemmelser regulerer ikke nøyaktig hvilke krav

som AI Office vil legge til grunn, men forordningens fortalepunkter inneholder veiledning som AI Office etter all sannsynlighet vil rette seg etter. Det spesifiseres i fortalepunkt 108 at tilbydere av generelle KI-modeller skal offentliggjøre en erklæring med sammendrag av innholdet til dataene som er brukt til treningen av modellen. Det følger av fortalepunkt 107 at sammenbraget skal være omfattende i sin rekkevidde for å gjøre det lettere for parter med legitime interesser, som rettighetshavere, å utøve og håndheve sine rettigheter under europeisk rett.

Det fremgår også at AI Office bør føre tilsyn med om tilbydere av generelle KI-modeller oppfyller disse forpliktelsene. Merk likevel at fortalepunkt 108 *ikke* legger opp til at AI Office skal gjøre en verk-forverk-vurdering av treningsdata med tanke på overholdelse av opphavsrett.

KI-forordningen legger også opp til et samspill med de nye reglene i DSM-direktivet ved at leverandører av generelle KI-modeller blir oppfordret til å ha på plass retningslinjer for å overholde opphavsrett. Det blir spesifikt fremhevet i fortalepunkt 106 at leverandører av generelle KI-modeller skal ha på plass rutiner for å sørge for at generelle KI-modeller klarer å identifisere og etterkomme de nye reglene til reservasjon for tekst- og datautvinning etter DSM direktivet artikkel 4(3) omtalt tidligere i denne artikkelen.

” Under den kommende KI-forordningen kan ikke KI-selskaper lenger nekte å informere om treningsdata er opphavsbeskyttet eller ikke.

14 <https://copyrightblog.kluweriplaw.com/2024/07/22/machine-readable-or-not-notes-on-the-bearing-in-laion-e-v-vs-kneschke/>

15 <https://copyrightblog.kluweriplaw.com/2024/01/25/ai-data-mining-french-music-collecting-society-sacem-opts-out-with-what-consequences/>

16 Jf. fortalepunkt 108.



Det antas at KI-forordningens regler om transparens rundt treningsmateriale både vil medføre bedre etterrettelighet og tilrettelegge for at rettighetshavere kan ivareta sine rettigheter.

## 5. «Det opphavsrettslige markedet» og lisensavtaler

På tross av mye uklarhet rundt detaljene i gjeldende rett for bruk av åndsverk i KI-utvikling, er det klart at rettighetshaverne skal ha muligheten til å forhindre at verkene deres brukes til å utvikle KI. Samtidig ligger det store verdier i data som kan brukes til KI-trening, noe som åpner for nye lisensieringsmuligheter. Det har vokst frem flere slike initiativer internasjonalt. Spørsmålet som oppstår er hvordan bruken eventuelt kan klarenes.

Opphavsretten er en individuell rettighet, og utgangspunktet er at de som ønsker å bruke verk, må innhente tillatelse hos hver enkelt rettighetshaver. Individuell klaring vil ofte være lite hensiktsmessig der det skal brukes en stor mengde verk, som f.eks. ved KI-utvikling. Enkelte aktører eier et stort sett med rettigheter, som f.eks. forlag og nyhetsutgivere. Derfor ser vi eksempler på lisensiering med aktører som Financial Times, Associated Press og Axel Springer (som nevnt i punkt 2).

For enkeltstående rettighetshavere som billedskapere, forfattere og komponister, har det utviklet seg en praksis for *kollektiv klaring* via organisasjoner som representerer et større antall rettighetshavere. Slike organisasjoner kan etter omstendighetene regnes som en *kollektiv forvaltningsorganisasjon*.<sup>17</sup> Kollektive forvaltningsorganisasjoner har som sitt hovedformål å inngå lisensavtaler på vegne av rettighetshaverne de representerer. Disse utgjør viktige aktører i

17 Se Lov om kollektiv forvaltning av opphavsrett mv. § 3 (a)

lisensieringsmarkedet i Europa, inkl. i Norge. I Norge finnes det 6 kollektive forvaltningsorganisasjoner, Norwaco, Kopinor, TONO, BONO, Gramo og Music Nest Norway.

Løsninger basert på avtaleinngåelse kan gi en fleksibel måte å balansere de motstridende interessene på. Den sterke tradisjonen med kollektiv forvaltning i Norden gir KI-utviklere mulighet til å søke lokale løsninger basert på avtaler med respektive rettighetshaverorganisasjoner/kollektive forvaltningsorganisasjoner.<sup>18</sup>

Et annet forslag som har blitt diskutert i juridiske fagmiljøer er *tvungen kollektiv forvaltning*.<sup>19</sup> Eksempler på tvungen kollektiv forvaltning er bestemmelser om tvangslisens og andre vederlagsordninger, f.eks. vederlag for offentlig fremføring og overføring til allmennheten av lydopptak jf. åvl. § 21 og privatkopieringskompensasjonsordningen jf. åvl. § 26. Felles for slike ordninger er at de ved lov gir rett til å bruke opphavsrettslig beskyttede verk på visse måter, mot oppfyllelse av en tilhørende betalingsplikt. Da slike ordninger krever eksplisitt lov hjemmel, vil en eventuell løsning basert på tvungen kollektiv forvaltning kreve stor grad av nasjonal og internasjonal koordinering, og sannsynligvis flere år med lovgivningsarbeid.

## 6. Avslutning

Den rettslige situasjonen for bruk av opphavsrettslig beskyttede verk i utviklingen av KI er uavklart, både i Norge og internasjonalt. I Norge

18 Flere av de norske kollektive forvaltningsorganisasjonene, Kopinor, Norwaco og BONO, nevner lisensavtaler som mulig løsning i sine høringssvar til KUD ifm. gjennomføringen av DSM-direktivet

19 Se f.eks. <https://copyrightblog.kluweriplaw.com/2023/10/19/generative-ai-digital-constitutionalism-and-copyright-towards-a-statutory-remuneration-right-grounded-in-fundamental-rights-part-2>

ligger flere av problemstillingene nå på Kultur- og likestillingsdepartementet sitt bord i forbindelse med gjennomføringen av DSM-direktivet. Departementet har imidlertid begrenset med spillerom, og det er først og fremst utviklingen som skjer i EU, herunder rettspraksis fra EU-domstolen, som vil få betydning. Da de største KI-selskapene er amerikanske og for øvrig opererer internasjonalt, vil også lover og rettspraksis fra land som USA forme bransjepraksis for større og mindre KI-aktører.

” Hvordan regelsettene i de ulike landene vil forholde seg til hverandre til slutt, gjenstår å se. Store forskjeller vil være lite hensiktsmessig av forutberegnelighetshensyn, og gi ulike spilleregler i det internasjonale KI-kappløpet.

I mellomtiden er det sannsynlig at det vil vokse frem nasjonale forskjeller. I land som Norge hvor det er en sterk tradisjon for kollektiv forvaltning av opphavsrett, og tilsynelatende en politisk vilje for å tilrettelegge for løsninger som ivaretar rettighetshaverne,<sup>20</sup> kan det være rom for sentraliserte initiativer som sikrer de motstridende interessene ved forhandlinger og enighet.

Hvordan regelsettene i de ulike landene vil forholde seg til hverandre til slutt, gjenstår å se. Store forskjeller vil være lite hensiktsmessig av forutberegnelighetshensyn, og gi ulike spilleregler i det internasjonale KI-kappløpet. Muligens vil «Brussel-effekten», og det

20 Se f.eks. «Mimir-prosjektet»: [https://www.nb.no/content/uploads/2024/08/Mimirprosjektet\\_teknisk-rapport.pdf](https://www.nb.no/content/uploads/2024/08/Mimirprosjektet_teknisk-rapport.pdf)

at EU har vært tidlig ute med å markere seg i KI-sammenheng med KI-forordningen, bidra til at EU-retten får betydning for de store selskapene. I Norge blir det viktig å følge med på den internasjonale regelutviklingen så vel som nasjonale initiativer.

*Veronika Lundqvist, juridisk rådgiver i BONO, den norske kollektive forvaltningsorganisasjonen for visuelle verk. Veronika har særskilt kunnskap om skjæringspunktet mellom opphavsrett og teknologi, og utfordringer for rettighetsbavere i møte med teknologiselskaper bak plattformtjenester, KI-tjenester, o.l.*

*Haakon Dahl Føyen, advokat Advokatfirmaet Føyen AS. Haakon arbeider hovedsakelig med problemstillinger knyttet til teknologirett, IT-avtaler, immaterialrett og personvern, og har en lidenskapelig interesse for kunstig intelligens og legal tech.*



Illustrasjon: Colourbox.com

# Mot ett starkare skydd för den enskildes integritet

Av Gaëlle Bjurström

I en artikel i Lov & Data som publicerades den 26 mars 2024 (se *Databasverksamheter med grundlagsskydd vägras allmänna handlingar med hänvisning till GDPR*) kommenterar författarna den senaste praxisutvecklingen genom vilken svenska domstolar ansett att hinder kan uppställas mot offentliggöranden av uppgifter om enskildas lagöverträdelser i sökbara databaser och andra medier. Författarna menar att en sådan rättstillämpning förefaller stå i konflikt med grundlag och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ("dataskyddslagen"), möjligen även i betydelsen att den skulle äventyra "principerna för statskicket".

Den 14 maj 2024 publicerade Integritetsskyddsmyndigheten ("IMY") ett rättsligt ställningstagande (Rättsligt ställningstagande IMYRS 2024:1 – Klagomål mot söktjänster med utgivningsbevis, dnr 2024/1234), där myndighet ger sin syn på flera av dessa frågeställningar. IMY:s ställningstagande grundar sig bland annat på en genomgång av förhållandet mellan EU-rätt och svensk rätt (inklusive grundlag) och den senaste praxisutvecklingen på området. Nedan redovisas huvuddragen i myndighetens resonemang. Dessutom ges några kommentarer till den pågående rättsutvecklingen.

## Konflikt med grundlag?

I sitt ställningstagande noterar IMY bl.a. att den svenska lagstiftaren, genom 1 kap. 7 § första stycket dataskyddslagen, har gett bestämmelserna i tryckfrihetsförordningen ("TF") och yttrandefrihets-



Gaëlle Bjurström

grundlagen ("YGL") företräde framför EU:s förordning 2016/679 ("GDPR") och dataskyddslagen. IMY konstaterar även att Europeiska kommissionen har uttryckt tvivel i fråga om Sverige därigenom har åstadkommit en rimlig balans mellan skyddet för personuppgifter och yttrandefriheten (se dir. 2023:145 s. 9 och Ju2019/01709).

” IMY konstaterar även att Europeiska kommissionen har uttryckt tvivel i fråga om Sverige därigenom har åstadkommit en rimlig balans mellan skyddet för personuppgifter och yttrandefriheten.

Vad gäller skyddet för databaser som publiceras på internet konstaterar IMY följande. Publiceringar på internet faller som huvudregel utanför YGL:s tillämpningsområde. Databasregeln i 1 kap. 4 § YGL,

som kan ge grundlagsskydd för en databas som innehåller uppgifter av betydelse för det allmänna meningsutbytet eller samhällsdebatten, utgör således ett undantag från huvudregeln. Syftet med detta undantag har aldrig varit att skydda databaser som utgör rena personregister. I grundlagsförarbetena framhölls istället detta som ett «worst-case scenario» som skulle kunna leda till allvarliga integritetskränkningar (se prop. 1997/98:115 s. 67).

IMY påpekar vidare att rättspraxis, såväl på EU-nivå som på svensk nivå, tyder på att 1 kap. 7 § första stycket dataskyddslagen (som ger TF och YGL företräde framför GDPR och dataskyddslagen) inte kan tillämpas fullt ut på den publicering av personuppgifter som utförs av söktjänster med utgivningsbevis. EU-domstolen har fastslagit att varje begränsning och undantag från de grundläggande rättigheterna till privatlivet och skydd för personuppgifter, även om de är tillåtna enligt GDPR, måste föregås av en proportionalitetsbedömning (se exempelvis EU-domstolens dom den 22 juni 2021, Latvijas Republikas Saeima, C-439/19, EU:C:2021:504). EU-domstolen har också understrukit behovet av en sammanjämkning mellan allmänhetens tillgång till allmänna handlingar med de grundläggande rättigheterna avseende respekt för privatlivet och skydd för personuppgifter (se EU-domstolens dom den 7 mars 2024, Endemol Shine Finland Oy, C-740/22, EU:C:2024:216, p. 55). Flera svenska domstolar har konstaterat att 1 kap. 7 § första stycket

dataskyddslagen inte kan tillämpas fullt ut på den publicering av personuppgifter som utförs av söktjänster med utgivningsbevis (se exempelvis Hovrätten för Övre Norrlands beslut den 28 mars 2024, dnr 2024/91 och Kammarrätten i Stockholms dom den 22 juni 2023 i mål nr 1128-23. Avgörandet har överklagats till Högsta förvaltningsdomstolen, se HFD:s pågående mål nr 4588-23). Vidare har Attunda tingsrätt begärt ett förhandsavgörande från EU-domstolen i frågan om det skydd som YGL ger söktjänsterna vid publicering är förenligt med GDPR (se Attunda tingsrätts beslut den 1 mars 2024 i mål nr T 3743-23).

### Äventyras "principerna för statsskicket" om EU-rätten ges företräde framför svensk rätt?

När det gäller EU-rättens förhållande till svensk rätt konstaterar IMY att EU-rätten har företräde framför svensk rätt (inklusive svensk grundlag), innebärande att svensk rätt inte får strida mot eller hindra tillämpningen av EU-rätten, och att EU-rätten ska ges företräde vid en eventuell konflikt mellan de två rättsordningarna. Det finns inte heller något förbehåll i det svenska anslutningsavtalet till EU i fråga om vilken normgivningskompetens som överlätts på TF- och YGL-området. Av 10 kap. 6 § första stycket RF framgår dock att riksdagen inte kan överlåta beslutanderätt till EU för sådant som rör principerna för statsskicket. Enligt förarbetena omfattar dessa principer förbudet mot censur, ansvarighetssystemet och andra viktiga principer i TF och YGL (se bet. 1993/94:KU21 s. 27). Argument som talar emot att det frivilliga grundlagsskyddet som typiskt sett används av söktjänster skulle kunna anses röra principerna för statsskicket är dock enligt IMY bl.a. att sådana söktjänster inte är en form av publiceringar som grundlagsstif-

taren har haft för avsikt att skydda, att grundlagsstiftaren genom 1 kap. 20 § YGL har begränsat grundlagsskyddet för söktjänster som publicerar känsliga personuppgifter och att en ny utredning pågår i syfte att stärka skyddet för den personliga integriteten när personuppgifter offentliggörs i sådana söktjänster (Dir. 2023:145).

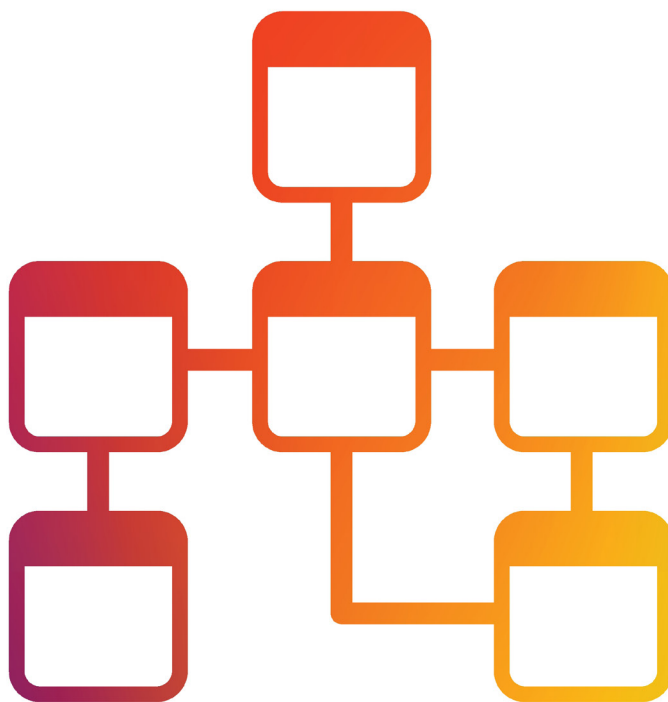
### IMY:s slutsats

Mot bakgrund av det ovan nämnda och med hänsyn till det stora antal klagomål som IMY under lång tid har mottagit från enskilda som upplever den omfattande publiceringen och spridningen av personuppgifter som sker genom söktjänster med utgivningsbevis som mycket kränkande och oroande, anser IMY sig (med ändring av sin tidigare inställning i frågan) ha behörighet att inleda tillsyn med anledning av klagomål mot den publicering av personuppgifter som sker i söktjänster med utgivningsbevis.

### Tillämpning av IMY:s resonemang och slutsatser i andra frågor

IMY:s ställningstagande framstår som välmotiverat, välgrundat och i överensstämmelse med den pågående rättsutvecklingen, där den enskildes integritet tillmäts allt högre vikt. Även om IMY:s ställningstagande är begränsat till frågan om IMY:s behörighet att inleda tillsyn med anledning av klagomål mot den publicering av personuppgifter som sker i söktjänster med utgivningsbevis, bör IMY:s genomgång och tolkning av rättsläget kunna användas för att besvara andra, likartade, frågor.

Exempelvis mottar myndigheter enligt offentlighets- och sekretesslagen ("OSL") ett stort antal begäranden om utlämnande av allmänna handlingar som får anses ligga utanför det kärnområde som offentlighetsprincipen syftar till att skydda. Offentlighetsprincipen används bland annat av enskilda för att få



information om en grannes elförbrukning, störningsanmälningar, ekonomi, m.m. Sådana begäranden kan svårligen anses omfattas av grundlagens syfte. Lagstiftaren har begränsat offentlighetsprincipen genom att i 21 kap. 7 § OSL ange att sekretess föreligger om det efter utlämnande kan antas att uppgifterna kommer att behandlas i strid med GDPR, dataskyddslagen eller 6 § etikprövningslagen. Det s.k. frågeförbudet i 2 kap. 14 § tredje stycket TF hindrar dock en myndighet från att efterforska vem det är som begär att få ta del av en handling eller vilket syfte han eller hon har med sin begäran, i större utsträckning än som behövs för att myndigheten ska kunna pröva om hinder föreligger mot att handlingen lämnas ut. Enligt ett JO-beslut måste det finnas en konkret omständighet (massuttag eller s.k. selekterade uppgifter) för att en myndighet ska ha rätt att ställa frågor för att ta reda på den tilltänkta användningen av personuppgifter (JO:s beslut den 28 augusti 2013, dnr 4171-2011). För att kunna göra den proportionalitetsbedömning som krävs enligt EU-domstolens praxis, bör dock myndigheter kunna ställa frågor även i andra fall (såsom om begäran om utlämnande omfat-

tar känsliga eller extra skyddsvärda personuppgifter eller personuppgifter som rör lagöverträdelse) för att kunna bedöma om personuppgifter får lämnas ut eller inte. I annat fall har myndigheterna ingen möjlighet att göra den avvägning som krävs enligt EU-domstolens praxis. Mot bakgrund av EU-rättens företräde framför svensk lag (inklusive grundlag) och eftersom begäranden som ligger utanför offentlighetsprincipens kärnområde inte kan anses röra principerna för statskicket, kan det inte finnas något hinder för myndigheter enligt OSL att, trots frågeförbudet i RF och JO:s beslut i frågan, ställa de frågor som behövs för att göra den proportionalitetsbedömning som enligt EU-rätten måste göras inför varje utlämnande av personuppgifter.



Sammanfattningsvis sker en utveckling mot ett starkare skydd för den personliga integriteten. Utvecklingen är driven av EU-rätten, som har företräde framför svensk rätt.

Sammanfattningsvis sker en utveckling mot ett starkare skydd för den personliga integriteten. Utvecklingen är driven av EU-rätten, som har företräde framför svensk rätt (inklusive svensk grundlag). Inte minst mot bakgrund av syftet med reglerna i TF och YGL är det svårt att se på vilket sätt en tillämpning av EU-rätten som tillmäter den enskildes integritet större vikt än andra enskildes (ekonomiska eller personliga) intressen skulle kunna äventyra ”principerna för statskicket”. Det framstår dock som positivt, inte minst mot bakgrund av den oro som de enskilda uttrycker i sina klagomål till IMY, att utredningar pågår i syfte att stärka skyddet för den enskildes integritet i svensk rätt.

*Gäille Bjurström är advokat hos Advokatfirman Delphi. Hon har ett särskilt intresse för gränssnittet mellan privaträtt och offentlig rätt och hjälper såväl privata företag som offentliga aktörer i frågor såsom dataskydd, offentlighet och sekretess, offentlig upphandling, kommersiella avtal och klimatanpassning.*

# Pasientens rett til informasjon ved bruk og utvikling av kunstig intelligens i helsehjelp

Av Julia D. Fuglestad Brodshaug og Simen Hafstad-Moi

## Implementering av kunstig intelligens i helsevesenet

Kunstig intelligens («KI») er allerede i bruk ved flere norske sykehus<sup>1</sup>. Fra slutten av 2023 tok imidlertid Bærum sykehus teknologien ett steg videre ved å implementere den i røntgenbildeanalyse<sup>2</sup>. Teknologien har gjort det mulig å analysere store mengder bilder svært hurtig og effektivt. Pasienter som før måtte vente potensielt flere timer på svar på røntgenbilder, kan nå på få minutter få beskjed om hvorvidt de kan dra hjem eller ikke. Eksempelet illustrerer litt av potensialet til KI i helsehjelp.

Grunnlaget for bruken av KI, og andre digitale hjelpemidler innen helsesektoren, er digitaliseringen av samfunnet<sup>3</sup>. Digitaliseringen har endret måten helsevesenet arbeider på, og har gjort en ny form for effektivitet tilgjengelig. Et viktig utviklingstrekk innen medisinsk behandling er mulig-



Julia D. Fuglestad Brodshaug



Simen Hafstad-Moi

heten til å bruke store mengder data og digitale hjelpemidler for å utvikle nye og bedre behandlingsmetoder som kan redde liv<sup>4</sup>.

Tekniske systemer blir en stadig vanligere og viktigere forutsetning for helsetjenestens evne til å gi effektiv og forsvarlig helsehjelp<sup>5</sup>. Ett av forsvarlighetskravets mange sider, er at det stilles krav til forsvarlig behandlingsform<sup>6</sup>. I denne sam-

menhengen er pasientens rett til informasjon, jf. pasient- og brukerrettighetsloven («pbrl») § 3-2, et viktig aspekt.

Ved økt implementering av KI i helsevesenet vil en viktig problemstilling være hvorvidt utviklingen og bruken av KI-systemer innen helse kan komme i strid med pasientens rett til informasjon etter pbrl. § 3-2.

## Pasientens rett til informasjon

Det følger av pbrl. § 3-2 første ledd at pasienten skal ha den informasjonen som er «nødvendig» for å kunne forstå sin helsetilstand og hva helsehjelpen innebærer. Det skal også informeres om mulige risikoer og bivirkninger, jf. bestemmelsens første ledd andre punktum. En tilsvarende plikt for helsepersonell til å yte en slik informasjon er hjemlet i helsepersonelloven («hpl») § 10.

Høyesterett har kommet med flere uttalelser om hva informasjonsplikten innebærer på et generelt grunnlag. I HR-2020-1332-A

- 1 Helsedirektoratet «Tilrettelegging for bruk av kunstig intelligens i helsesektoren med utgangspunkt i det radiologiske fagområdet», hjemmeside, 1. oktober 2021, s. 6 punkt 1, *Tilrettelegging for bruk av kunstig intelligens i helsesektoren.pdf* (helsedirektoratet.no) (lest september 2023).
- 2 Rolv Christian Topdahl, Magnus Ekeli Mullis, Anders Nøking, «Er vi forberedt på å la maskinene behandle oss?», nettavis, 25. september 2023, [https://www.nrk.no/rogaland/xl/snart-vil-kunstig-intelligens-analysere-kroppen-din\\_-vi-er-for-darlig-forberedt-1.16553955](https://www.nrk.no/rogaland/xl/snart-vil-kunstig-intelligens-analysere-kroppen-din_-vi-er-for-darlig-forberedt-1.16553955) (lest 17. oktober 2023).
- 3 Anne Kjersti Befring mfl., *Kunstig intelligens og big data i helsesektoren – rettslige perspektiver*, 1. utgave, Gyldendal 2020, s. 27.

- 4 Anne Kjersti Befring mfl., *Kunstig intelligens og big data i helsesektoren – rettslige perspektiver*, 1. utgave, Gyldendal 2020, s. 30.
- 5 Helsetilsynet, «Forsvarlig pasientbehandling uten IKT?», hjemmeside, 2021, s. 10, *Forsvarlig pasientbehandling uten IKT? Risikovurderinger, nødrutiner og forbedringsarbeid ved 17 sykehus. Rapport fra helsetilsynet 2/2021* (lest 14.05.2024).
- 6 Bakken, Oda. «Forsvarlighetsplikten ved bruk av kunstig intelligens i helsetjenesten». I *Kunstig intelligens og big data i helsesektoren – rettslige perspektiver*. Inger-Johanne Sand og Anne Kjersti Befring red., 1. utg, Oslo: Gyldendal, 2020, s. 400-435. s. 405.

fremhevet Høyesterett at terskelen for hva som er nødvendig informasjon vil måtte bero på «helsepersonellens skjønn innenfor det som er forsvarlig og nødvendig». Saken gjaldt spørsmål om erstatning grunnet manglende informasjon om behandling i forbindelse med hjerteflimmer. Dommen viser til følgende uttalelse fra HR-2017-687-A, om at det:

*«(...) i utgangspunktet vil være opp til legens skjønn å vurdere hvilke opplysninger som det er nødvendig å gi pasienten, og at opplysningene må tilpasses pasientens tilstand og sykdom, vedkommendes kunnskaper og muligheter til å ta til seg og oppfatte informasjonen, samt pasientens livssituasjon.<sup>7</sup>».*

Som det fremgår av uttalelsen fra dommen, beror det på en konkret vurdering av det enkelte tilfellet hva som anses som nødvendig informasjon. Dette vil naturligvis også gjelde ved bruk av KI-systemer innen helse. Behovet for informasjon vil for eksempel avhenge av hva slags form for KI-system man benytter, hvor stor rolle KI-systemet har i det aktuelle utrednings- og behandlingsløpet til den konkrete pasienten, og risikofaktorene ved bruk av KI-systemet for den aktuelle pasienten sin situasjon. Ved bruk av KI-systemer for å analysere røntgenbilder, slik som i eksempelet fra Bærum sykehus, vil det for eksempel kunne være nødvendig for pasientene å få informasjon om hvorvidt systemet fungerer like bra på alle. Er det for eksempel forskjeller i ytelse basert på kjønn, alder eller hvor personen kommer fra? Hvis dette er tilfellet, vil det være avgjørende for å ivareta hensynet til forsvarlighet og nødvendig informasjon at pasientene blir gjort oppmerksom på dette.

### Pasientens rett til medvirkning

Pasientens rett til informasjon henger tett sammen med pasientens

medvirkningsrett. Det følger av pbrl. § 3-1 første ledd andre punktum at pasienten blant annet har «rett til å medvirke ved valg mellom tilgjengelige og forsvarlige tjenesteformer og undersøkelses- og behandlingsmetoder». Etter sin ordlyd viser dette at pasienten skal ha stor innflytelse i behandlingsprosessen, særlig der det foreligger flere alternative og forsvarlige behandlingsmetoder. Bestemmelsen bygger på retten til samtykke, og forutsetter at det skal være et samarbeid mellom pasient og helsepersonell<sup>8</sup>. Pasientens ønsker skal derfor vurderes og vektlegges sterkt i vurderingen av de ulike valgene som skal gjøres i forbindelse med et behandlingsforløp.

” Er det for eksempel forskjeller i ytelse basert på kjønn, alder eller hvor personen kommer fra?

Retten til medvirkning har de siste årene fått økt relevans, ettersom den digitale utviklingen i samfunnet legger til rette for flere behandlingsmuligheter<sup>9</sup>. Samtidig har dette gjort at problemstillinger knyttet til implementeringen av KI-systemer har fått økt aktualitet. utfordringer i denne sammenheng knytter seg til hvordan medvirkningsretten, og i forlengelsen av denne retten til informasjon, ivaretas på bakgrunn av det såkalte «svart boks»-problemet<sup>10</sup>.

8 Duvaland, Lars, «Karnov lovkommentar: Pasient- og brukerrettighetsloven.», Lovdata Pro, 2021, § 3-1 note 1 (lest 25.09.2023).

9 Duvaland, Lars, «Karnov lovkommentar: Pasient- og brukerrettighetsloven.», Lovdata Pro, 2021, § 3-1 note 1 (lest 25.09.2023).

10 Lie, Thomas Endre. «Noen problemstillinger ved implementering av persontilpasset medisin.». I «Kunstig intelligens og big data i helsesektoren – rettslige perspektiver». Inger-Johanne Sand og Anne Kjersti Befring red., 1. utg, Oslo: Gyldendal, 2020, s. 442.

### «Svart boks»-problemet og pasientens rett til informasjon og medvirkning

I enkelte tilfeller blir KI-systemer så vanskelige å forstå, at det blir umulig for de ulike aktørene å skjønne hvordan den enkelte beslutningen har blitt tatt. Dette kalles gjerne for «svart boks»-problemet<sup>11</sup>.

” Ved bruk av kunstig intelligens i helsehjelp, kan det bli vanskelig for helsepersonell å få oversikt over store mengder analyserte data og hvordan beslutningene blir tatt, og følgelig hvilken risiko dette innebærer for pasienten.

For at helsepersonell skal kunne formidle kunnskap om ulike sykdomstilstander og gjøre pasienten oppmerksom på ulike former for helsehjelp, kreves det en viss innsikt og forståelse for beslutningsgrunnlaget<sup>12</sup>. Ved bruk av kunstig intelligens i helsehjelp, kan det bli vanskelig for helsepersonell å få oversikt over store mengder analyserte data og hvordan beslutningene blir tatt, og følgelig hvilken risiko dette innebærer for pasienten. For at helsepersonell skal kunne oppfylle sin informasjonsplikt, kan det argumenteres for at det kreves en god utveksling av informasjon mellom helsepersonell, virksomhet og de

11 Lie, Thomas Endre. «Noen problemstillinger ved implementering av persontilpasset medisin.». I «Kunstig intelligens og big data i helsesektoren – rettslige perspektiver». Inger-Johanne Sand og Anne Kjersti Befring red., 1. utg, Oslo: Gyldendal, 2020, s. 439.

12 Aarli, Ragna. «'Big data' og helsehjelpens nye aktorbilde.». I «Kunstig intelligens og big data i helsesektoren – rettslige perspektiver». Inger-Johanne Sand og Anne Kjersti Befring red., 1. utg, Oslo: Gyldendal, 2020, s. 245.

7 HR-2017-687-A premiss (43).

som har utviklet KI-systemet. Der-  
som dette ikke skjer, vil det ikke  
være noen som egentlig har full  
oversikt over beslutningene som  
blir tatt, og risikoen disse innebærer.  
På denne måten blir det svært viktig  
at de som har utviklet KI-verktøyet,  
og som forstår analysen, kan klar-  
legge automatiseringen som har  
skjedd, og hvilken risiko dette med-  
fører. Uten en slik informasjons-  
utveksling mellom de ulike aktørene  
vil det potensielt kunne bli få mulig-  
heter for pasienten til å få tilstrekke-  
lig informasjon, samt medvirke til  
sin behandlingsform.

Når dette er sagt, er det ikke  
nødvendigvis slik at helsepersonell  
trenger å forstå alle de tekniske spe-  
sifikasjonene ved et KI-system for  
å kunne oppfylle informasjonsplik-  
ten etter hpl. § 10. Videre stiller  
blant annet den nylig vedtatte AI  
Act opp en rekke bestemmelser  
som skal regulere utviklingen og  
bruken av kunstig intelligens, slik at  
problemer som det forannevnte  
ikke oppstår innen helse.

Digitale hjelpemidler har blitt  
brukt innen helse siden den digitale  
utviklingen skjøt fart mot slutten av  
1960-tallet<sup>13</sup>. Kunstig intelligens er  
i dag en del av denne utviklingen,  
og man ser at omfanget og tilgjeng-  
ligheten av en slik teknologi øker.  
Parallelt med denne utviklingen  
oppstår det et behov for effektiv  
rettslig regulering.

” Digitale hjelpemidler  
har blitt brukt innen  
helse siden den  
digitale utviklingen  
skjøt fart mot slutten  
av 1960-tallet

AI Act er det første juridiske  
rammeverket som tar sikte på  
å regulere kunstig intelligens. For-  
ordningen er bygget opp slik at den  
knytter flere krav og reguleringer til

13 NOU 2023: 4.

KI-systemer som innebærer høy  
risiko ved bruk, enn systemer med  
lav risiko. Kunstig intelligens innen  
helsesektoren faller inn under det  
som defineres som «høy risiko»<sup>14</sup>,  
ettersom det er snakk om systemer  
som fungerer innen kritisk infra-  
struktur og som potensielt kan  
påføre uopprettelig skade dersom  
de ikke er undergitt strenge krav.

” AI Act er det første  
juridiske rammeverket  
som tar sikte på  
å regulere kunstig  
intelligens.

AI Act artikkel 29 og 13 kan  
trekkes frem som eksempler på  
bestemmelser som kan bidra til  
å sikre at «svart-boks»-problematikk  
ikke oppstår innen helse. Først-  
nevnte bestemmelse, artikkel 29,  
fremhever flere forpliktelser ved  
bruk av AI-systemer med høy  
risiko. For det første stilles det krav  
om at systemene skal brukes på til-  
tenkt måte. Videre stilles det krav  
om at det skal skje en kontinuerlig  
overvåkning under bruken av syste-  
met, og en rapportering mellom  
ulike aktører om en mulig økning  
i risiko. Sistnevnte bestemmelse, AI  
Act artikkel 13, handler om retten  
til åpenhet. Bestemmelsen innebæ-  
rer at systemene skal være designet  
og utviklet på en slik måte at bru-  
ken er «sufficiently transparent to  
enable users to interpret the  
system's output» og «use it appro-  
priately». Dette kan gjøre bruken av  
KI i helsehjelp mer i tråd med for-  
svarlighetskravet, herunder kravet til  
medvirkning og informasjon jf. hpl.  
§ 4.

14 COM/2021/206 final, Proposal For  
A Regulation Of The European Par-  
liament And Of The Council Laying  
Down Harmonised Rules On Arti-  
ficial Intelligence (Artificial Intelli-  
gence Act) And Amending Certain  
Union Legislative Acts [AI Act]  
punkt 5.2.3.

Videre vil blant annet lov om  
medisinsk utstyr og EUs person-  
vernforordning kunne hindre at  
«svart boks»-problematikk oppstår  
innen helse. Lov om medisinsk  
utstyr stiller høye generelle krav til  
merking, overvåkning og dokumen-  
tasjon der KI-systemer regnes som  
medisinsk utstyr. GDPR stiller  
videre strenge krav til åpenhet og  
bruk av helseopplysninger.

Det kan på bakgrunn av dette  
argumenteres for at «svart boks»-  
problematikken ikke nødvendigvis  
vil være et praktisk problem i for-  
hold til pasientens rett til informa-  
sjon ved bruk av KI-systemer innen  
helse. Det er flere sentrale bestem-  
melser som sikrer at informasjonen  
rundt beslutningsgrunnlaget til et  
KI-system ikke går tapt, og en  
løpende kvalitetssikring vil kunne  
hindre uforutsette resultater.

På den andre siden kan det stilles  
spørsmålsteget ved hvor effektivt AI  
Act vil regulere kunstig intelligens  
i praksis etter implementering, og  
hvilken retning utviklingen av KI  
innen helse faktisk vil ta i fremtiden.

### Avsluttende bemerkninger

Med fremveksten av stadig mer  
komplekse digitale systemer og  
behandlingsmetoder vil pasientens  
behov for god informasjon stå sen-  
tralt. Denne artikkelen har blant  
annet sett på pasientens rett til  
informasjon opp mot «svart boks»-  
problematikk ved implementeringen  
av KI-systemer innen helse. Artikkelen  
er ment som et utgangspunkt  
for rettslig refleksjon rundt infor-  
masjonsplikten i tiden som kom-  
mer.

*Julia Desiré Fuglestad Brodshaug,  
jurist i Helfo.*

*Simen Hafstad-Moi, seniorrådgiver  
i Helfo.*



# Innsyn i klasselister er i strid med GDPR

Av Ida Thorsrud

I 2009 fastslo Justisdepartementet at klasselister er offentlige dokumenter, og at skoleeiere derfor må gi innsyn i dem etter offentleglova. I denne artikkelen argumenterer jeg for at den tolkningen er utdatert, at det å gi innsyn i klasselister ikke er nødvendig for å oppfylle formålene i offentleglova, og at dette dermed er et brudd på GDPR.

## Innledning

Spørsmålet om offentleglova (2006) gir rett til innsyn i klasselister ble opprinnelig klargjort av Justisdepartementet i en tolkningsuttalelse fra 2009.<sup>1</sup> Lovavdelingens uttalelse var basert på en tidligere tolkningsuttalelse fra 2004 som avklarte forholdet mellom personopplysningsloven (2000) og offentlighetsloven (1970).<sup>2</sup>

Dette spørsmålet er for alle praktiske formål avklart. Alle skoleeiere som søker informasjon om dette, vil finne veiledningen til Datatilsynet



Ida Thorsrud

net som forklarer at klasselister er offentlige dokumenter,<sup>3</sup> og at man dermed plikter å gi innsyn i dem.

Problemstillingen kommer imidlertid fortsatt opp ved ujevne mellomrom. For eksempel søkte Stavanger arbeiderparti i 2023 innsyn i klasselister for barn i 1. og 2. klasse og brukte e-postadressene til foresatte for å sende dem politisk reklame.

Både reaksjonene i etterkant av denne saken<sup>4</sup>, og ikke minst det at rettstilstanden har endret seg vesentlig siden Justisdepartementet vurderte spørsmålet i 2009, gjør det aktuelt å se på denne problemstillingen på nytt. I denne artikkelen skal jeg derfor redegjøre for hvordan GDPR, som trådte i kraft i 2018, endrer rettstilstanden og hvordan dommen C-439/19 «Penalty points» innebærer at innsyn

i klasselister nå er i strid med GDPR.

” I denne artikkelen skal jeg derfor redegjøre for hvordan GDPR, som trådte i kraft i 2018, endrer rettstilstanden og hvordan dommen C-439/19 «Penalty points» innebærer at innsyn i klasselister nå er i strid med GDPR.

## Personopplysningsloven (2000) § 6 og forholdet mellom offentlig innsyn og GDPR

Personopplysningsloven (2000) § 6 regulerte forholdet til offentlighetsloven (1970 og senere 2006). Bestemmelsen fastslo at «Loven her begrenser ikke innsynsrett etter offentlighetsloven (...)

Justisdepartementet skilte i tolkningsuttalelsen fra 2004 mellom innsynsrett og vurderinger om meroffentlighet etter offentlighetsloven (1970).<sup>5</sup> Innsynsretten betyr at innsyn *må* gis, mens meroffentlighet betyr at innsyn etter en konkret vurdering *kan* gis.)

Om innsynsretten uttalte departementet:

1 *Tolkningsuttalelse av 26.06.2009 fra lovavdelingen i Justisdepartementet (200703385 EO MHG)*

2 *Tolkningsuttalelse av 16.07.2004 fra lovavdelingen i Justisdepartementet (2004/04600 ES KES/MHG/GMA)*

3 *Artikkelen «Klasselister er offentlige dokumenter» opprinnelig publisert på datatilsynet.no den 21.06.2018*

4 *Artikkelen «Reagerer på Ap-stunt: Datatilsynet har mottatt flere klager» opprinnelig publisert på VG.no den 25.08.2023*

5 *Tolkningsuttalelse av 16.07.2004 fra lovavdelingen i Justisdepartementet (2004/04600 ES KES/MHG/GMA) Punkt 4.1*

«Når det foreligger innsynsrett etter offentlighetsloven, følger det av personopplysningsloven § 6 første ledd at det skal gis innsyn uten at det er nødvendig å vurdere om vilkårene for behandling av personopplysninger i personopplysningsloven og i personverndirektivet er oppfylt. I slike tilfeller skal det altså gis innsyn også om dette eventuelt vil være i strid med våre folkerettslige forpliktelser etter direktivet».

Departementet sa med andre ord at så lenge offentlighetsloven pålegger utlevering av personopplysninger (innsynsrett), gjaldt ikke personverndirektivet av 1995 eller personopplysningsloven av 2000. Dette er en konklusjon direkte med grunnlag i ordlyden i personopplysningsloven (2000) § 6(1) som dermed gjorde unntak fra personvernreglene.

Ifølge tolkningsuttalelsen fra 2009,<sup>6</sup> ville innsyn i klasselister falle inn under innsynsretten i offentleglova (2006). Dette betyr at personopplysningsloven av 2000 ikke gjaldt når det ble gitt innsyn i klasselister. Departementet sa følgende i tolkningsuttalelsen:

«I den utstrekning det foreligger en innsynsrett etter offentlighetsloven følger det av personopplysningsloven § 6 første ledd at personopplysningsloven ikke kommer til anvendelse.»

Personopplysningsloven av 2018 inneholder ikke en tilsvarende bestemmelse, men GDPR regulerer til en viss grad forholdet mellom offentlig innsyn og personvern i artikkel 86:

*«Personopplysninger i offentlige dokumenter (...), kan utleveres (...) i samsvar med unionsretten eller medlemsstatenes nasjonale rett (...) for å bringe allmennhetens rett til innsyn i offentlige dokumenter i samsvar med retten til vern av personopplysninger i henhold til denne forordning.»*

6 Tolkningsuttalelse av 26.06.2009 fra lovavdelingen i Justisdepartementet (200703385 EO MHG)

I forarbeidene<sup>7</sup> til personopplysningsloven som inkorporerer GDPR i norsk rett, mente Justisdepartementet at det ikke var nødvendig å videreføre personopplysningsloven (2000) § 6(1). Dette fordi GDPR artikkel 86 regulerer forholdet mellom personvern og innsyn etter nasjonale regler som offentleglova. Departementet uttalte i denne forbindelse:

«Ettersom artikkel 86 ikke stiller andre krav til utleveringen av personopplysningene enn at den er 'i samsvar med' reglene om allmennoffentlighet, går forordningen på dette punktet noe lenger i retning av offentlighet enn unntaksregelen i dagens lov. Mens unntaksregelen i personopplysningsloven § 6 første ledd kun gjelder ved innsynsrett etter offentleglova, omfatter unntaket i forordningen artikkel 86 også de tilfellene der offentleglova bare gir adgang, og ikke plikt, til å gi innsyn, jf. offentleglova § 11 om meroffentlighet.»

Justisdepartementet omtaler GDPR artikkel 86 som en unntaksregel som går lenger enn personopplysningsloven (2000) § 6(1). Det er denne unntaksbestemmelsen som er sentral i departementets tolkningsuttalelse fra 2004 om forholdet mellom personopplysningsloven og offentlighetsloven (1970). Det er derfor nødvendig å undersøke om GDPR artikkel 86 er en unntaksbestemmelse, og hvor langt unntaket i så fall strekker seg.

### GDPR artikkel 86 er ingen unntaksbestemmelse

Som det fremgår av GDPR artikkel 86 sin ordlyd, åpner bestemmelsen for at personopplysninger som fremgår av offisielle dokumenter kan deles i tråd med nasjonal lovgivning for å bringe offentlig innsyn i overensstemmelse med personvern-

7 Prop. 56 .S (2017-2018) punkt 15.2 side 105

rettighetene etter GDPR.<sup>8</sup> Bestemmelsen krever at hensynet til offentlig innsyn forenes med personvern når det gis innsyn i offentlige dokumenter som også inneholder personopplysninger.<sup>9</sup>

Det er med andre ord ikke slik at GDPR artikkel 86 kun stiller krav til at utleveringen av personopplysningene er «i samsvar med» reglene om allmennoffentlighet slik departementet gir uttrykk for i forarbeidene nevnt ovenfor. Hensynet til personvern skal også tas i betraktning. Dette understrekes også i fortalepunkt 154 hvor det står at nasjonale innsynsregler skal forenes med retten til personvern. Verken GDPR artikkel 86 eller fortalen gir ytterligere informasjon om hvordan hensynene skal balanseres.

Det er verdt å merke seg at ordlyden i GDPR artikkel 86 ikke uttrykkelig sier at dette er en unntaksbestemmelse. Hvis vi sammenligner artikkel 86 med artikkel 85 som gjelder forholdet mellom behandling av personopplysninger og ytrings- og informasjonsfrihet, ser vi en helt klar forskjell i utformingen av artiklene. GDPR artikkel 85(2) regulerer tydelig i hvilke tilfeller det enkelte landet kan gjøre unntak fra GDPR i nasjonal rett for å ivareta ytrings- og informasjonsfriheten. Vi finner ingen tilsvarende formulering i GDPR artikkel 86. Det tyder på at artikkel 86 ikke åpner for unntak fra GDPR.

Ifølge Oxfords lovkommentar til GDPR, har artikkel 86 en deklarerende, snarere enn normativ, natur. GDPR artikkel 86 bekrefter at

8 «Personal data in official documents (...) may be disclosed (...) in accordance with Union or Member State law (...) in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.»

9 Jf. GDPR artikkel 86 og ordlyden «in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation»

offentlig innsyn i forvaltningsdokumenter er et legitimt formål for å oppfylle en rettslig forpliktelse eller en oppgave i allmennhetens interesse. Ifølge lovkommentaren, støtter fortalepunkt 154 opp om denne tolkningen, idet det fremgår av dette fortalepunktet at «innsyn i offentlige dokumenter kan anses for å være i allmennhetens interesse».

GDPR artikkel 86 er med andre ord ikke en unntaksbestemmelse som lar offentliglova overstyre GDPR. Det er heller en bestemmelse som anerkjenner at medlemslandene kan lage nasjonale bestemmelser som regulerer innsyn. Det fremgår av GDPR artikkel 86 at slike innsynsregler må forene hensynet til offentlig innsyn med personvernrettighetene i GDPR. Det betyr at GDPR gjelder også ved offentlig innsyn så lenge det gis innsyn i personopplysninger.

GDPR gir ikke ytterligere veiledning om hvordan forene hensynet til offentlig innsyn med personvern-hensyn. Imidlertid gir C-439/19 «Penalty points» fra EU-domstolen oss et utgangspunkt for en slik vurdering.

### C-439/19 «Penalty points»

I C-439/19 «Penalty points», vurderte EU-domstolen om en lov i Latvia som hjemlet innsyn i personopplysninger om trafikkover-tredelser, var et brudd på GDPR. Loven gikk ut på at enhver som kjente til fødsels- og personnumme-ret til en person, kunne be om inn-syn i hvor mange trafikkover-tredelser vedkommende hadde i form av «penalty points».

Domstolen slo fast at all behandling av personopplysninger må være i tråd med GDPR, særlig prinsip-pene i GDPR artikkel 5 og krav til behandlingsgrunnlag i GDPR artikkel 6.<sup>10</sup> Spørsmålet i denne saken var om innsyn i personopplysninger om trafikkover-tredelser var i lovlig

etter GDPR, nærmere bestemt proporsjonalitetsprinsippet.<sup>11</sup>

Domstolen konstaterte at selv om GDPR ikke inneholder noe generelt forbud mot publisering,<sup>12</sup> må offentliggjøringen av personopplysninger likevel være «nødvendig», jf. artikkel 6(1).<sup>13</sup> Retten til personvern er ikke absolutt. Inngrep kan aksepteres hvis det er hjemlet i lov, respekterer grunnleggende rettigheter<sup>14</sup> og er proporsjonalt, jf. art 52(1) i EU-Charteret. Som en del av proporsjonalitetsvurderingen, uttalte domstolen at det må vurderes om inngrepet er nødvendig og om det «genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others». Videre må inngrepet være «strictly necessary» og reglene som hjemler inngrepet må sette klare og tydelige rammer for inngrepets omfang.<sup>15</sup>

Domstolen la vekt på følgende momenter i proporsjonalitetsvurderingen:

1. «the seriousness of the interference with the fundamental rights to respect for private life and protection of personal data caused by that disclosure» og
2. «the purpose of achieving the objectives pursued»<sup>16</sup>

Sagt på en annen måte var det relevant å legge vekt på hvor inngripende innsyn var for personvernet, og om innsyn oppfylte et legitimt formål.

11 C-439/19, avsnitt 97

12 C-439/19, avsnitt 103

13 I denne saken vurderte EU-domstolen nødvendighetskravet i GDPR artikkel 6(1)e) (utøvelse av offentlig myndighet eller oppgave i allmennhetens interesse), men nødvendighetsvurderingen vil være den samme etter GDPR artikkel 6(1)c), jf. ordlyden «behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige» (forfatters understreking).

14 «the essence of the fundamental rights»

15 C-439/19, avsnitt 105

16 C-439/19, avsnitt 106

Innsynet var hjemlet i latvisk lov, og EU-domstolen anerkjente trafikk-sikkerhet som et legitimt hensyn.<sup>17</sup> Innsyn måtte likevel ikke gå lenger enn det som var nødvendig for å oppfylle formålet med behandlingen av personopplysninger (her publisering for å ivareta trafikk-sikkerhet).<sup>18</sup> Hvis formålet kunne oppfylles på en mindre inngripende måte, var nødvendighetskravet ikke oppfylt.<sup>19</sup> Domstolen påpekte at alternative tiltak kunne ha oppfylt formålet uten at personopplysninger måtte bli utlevert, men alternativer til innsyn hadde ikke blitt vurdert.<sup>20</sup> Domstolen la også vekt på at det å gi innsyn i noens trafikkover-tredelser er relativt inngripende, og kom til nødvendighetskravet ikke var oppfylt.<sup>21</sup>

Domstolen konkluderte at dette måtte gjelde selv ved innsyn i et offisielt dokument som nevnt i GDPR artikkel 86.<sup>22</sup> Domstolen uttalte i denne forbindelse at selv om innsyn i offentlige dokumenter er et hensyn som kan begrunne ut-levering av personopplysninger,<sup>23</sup> må den typen innsyn likevel skje på en måte som ivaretar krav til personvern.

### Er innsyn i klasselister nødvendig for å oppfylle formålene i offentliglova?

Innsyn i klasselister innebærer deling av personopplysninger om barn og deres foresatte, noe som er et inngrep i personvernet. Spørsmålet er om dette inngrepet er lovlig. Svaret på det avhenger ifølge C-439/19 av:

1. Om inngrepet er hjemlet i lov,
2. Om inngrepet respekterer «the essence of fundamental rights», og
3. Om inngrepet er proporsjonalt.

17 C-439/19, avsnitt 108

18 C-439/19, avsnitt 109

19 C-439/19, avsnitt 110, jf. fortalepunkt 39

20 C-439/19, avsnitt 111

21 C-439/19, avsnitt 113

22 C-439/19, avsnitt 119

23 Jf. fortalepunkt 154

10 C-439/19, avsnitt 96

I vurderingen av hvorvidt inngrepet er proporsjonalt, la EU-domstolen i C-439/19 vekt på:

- a. Om inngrepet søker å oppnå en legitim interesse, og
- b. Om inngrepet er nødvendig for å oppfylle det hensynet. Hvis hensynet kunnet kunne oppfylles på en mindre personverninngrående måte, var ikke inngrepet proporsjonalt.

Innsyn i klasselister er hjemlet i lov, og kan sies å respektere «the essence of fundamental rights». Spørsmålet er om innsynet – eller utlevering av personopplysninger – er proporsjonalt.

I vurderingen av om inngrepet er proporsjonalt, er det på det rene at innsyn i klasselister søker å oppnå en legitim interesse eller et legitimt hensyn. Det fremgår tydelig av GDPR fortalepunkt 154 at «innsyn i offentlige dokumenter kan anses for å være i allmennhetens interesse». Spørsmålet er imidlertid om det er nødvendig å gi innsyn i klasselister for å oppnå formålet med offentleglova.

Formålet i offentleglova fremgår av § 1 som blant annet sier at «Formålet med lova er å leggje til rette for at offentlig verksemd er open og gjennomiktig, for slik å styrkje informasjons- og yringsfridommen, den demokratiske deltakinga, rettstryggleiken for den enkelte, tilliten til det offentlege og kontrollen frå

” Innsyn i klasselister er hjemlet i lov, og kan sies å respektere «the essence of fundamental rights».

ålmenta. (...)»

I veiledningen til offentleglova oppsummeres formålene i loven som demokratihensynet, kontrollhensynet og rettsikkerhetshensynet.<sup>24</sup>

Demokratihensynet lar borgere få innsikt i forvaltningen for å delta i demokratiet. Kontrollhensynet muliggjør tilsyn med forvaltningen f.eks. for å sikre forsvarlig bruk av offentlige midler. Rettsikkerhetshensynet sikrer en forvaltning som reduserer risiko for usaklig forskjellsbehandling og maktmisbruk. Dette er alle hensyn som er anerkjent som legitime formål, jf. GDPR artikkel 86 og fortalepunkt 154. Spørsmålet etter C-439/19 blir om det å gi innsyn i klasselister er nødvendig for å oppfylle disse formålene.

Det å gi innsyn i klasselister, er først og fremst å gi innsyn i personopplysninger til barn i skolen og deres foresatte. Selv om klasselister etter Justisdepartementets vurdering er et saksdokument, er det først og fremst en liste over personopplysningene til privatpersoner. Dette er privatpersoner som i utgangspunktet ikke har annen tilknytning til det offentlige enn at de er barn som går på offentlig skole eller er foresatte til slike barn.

Når vi vurderer hensynene i offentleglova,<sup>25</sup> er det klart at innsyn i klasselister verken vil fremme samfunnsdebatten eller bidra til en åpen forvaltning. Det å få innsyn i klasselister vil heller ikke bidra til en åpen og gjennomiktig forvaltning. Klasselister inneholder primært personopplysninger og gir ikke innsikt i forvaltningens praksis eller beslutningsgrunnlag. Derfor oppfylles verken demokratihensynet, kontrollhensynet eller rettsikkerhetshensynet ved at det gis innsyn i klasselister. Dette betyr at det å gi innsyn i klasselister ikke er nødvendig for å oppfylle formålene i offentleglova, noe som taler for at proporsjonalitetsprinsippet ikke er oppfylt.

24 *Rettleiar til offentleglova, Justisdepartementet, 2009 s. 11*

25 *Rettleiar til offentleglova, Justisdepartementet, 2009, s. 11*

Innsynsbestemmelsene i offentleglova har som formål å styrke tilliten til offentlig forvaltning. En bør derfor stille seg spørsmålet om det å gi innsyn i klasselister faktisk styrker denne tilliten. Reaksjonene etter saken med Stavanger arbeiderparti tyder på at slikt innsyn tvert imot kan svekke tilliten til offentlig forvaltning. Som borger i Norge og bruker av offentlige tjenester (for eksempel offentlig skole), må den enkelte kunne ha tillit til at personopplysningene deres ikke deles med andre som så bruker dem til formål som ikke er forenelige med det opprinnelige formålet de ble samlet inn til. Dette er et forbud mot formålsutglidning, og det er dette personvernprinsippet som blir utfordret når Justisdepartementet mener at offentleglova hjemler innsyn i klasselister. Det er nemlig nærliggende at innsyn i klasselister søkes for å få utlevert kontaktinformasjon til foresatte, slik som vi så i saken om Stavanger arbeiderparti. Denne typen viderebehandling svekker tilliten til offentlig forvaltning heller enn å styrke den, noe som er i strid med formålet i offentleglova. Dette taler også for at proporsjonalitetsprinsippet ikke er oppfylt.

Når det gis innsyn i klasselister, åpnes det for at personopplysninger om barn og foresatte blir delt med hvem som helst. Det er ikke noe krav til at den som søker innsyn etter offentleglova oppgir formålet med innsynsforespørselen. Skoleeier har heller ikke hjemmel til å kontrollere at den som har fått innsyn ikke viderebehandler personopplysningene til nye og uforenelige formål. Innsyn i klasselister er ikke innsyn i personopplysninger om straffbare forhold i form av trafikkovertrедelser som i C-439/19. Det er som regel snakk om kontaktinformasjon, det vi si personopplysninger som ofte er mer offentlig tilgjengelige. Dette kan tilsi at denne typen innsyn er et mindre inngripende inngrep i den enkeltes personvern. Imidlertid er det nærlig-

gende å anta at hovedpoenget med å søke innsyn i klasselister nettopp er å få tilgang til kontaktinformasjon som så brukes til å ta kontakt med foresatte på en måte de ikke har samtykket til. Reaksjonene på Stavanger arbeiderpartis bruk av klasselister for å sende politisk reklame viser at dette oppleves som inngripende. Denne forståelsen understøttes av Datatilsynets varsel om vedtak i saken:<sup>26</sup>

*«Det fremstår som åpenbart for Datatilsynet at behandlingen har hatt faktisk negativ innvirkning på de registrerte. Vi legger til grunn at denne behandlingen har fått reaksjoner blant annet fordi den ikke var påregnelig for de den gjelder.»*

26 23/03206-15

Det å gi innsyn i klasselister er med andre ord en inngripende behandling, og det taler også for at proporsjonalitetskravet ikke er oppfylt.

” Når det gis innsyn i klasselister, åpnes det for at personopplysninger om barn og foresatte blir delt med hvem som helst.

### Konklusjon

Redegjørelsen ovenfor har vist at det å gi innsyn i klasselister ikke er nødvendig for å oppfylle formålene i offentleglova. Proporsjonalitets-

prinsippet er ikke oppfylt, noe som betyr at det å gi innsyn i klasselister er et inngrep som er i strid med GDPR.

I vurderingen er det særlig vekt på at innsyn i klasselister innebærer at det utleveres personopplysninger om brukere av offentlige tjenester, noe som ikke er nødvendig for å oppfylle formålene i offentleglova. Det er også lagt vekt på at innsyn i klasselister kan svekke tilliten til offentlig forvaltning på grunn av risikoen for formålsutglidning. Til slutt er det lagt vekt på at denne typen deling kan ha negative konsekvenser for den enkelte og oppfattes som inngripende.

*Ida Thorsrud, jurist og prosjektleder for den nasjonale Google-DPLAen (KS).*



Illustrasjon: Colourbox.com

# FN-konvensjon om cyberkriminalitet

Av Stein Schjøllberg

## 1. Innledning

Etter mer enn 2 ½ år og syv møter i komiteen har vi nå fått et forslag om en FN-konvensjon om cyberkriminalitet. Hva betyr dette for verdenssamfunnet og kampen mot cyberkriminalitet?

Helt siden kravet om en FN-konvensjon ble fremmet av Russland i 2018 har det vært en klar polarisert uenighet blant medlemslandene om behovet for en konvensjon. Ad-hoc-komiteen hadde vært uenig om kravet helt siden drøftelsene i komiteen begynte i januar 2022. Det var heller ikke mulig å oppnå enighet under *Concluding Session* i februar 2024.

Det ble derfor besluttet å arrangere en *Reconvened concluding session*<sup>1</sup>

” Etter mer enn 2 ½ år og syv møter i komiteen har vi nå fått et forslag om en FN-konvensjon om cyberkriminalitet. Hva betyr dette for verdenssamfunnet og kampen mot cyberkriminalitet?

som ble berammet til 29. juli-9. august 2024. Under forhandlingene ble det utarbeidet et nytt forslag av 7. august 2024 om en FN-konvensjon: *Draft United Nations convention against cybercrime*.<sup>2</sup>

1 Se [https://www.unodc.org/unodc/en/cybercrime/ad\\_hoc\\_committee/abc\\_reconvened\\_concluding\\_session/main](https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/abc_reconvened_concluding_session/main)

2 Se <https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf>



Stein Schjøllberg

Som følge av de mange tilfeller av uenighet var det stor overraskelse at forslaget ble vedtatt med akklamasjon torsdag 8. august 2024. Bare et land, Iran, fremmet forslag om votering av enkelte artikler. Ad Hoc komiteen har 9. august 2024 redegjort for utviklingen av diskusjonene.<sup>3</sup>

Den teknologiske utvikling i cyberspace har vært så hurtig og overveldende at samfunnet har problemer med å tilpasse lovgivning, kontroll- og sikkerhetstiltak. Nye former for internasjonale lovtiltak med sikte på å forebygge og bekjempe cyberkriminalitet er nødvendig og må føre til tiltak på FN-nivå.

En FN-konvensjon om cyberkriminalitet er nødvendig for å oppnå globale standarder for sikkerhet, fred og rettsikkerhet i cyberspace. Det er nødvendig at FN etablerer globale rammeverk og retningslinjer for cyberspace og styrker cybersikkerheten, rettsikkerheten og samarbeidet mellom alle nasjoner.

Utviklingen av globale IT-selskaper slik som Google, Facebook,

3 Se <https://documents.un.org/doc/undoc/ltl/v24/055/00/pdf/v2405500.pdf>

Apple, Amazon og Microsoft har vært så altomfattende at disse private globale selskapene nå styrer utviklingen av cyberspace uten nasjonale eller globale reguleringer og retningslinjer. Det kan anføres at disse globale selskapene er blitt ledende organisasjoner for styringen av *Internet Governance* i stedet for FN-institusjonene. *Puss futen på dem*, skrev Aftenposten allerede 6. februar 2018 og viste til at Google, Facebook, Apple og Amazon tappet Norge for enorme verdier. Et alternativ til FN finnes ikke!

Jeg ble 20. januar 2022 oppnevnt av FN som en *Civil society delegate in the United Nations Ad Hoc Committee*, som den eneste *Civil Society* representant fra de nordiske land. Jeg skrev flere innspill, *contributions for sessions*. Det femte innspill ble sendt til *Concluding Session* den 11. desember 2023.<sup>4</sup>

## 2. Draft United Nations convention against cybercrime

Forslaget fra Ad-hoc-komiteen som skal behandles i FN's hovedforsamling i løpet av høsten 2024, inneholder 9 kapitler og 68 Artikler. I en pressemelding 9. august 2024 ble det uttalt blant annet:<sup>5</sup>

*After three years of work, the committee established by the UN General Assembly to negotiate a new convention on cybercrime agreed today on a draft convention text.*

*The draft convention is expected to be adopted by the General Assembly later this year, thus becoming the first global legally binding instrument on cybercrime.*

4 Se [https://www.unodc.org/unodc/en/cybercrime/ad\\_hoc\\_committee/abc\\_concluding\\_session/main](https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/abc_concluding_session/main)

5 <https://www.unodc.org/unodc/en/front-page/2024/August/united-nations-member-states-finalize-a-new-cybercrime-convention.html>

*This achievement represents the culmination of a five-year effort by UN Member States, with the input of civil society, academic institutions and the private sector. UNODC served as the substantive secretariat for the negotiations.*

Under forhandlingene var det særlig diskusjoner om personvern. Forslaget om personvern (Human Rights) i Article 6 er et viktig forslag i FN-konvensjon om cyberkriminalitet:

*Article 6. Respect for human rights*

1. States Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law.
2. Nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law.

### **De straffbare handlinger**

De straffbare handlinger er beskrevet i forslaget til FN-konvensjonen i kapittel 2. Forslaget bygger mye på de handlinger som er gjort straffbare i Budapest konvensjonen, som nå er ratifisert av 76 land, med 27 land utenfor Europa (august 2024).<sup>6</sup> Europarådet uttaler 8. august 2024 sin støtte til forslaget om en FN-konvensjon som er basert på prinsipper i Budapest konvensjonen:<sup>7</sup>

The Council of Europe – through its Cybercrime Programmes Office (C-PROC)– supported this treaty process from 2022 in order to ensure consistency with the Convention

on Cybercrime (Budapest Convention) and the inclusion of a minimum of necessary human rights and rule of law safeguards. Key provisions of the Budapest Convention have been reproduced in the draft treaty but concerns remain regarding safeguards given positions expressed by some States.

Følgende straffbare handlinger er nevnt i Budapest konvensjonen:

- Article 2 - Illegal access
- Article 3 – Illegal interception
- Article 4 – Data interference
- Article 5 – System interference
- Article 6 – Misuse of devices
- Article 7 – Computer-related forgery
- Article 8 – Computer-related fraud
- Article 9 – Offences related to child pornography

Følgende straffbare handlinger er nevnt i forslaget til en FN konvensjon:

- Article 7. Illegal access
- Article 8. Illegal interception
- Article 9. Interference with electronic data
- Article 10. Interference with an information and communications technology system
- Article 11. Misuse of devices
- Article 12. Information and communications technology system-related forgery
- Article 13. Information and communications technology system-related theft or fraud
- Article 14. Offences related to online child sexual abuse or child sexual exploitation material

I tillegg inneholder forslagene i kapittel 2 nye straffbare handlinger som er nødvendige i tilknytning til Article 14 om *online child sexual abuse*, og som er inntatt i Articles 15 og 16. En ny straffbar handling som er nødvendig som følge av utviklingen i kriminaliteten er inntatt i Article 17.

- Article 15. Solicitation or grooming for the purpose of committing a sexual offence against a child
- Article 16. Non-consensual dissemination of intimate images
- Article 17. Laundering of proceeds of crime

Forslagene i kapittel 2 inneholder som i Budapest konvensjonen også regler om:

- Article 18. Liability of legal persons,
- Article 19. Participation and attempt,
- Article 20. Statute of limitations,
- Article 21. Prosecution, adjudication and sanctions

### **De andre kapitler**

Bestemmelsene i de andre kapitler angår jurisdiksjon, saksbehandling, og samarbeid mellom medlemslandene, og bygger også mye på prinsippene i Budapest-wkonvensjonen. Kapitlene omfatter *Jurisdiction, Procedural measures and law enforcement, International cooperation, Preventive measures, Technical assistance and information exchange, Mechanism of implementation, Final provisions.*

Særlig skal nevnes Artikkelen 65 som bestemmer at konvensjonen skal tre i kraft 90 dager etter *the date of deposit of the fortieth instrument of ratification, acceptance, approval or accession.*

### **3. Erklæringer fra medlemsland og organisasjoner**

United Kingdom har blant annet uttalt:<sup>8</sup>

*In the spirit of compromise, the UK joined consensus on the basis of robust human rights safeguards that balance the Convention's broad scope of international cooperation and intrusive procedural powers.*

*Our negotiations over the past two and a half years have demonstrated that there*

<sup>6</sup> Se <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>

<sup>7</sup> Se <https://www.coe.int/en/web/cybercrime/-/united-nations-treaty-on-cybercrime-agreed-by-the-ad-hoc-committee>

<sup>8</sup> Se [https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened\\_concluding\\_session/Written\\_submissions/MEMBER\\_STATES/EOP\\_ltnes.pdf](https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/EOP_ltnes.pdf)

is no consensus on additional criminal offences.

*United States uttaler blant annet.<sup>9</sup>*

*Our committee has adopted a Convention against Cybercrime that reflects universal values and U.S. interests, including focused criminalization provisions, robust and flexible provisions on technical assistance, and strong provisions to safeguard human rights that are unprecedented in a UN criminal justice convention.*

*We welcome the Committee's adoption of the UN Convention Against Cybercrime as a rights-respecting criminal justice instrument for the 21<sup>st</sup> century and beyond.*

Det må antas at flere land syntes det nå var viktig å bli enige i FN-komiteen om et forslag. Det viste også den norske delegasjonen til i det siste møtet den 9. august 2024. Jeg slutter meg til denne begrunnelse.

Men mange globale organisasjoner er ikke tilfredse med innholdet i konvensjonen, og har kommentarer til forslaget om konvensjonen.

Det vises særlig til uttalelser fra Cisco:<sup>10</sup>

*While the recently adopted UN Convention against Cybercrime addresses important issues around the need for increased cyber capacity building, it raises concerns around the protection of shared rights and values, and requires more attention before ratification by member states.*

*Atlantic Council uttaler blant annet.<sup>11</sup>*

*However, this landmark achievement should not be celebrated, as it poses significant risks to human rights, cybersecurity, and national security.*

Privacy International uttaler:<sup>12</sup>

*Throughout these negotiations, Privacy International and other civil society organizations, UN human rights experts, academics, security researchers and the industry have consistently recommended that any UN cybercrime treaty is narrow in scope and contains robust safeguards to mitigate the risks of human rights abuses. It is regrettable that our recommendations have not been reflected in this final draft.*

*As Privacy International has consistently affirmed, if the draft treaty cannot be fixed, it should be rejected. There is no longer time for negotiations to significantly improve the text.*

*It is now time to reject this draft treaty.*

Several Civil Society and Industry Stakeholders har følgende konklusjon:<sup>13</sup>

*Unless substantial changes are included to the final draft Convention to address these broad-based and fundamental concerns, we urge governments not to adopt the treaty, and if it is adopted, not to ratify it.*

#### 4. Behandlingen i Hovedforsamlingen i FN

Behandlingen i Hovedforsamlingen i FN kan drøfte tilleggsforslag. Det bør under forhandlingene i Hovedforsamlingen i FN bli enighet om at konvensjonen skal inneholde en særskilt Artikkel om global myndighet for INTERPOL. En slik Artikkel bør omfatte koordinering og bistand til politiet i medlemslandene med etterforskning og forebyggelse av cyberkriminalitet. INTERPOL kan organisere og koordinere innholdet i de fleste Artikler i kapitlene V–IX.

INTERPOL er nevnt i *Article 37. Extradition, Article 40. General principles and procedures relating to mutual legal assistance, Article 41. 24/7 network, og Article 47. Law enforcement cooperation.*

” Det bør under forhandlingene i Hovedforsamlingen i FN bli enighet om at konvensjonen skal inneholde en særskilt Artikkel om global myndighet for INTERPOL.

INTERPOL har siden 1980-årene vært den ledende internasjonale politiorganisasjonen for å utvikle samarbeid under etterforskningen av cyberkriminalitet, kompetanse og trening i etterforskning av cyberkriminalitet, og forebyggelse av cyberkriminalitet.<sup>14</sup> INTERPOL har etablert et globalt 24/7-nettverk, hvor organisasjonen samler, lagrer, deler og analyserer informasjon om cyberkriminalitet med alle sine 196 medlemsland. INTERPOL gir også medlemslandene støtte i teknikk, analyser, trening, og nettverk i etterforskningen av cyberkriminalitet, og i tillegg forskning på utviklingen av den globale cyberkriminalitet.

*Stein Schjølberg, pensjonert sorenskriver. Oppnevnt av FN som en Civil society delegate i Ad Hoc komiteen.*

9 Se [https://www.unodc.org/unodc/en/cybercrime/ad\\_hoc\\_committee/abc\\_reconvened\\_concluding\\_session/main](https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/abc_reconvened_concluding_session/main)

10 Se <https://blogs.cisco.com/gov/un-convention-against-cybercrime-2024>

11 Se <https://www.atlanticcouncil.org/blogs/new-atlanticist/the-un-finally-adopts-a-convention-on-cybercrime-and-no-one-is-happy/>

12 Se [https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened\\_concluding\\_session/Written\\_submissions/OP8/PI\\_written\\_statement\\_on\\_UN\\_cybertreaty\\_7August2024.pdf](https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP8/PI_written_statement_on_UN_cybertreaty_7August2024.pdf)

13 Se [https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened\\_concluding\\_session/Written\\_submissions/OP9/Final\\_Draft\\_Cybercrime\\_Convention\\_-\\_Multistakeholder\\_Statement.pdf](https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Final_Draft_Cybercrime_Convention_-_Multistakeholder_Statement.pdf)

14 Se <https://www.interpol.int/Crimes/Cybercrime>





## Endelig dom i skattestriden mellom Apple og EU

De siste ti-årene har det vokst frem en rekke multinasjonale virksomheter som leverer digitale tjenester på tvers av landegrensener, verdensdeler og kontinenter. Her er det bare å vise til aktører som Google, Apple, Facebook, Amazon og en rekke andre digitale tjenestetilbydere. Typisk for disse er at de tilbyr tjenester som leveres fra sentraliserte distribusjonsnettverk som dekker over større geografiske områder. Etablering av en base for denne typen distribusjon vil kunne gi store ringvirkninger både lokalt og nasjonalt, og vil være på ønskelisten til flere potensielle vertsnaasjoner.

I Europa har Irland fremstått som et vertsland med spesielt gunstige betingelser for virksomhetsbeskatning for utenlandske selskaper. Dette har vært en suksess, i den forstand at flere store utenlandske aktører faktisk har etablerte sine europeiske distribusjonssystemer nettopp her. For Irland betyr ikke dette bare økte skatteinntekter, men også en langsiktig utvikling av teknologisk kompetanse og infrastruktur, arbeidsplasser, sterkere tilbud innen IT-utdanning og andre tilhørende fordeler som setter seg over tid.

En utvikling der enkelte land søker å fremstå som spesielt gunstig når det gjelder skattebetingelser vil raskt kunne ende i et kappløp mot

et bunnivå som hverken er optimalt eller rettferdig sett i et større, og i dette tilfellet, europeisk perspektiv. Sett med skattebrillene på, vil det være mer fornuftig om land innenfor de aktuelle geografiske og økonomiske områdene samordner sine skatteregler og -betingelser. Skatetrykket bør ideelt sett ikke være et så fremtredende moment når virksomhetene skal velge tilholdssted.

I en tidligere artikkel i Lov & Data (L&D nr. 143 s. 10 flg.) diskuterte jeg en sak der EU-Kommisjonen hadde fattet interesse for et skattevedtak overfor Apple i nettopp Irland helt tilbake til 1991. EU-Kommisjonen var av den oppfatning at dette vedtaket og et senere vedtak fra 2007 i realiteten innebar at Irland hadde fraveket prinsippet om armlengdes avstand, og at Apples skattevilkår ikke var i tråd med alminnelige markedsbetingelser. Med armlengdes avstand siktes det her til forholdet mellom Apples selskap som mottok inntekten i USA og virksomheten i Irland. Kravet til armlengdes avstand innebærer litt forenklet at det stilles krav til at de to partene opptrer som separate og uavhengige av hverandre, og at det fattes rasjonelle forretningsmessige beslutninger med dette som utgangspunkt.

Videre mente Kommisjonen at Apple gjennom skattevedtakene ble

gitt en urimelig fordel i form av statsstøtte fra Irland. Bakgrunnen for dette var at Apple i praksis var blitt innvilget en spesielt gunstig skatteordning. Dette skjedde i praksis først og fremst ved at inntekter under lisensavtaler i konsernet ble allokert til USA i stedet for den lokale virksomheten i Irland, hvor den reelle aktiviteten var utøvd. Kommisjonen avsa i 2016 sitt vedtak som innebar at Apple måtte overføre 13 milliarder Euro til Irland.

Apple klaget Kommisjonens vedtak inn for EUs General Court (her omtaler jeg Retten som General Court og Domstolen som EU-domstolen). Avgjørelsen fra General Court syvende kammer falt 15. juli 2021, og Apple og Irland fikk medhold i klagen.. Denne avgjørelsen er altså drøftet i artikkelen i Lov & Data som det er vist til ovenfor. General Court la særlig vekt på at Kommisjonen ikke hadde påvist at skattevedtakene fra Irland utgjorde ulovlig statsstøtte. I denne forbindelse ble det pekt på at det ikke var gitt at de underliggende inntektsstrømmene skulle allokere til Irland i stedet for kontoret i USA slik Kommisjonen hadde anført. General Court fant heller ikke tilstrekkelig grunnlag for å legge til grunn at en utilstrekkelig inntektsandel var blitt henført som beskatningsgrunnlag for Apples virksomhet i Irland. Videre fremsto

ikke avgjørelsene knyttet til skattevedtakene etter rettens oppfatning som skjønnsmessige.

Avgjørelsen fra General Court kan langt på vei leses slik at retten ikke er enig i Kommisjonens metodiske utgangspunkt og de konklusjoner som ble ledet ut fra dette. Retten mente eksempelvis at Kommisjonen hadde lagt til grunn en presumsjon om at Apples avdeling i USA ikke hadde noen reell aktivitet rettet mot Irland, slik at inntektene i stedet skulle ha blitt allokert til den lokale avdelingen i Irland. På samme måte ble det lagt til grunn en presumsjon om at de irske skattereglene åpnet for en skjønnsutøvelse som ville innebære en ulovlig skattefordel. Retten synes med dette å stille sterkere krav til analysen av faktiske årsakssammenhenger mellom skattevedtakene og den påståtte ulovlige statsstøtten, og at Kommisjonen her ikke hadde gjort en god nok jobb.

Kommisjonen anket avgjørelsen fra General Court videre til EU-domstolen 25. september 2020.

Utfallet i ankensaken fremstår som overraskende, all den tid underinstansen var såpass klar på at det ikke var grunnlag for å snu de underliggende vedtakene fra Irland. EU-domstolen i storkammer har nå fattet endelig avgjørelse i denne saken, som altså har pågått siden Kommisjonen rettet den første henvendelsen til Irland i 2013. Avgjørelsen snur resultatet fra EU-General Court, og skattevedtakene ble funnet å utgjøre ulovlig statsstøtte fra Irland til Apple. Apple må som følge av dette betale over 13 milliarder Euro tilbake til Irland.

EU-domstolen la til grunn at Kommisjonen hadde tilstrekkelig dekning for å konkludere med at det forelå ulovlig statsstøtte og at det forelå vilkårlig forskjellsbehandling. Det ble videre lagt til grunn at skattevedtakene fra Irland åpnet for at Apple kunne allokere inntekter fra lisensavtaler for immaterielle ret-



Illustrasjon: Habior Manshaus / Midjourney.

tigheter til USA, uten at det var faktisk grunnlag for dette.

I avsnitt 125 i avgjørelsen gjør EU-domstolen rede for hvordan prinsippet om armlengdes avstand skal anvendes i denne typen saker. Det vises her til vurderingen under de irske skattereglene, men prinsippet gjelder generelt i skattesaker:

*“...[t]he profits to be allocated to the branch of a non-resident company pursuant to that section are ‘the profits that that branch would have earned at arm’s length, in particular in its dealings with the other parts of the company, if it were a separate and independent enterprise engaged in the same or similar activities under the same or similar conditions, taking into account the assets used, the functions performed and the risks assumed by the company through its branch and through the other parts of the company...’”*

Deretter går retten fra det generelle til det konkrete, og påpeker at de irske skattemyndighetene skulle ha gjort en vurdering av kravet til armlengde vurdert opp mot Apples disposisjoner knyttet til lisensinntektene:

“In order to do so, they should have compared the functions performed, the assets used and the risks assumed by ASI and AOE through their head offices and their Irish branches...”

Med utgangspunktet på plass, og en gjennomgang av hva som skulle ha blitt vurdert, går EU-domstolen deretter i avsnitt 126 inn og vurderer Kommisjonens vedtak på dette punktet. Her gjengis Kommisjonens anvendelse av armlengde-prinsippet, som konkluderer med at de to virksomhetene i henholdsvis USA og Irland ikke ville ha blitt enige om en slik fordeling av inntekter:

*“In particular, it concluded that an allocation outside Ireland of profits generated by the IP licences held by ASI and AOE would not have been agreed to by the Irish branches of those companies if they had been separate and standalone companies acting under normal market conditions and, moreover, that, given the lack of functions performed by the head offices and/or given the activities carried out by those branches, those IP licences should have been allocated to the Irish branches for tax purposes (recital 305 of the decision at issue).”*

EU-domstolen går inn på flere forhold i Kommisjonens vedtak, og påpeker at presumsjoner knyttet til fysisk tilstedeværelse og ansatte ikke alene har vært avgjørende for spørsmålet om armlengde. I avsnitt 129 fremhever retten at Kommisjonen trakk sin konklusjon etter en bredere anlagt vurdering:

*“The Commission drew that conclusion after linking two separate findings, that is to say, first, the absence of active or critical functions performed and risks assumed by the head offices and, secondly, the multiplicity and centrality of the functions performed and risks assumed by those branches, applying the legal test set out in recital 272 of the decision at issue.”*

EU-domstolen stiller seg på dette grunnlag kritisk til avgjørelsen fra General Court, som hadde trukket frem selve metoden og oppstilte presumsjoner i vedtaket fra Kommisjonen som kritikkkverdige. EU-domstolen mener å kunne vise at

Kommisjonen både ved spørsmålet om aktivitet i det utenlandske selskapet og andre spørsmål i saken ikke bare har gjort en vurdering bundet opp mot en presumsjon, eller en «exclusion approach», men hadde gått dypere inn i faktum og selve analysen. Vedtaket ble altså opprettholdt, i en avgjørelse som lander på diametralt motsatt resultat av underinstansen.

Irland er nå pålagt å kreve inn de utestående skattekravene fra Apple. Det er verdt å merke seg at det omstridte kravet ble deponert på en egen konto etter vedtaket fra Kommisjonen i 2016, slik at det nå er snakk om å overføre disse midlene fra Apple til Irland. Overføringen av disse midlene i tråd med deponeringsordningen er i seg selv en komplisert affære som forventes å ta flere måneder å gjennomføre.

Beslutningen fra EU-domstolen er endelig og kan ikke ankes videre. Den irske finansministeren Jack Chambers uttalte følgende om denne store pengeoverføringen til Irland:

*“The government will need to carefully consider what is the best course of action to take with this revenue, and I will be engaging with the party leaders over the coming weeks on the matter.”<sup>1</sup>*

Det skal påpekes at Irland sto fast ved Apples side gjennom saken, både ved at Irland inngikk i sakskomplekset gjennom en egen sak

1 <https://www.gov.ie/en/speech/361b9-statement-by-minister-chambers-on-judgement-by-the-court-of-justice-of-the-european-union-in-the-apple-state-aid-case/#:~:text=Both%20Ireland%20and%20Apple%20rejected,put%20forward%20by%20the%20Commission.>

forent til felles behandling med Apple-saken og ved at partene begge argumenterte for at skattevedtakene fra 1991 og 2007 var riktige.

For aktører som skal orientere seg etter denne siste avgjørelsen, er det viktig å fremheve betydningen av å ha notoritet og dokumentasjon knyttet til beslutningsprosesser, organisering, risikofordeling og tilsvarende mellom de ulike filialene. Roller og oppgaver som fordeles til ulike ledd og deler av organisasjonen må etterleves og kunne dokumenteres. For ledere og ansatte er det også et poeng å klargjøre hvor i systemet og innenfor hvilken virksomhetsdel disse er ansatt og hvor de utøver sin funksjon. Dette bør både dokumenteres og følges opp i den daglige driften.

Da jeg skrev om avgjørelsen fra General Court, avsluttet jeg med å vise til at veien mot en effektiv og samordnet beskatningsordning på tvers av landegrensene fortsatt hadde et stykke igjen. Selv om resultatet nå ble snudd, viser tidslinjen i denne saken utfordringen med å følge opp denne typen saker. Saken strekker seg tilbake til det første skattevedtaket fra Irland i 1991, og endelig avgjørelse falt nå altså først i september 2024. Kommisjonen innledet sin sak ved de første henvendelsene til Irland i 2013, mens selve vedtaket fra Kommisjonen kom i 2016. Irland ved finansministerens uttalelse opplyser selv at landet for lengst har endret sine skatteregler slik at saken kun har «historical relevance». Dette viser at selv om slike rettssaker kan ha betydning og kan være verdt å forfølge, så ligger de endelige og viktige avklaringene i større grad i et samordnet regelverk og avklaringer som harmoniserer skattereglene på tvers av landegrensene.

# CompLex 1/24 – Forslag til lover og forskrifter med betydning for personvern



Forfattere: Lars Petter Fremstad, Lene Jeanette Johansen, Inger Marie Kristiansen Liepelt, Rose Margrethe Monrad og Dag Wiese Schartum. *Forslag til lover og forskrifter med betydning for personvern perioden 2018–2022*. Oslo: Universitetet i Oslo, Juridisk fakultet, Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk 2024, 1/2024. ISSN 2703-8777 Complex (online)

I perioden 2018–2022 ble det i alt fremmet ca. 700 lov- og forskriftsaker som reiste personvernsspørsmål på en slik måte at departementene anså Datatilsynet å være relevant høringsinstans.

Rapporten inneholder enkel statistikk som tallfester viktige sider ved denne rettsutviklingen, og refererer hovedinnholdet av alle 169 saker Datatilsynet gav hørings svar på. Rapporten er en gullgrube for den som

vil forstå hvordan lovgivning av betydning for personvern utvikler seg. Datagrunnlaget fra prosjektet er tilgjengelig for de som vil forske videre på disse endringene.

CompLex is a series of publications from the Norwegian Research Center for Computers and Law, the University of Oslo.

*Les hele utgivelsen på CompLex1/24 (pdf)*

## Personvern og GDPR i praksis



Forfattere: Eva Jarbekk og Simen Sommerfeldt. Oslo: Cappelen Damm Akademisk 2024, 372 s. ISBN: 9788202725969

GDPR-forordningen er et helt sentralt regelverk nærmest uansett hvilken bransje eller samfunnssektor man er en del av. I *Personvern og GDPR i praksis* sammenfattes kunnskap fra et spredt og uoversiktlig kildetilfang, samtidig gir forfatterne praktiske råd og løsningsforslag. Boken er utstyrt med sjekklister og har oppdaterte, konkrete tips fra erfarne personvernombud samt er ajourført med regelverk og praksis.

*Personvern og GDPR i praksis* tar blant annet for seg:

- sentrale begreper, roller og ansvarsforhold
- behandlingsgrunnlag som samtykke, avtale og «berettiget interesse»
- utforming av personvernerklæring
- dokumentasjonskrav og rutiner

- smidig utvikling av IT-systemer med innebygd personvern
- risikovurdering (ROS) og personvernkonsekvenser (DPIA)
- anonymisering og pseudonymisering
- hva databehandleravtalen bør inneholde

Andre emner som behandles, er individets rettigheter og innsynsrett, gjenbruk av personopplysninger til andre formål og avvikshåndtering. Forfatterne gir også praktiske råd om kundedatabehandling og markedsføringshenvendelser og for personvernombud og HR-avdelingen.

*Omtalen er hentet fra: [https:// utdanning.cappelendamm.no/ \\_personvern-og-gdpr-i-praksis-eva-jarbekk-simen-sommerfeldt-9788202725969](https://utdanning.cappelendamm.no/_personvern-og-gdpr-i-praksis-eva-jarbekk-simen-sommerfeldt-9788202725969)*



# The Verge

## ALL STORIES TAGGED

### Artificial Intelligence



Illustrasjon: The Verge

Artificial intelligence is more a part of our lives than ever before. While some might call it hype and compare it to NFTs or 3D TVs, AI is causing a sea change in nearly every part of the technology industry. OpenAI's ChatGPT is arguably the best-known AI chatbot around, but with Google pushing Gemini, Microsoft building Copilot, and Apple

working to make Siri good, AI is probably going to be in the spotlight for a very long time. At The Verge, we're exploring what might be possible with AI — and a lot of the bad stuff AI does, too.

*The Verge:* <https://www.theverge.com/ai-artificial-intelligence>

## Velkommen til årets faglige høydepunkt – AFIN fyller 30 år!

Avdeling for forvaltningsinformatikk (AFIN), UiO inviterer herved til konferanse med etterfølgende festmiddag for å feire AFINs 30-års jubileum.

Fredag 18. oktober inviterer vi til heldagskonferanse i Gamle Logen med topp innledere om viktige og vanskelig spørsmål for oss med interesse for digital forvaltning.

### Digital forvaltning: Hvor står vi, hvor går vi?

Fra programmet sakser vi *bl.a.*:

- direktør i Datatilsynet, Line Coll om «KI og personvern: Vil det bli mulig å gi effektivt vern av rettigheter og friheter?»
- direktør i NAV Hans Christian Holte «Om møtet mellom rettslige regulering og praktisk digitale forvaltning»,
- LDO-ombud Bjørn Erik Thon «Kan det være diskriminering å ikke ta hensyn til de «ikke-digitale»?» og

- professor Lee A. Bygrave om «Krav til transparens for KI-systemer som interagerer direkte med mennesker.»

Samme kveld blir det **festmiddag** for å feire at faget forvaltnings-

informatikk er 30 år. Vi tror dette blir en morsom fest og en hyggelig avslutning på en lærerik dag. Alle konferansedeltakere er hjertelig velkomne til å delta på middagen.

Se arrangementsside med fullt program *her*.





Gorrissen Federspiel

Tue Goldschmieding

## Nyt om persondataret i Danmark

### Datatilsynet indleder ikke tilsynssag mod Aarhus Kommune efter brug af referenceregister for medarbejderes voldelige forseelser

Det danske Datatilsyn (»Datatilsynet«) tog den 9. april 2024 i en sag med journalnummer 2024-432-0031 stilling til, om der var grundlag for at rejse en tilsynssag mod Aarhus Kommune efter, at kommunen havde oprettet et referenceregister indeholdende oplysninger om medarbejderes voldelige forseelser.

Datatilsynet anmodede i marts 2024 Aarhus Kommune om at besvare en række spørgsmål om referenceregisteret. I Aarhus Kommunes redegørelse fremgik det, at der var tale om et internt register til brug for Magistratsafdelingen for Sundhed og Omsorg. Referenceregisteret blev ikke delt på tværs af afdelinger i Aarhus Kommune.

Oplysninger om medarbejderes forseelser blev i forvejen behandlet af Magistratsafdelingen for Sundhed og Omsorg, hvorfor der alene var tale om en systematisering af oplysningerne i referenceregistret. Aarhus Kommune forklarede desuden, at oplysningerne i referenceregistret bliver slettet efter fem år.

I ansættelsessituationer kan ledere i Magistratsafdelingen for Sundhed og Omsorg foretage CPR-nummer søgninger i referenceregistret, men de kan kun se, om en person står registreret. Specifikke oplysninger om eventuelle forseelser er derimod kun tilgængelige

for HR. Herefter skal der foretages en konkret afvejning af hensynet til borgerne, herunder risikoen for gentagelse af den pågældende forseelse i forbindelse med medarbejderens genansættelse.

På baggrund af Aarhus Kommunes redegørelse vurderede Datatilsynet, at der ikke var anledning til at rejse en tilsynssag på det foreliggende grundlag.

Læs Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/apr/referenceregister-i-aarhus-kommune>

### Datatilsynet udtaler kritik af Roskilde Katedralskole brug af eksamensovervågningsprogram

Det danske Datatilsyn (»Datatilsynet«) afsluttede den 19. april 2024 tilsynssagen med journalnummer 2023-421-0019 om Roskilde Katedralskoles overholdelse af databeskyttelsesreglerne i forbindelse med eksamensovervågning.

Datatilsynet besluttede i februar 2023 at føre tilsyn med Roskilde Katedralskole, der ligesom mange andre danske gymnasier var begyndt at anvende eksamensovervågning for at forhindre eksamenssnyd. I forbindelse med eksamensovervågningen skete en behandling af elevernes personoplysninger i form af blandt navn, alder, CPR-nummer og konkret skærmsaktivitet.

Datatilsynet fandt indledningsvist, at behandlingen af personoplysningerne var nødvendige af hensyn til udførelsen af Roskilde

Katedralskoles myndighedsudøvelse jf. GDPR artikel 6, stk. 1, litra e.

Roskilde Katedralskole havde konkret vurderet, hvilke typer oplysninger der var nødvendige at indsamle, og fastsat en opbevaringsbegrænsning på 30 dage. Datatilsynet konkluderede på denne baggrund, at indsamlingen og opbevaringen af elevernes oplysninger var i overensstemmelse med GDPR artikel 5.

Eleverne fik udleveret skriftligt oplysningsmateriale, der forklarede, hvordan deres oplysninger blev behandlet som led i eksamensovervågningen. Selvom materialet som udgangspunkt var i overensstemmelse med oplysningspligten og GDPR artikel 13 og 14, opfordrede Datatilsynet til at anvende et mere letforståeligt og enklere sprog, da de henvender sig til unge studerende.

Datatilsynet udtalte afslutningsvist kritik af Roskilde Katedralskole, der ikke havde foretaget den nødvendige risikovurdering ved implementeringen af det nye eksamensovervågningsprogram. Efter GDPR artikel 25 skal specifikke risici identificeres ved den påtænkte behandlingsaktivitet. Datatilsynet vurderede, at Roskilde Katedralskole ikke havde taget tilstrækkelig stilling til risici i forbindelse med behandling af elevernes skærmbilleder, der blandt andet kunne indeholde informationer som private bogmærker, browserhistorik og personlige filnavne.

Læs Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/apr/kritik-af-gymnasi>

ums-brug-af-eksamensovervaagningssoftware

## Datatilsynet udtaler kritik af Telmore A/S' deling af personoplysninger med Facebook

Det danske Datatilsyn (»Datatilsynet«) traf den 29. april 2024 afgørelse i en sag med journalnummer 2023-31-0007, hvor en borger havde klaget over Telmore A/S' (»Telmore«) videregivelse af borgers personoplysninger til Meta Ireland (»Meta«).

Det var i sagen lagt til grund, at Telmore havde videregivet klagerens e-mailadresse til Meta med henblik på, at klageren ikke skulle modtage målrettet annoncering fra Telmore på Facebook. Da Telmore og Meta i fællesskab bestemte formålene og hjælpemidlerne for behandlingen af klagerens e-mailadresse, konkluderede Datatilsynet, at Telmore og Meta var fælles dataansvarlige.

Videregivelsen og behandlingen af klagerens e-mailadresse var sket på baggrund af interesseafvejningsreglen i GDPR artikel 6, stk. 1, litra f, idet Telmore havde en legitim interesse i, at kunderne ikke blev udsat for uønsket reklame. Datatilsynet mente dog, at Telmore ikke havde truffet tilstrækkelige foranstaltninger, der sikrede, at den registrerede blev gjort tydeligt opmærksom på, at oplysningerne ville blive brugt i markedsføringsøjemed, at oplysningerne ville blive delt med sociale medier, og at den registrerede havde muligheden for at modsætte sig denne behandling.

Klageren havde en berettiget forventning om, at oplysningerne, der blev givet som led i mobilaftalen med Telmore, ikke blev benyttet til markedsføring. Datatilsynet fandt således efter en samlet vurdering, at behandlingen ikke var sket i overensstemmelse med interesseafvejningsreglen i GDPR artikel 6, stk. 1, litra f.

Da Telmore fejlagtigt havde antaget, at Meta var databehandler, var den grundlæggende forudsætning om den korrekte rollefordeling blevet tilsidesat. En fortsat undersøgelse vurderedes ikke at kunne hjælpe klager eller højne databeskyttelsesniveauet, især da Telmore ikke længere deler klagers e-mailadresse med Meta.

Datatilsynet udtalte afslutningsvist, at fremtidig brug af Metas værktøj til behandling af personoplysninger som sket i nærværende sag, kræver en ordning om fælles dataansvar efter GDPR artikel 26.

Læs Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/apr/kritik-af-telmore-as/2%80%99-behandling-af-personoplysninger>

## Datatilsynet udtaler alvorlig kritik af Nets DanID A/S i sag om nedbrud af NemID

Det danske Datatilsyn (»Datatilsynet«) traf den 2. maj 2024 afgørelse i en sag med journalnummer 2023-432-0017. Sagen angik Nets DanID A/S (»Nets«) som var dataansvarlig i forhold til administrationen af NemID, da der skete et nedbrud den 21. juni 2022. Nedbruddet medførte, at op mod 1.5 mio. brugere ikke kunne anvende NemID og normaldriften blev ikke genoprettet før den 25. juni 2022, da backup-løsningen var utilgængelig.

Datatilsynet udtalte, at kravet i GDPR artikel 32, stk. 1 om passende sikkerhed indebærer, at der jævnligt bør foretages test af backup og genetablering. Det skal derfor testes om backup udføres med passende intervaller, om backup-kopien er tilgængelig og indeholder alle relevante data, samt om backup-kopien er retvisende. Det skal endvidere testes, hvorvidt genetablering kan udføres med eksisterende procedurer, hvorvidt kopierne kan fungere sammen, samt hvorvidt genetablering kan ske hurtigt nok i forhold til, at konsekvensen sædvanligvis stiger med tiden.

Datatilsynet konkluderede, at de procedurer Nets havde implementeret i forhold til afprøvning, vurdering og evaluering af effektiviteten, ikke var tilstrækkelige. Datatilsynet lagde vægt på, at den seneste test af nødproceduren var sket to år inden nedbruddet, og at det ikke var muligt at genoprette normaldriften i fire dage efter nedbruddet. Datatilsynet havde ved vurderingen særligt lagt vægt på, at der var tale om kritisk, national infrastruktur.

På baggrund af ovenstående udtalte Datatilsynet alvorlig kritik af, at Nets behandling af personoplysninger ikke var sket i overensstemmelse med GDPR artikel 32, stk. 1.

Læs Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/maj/datatilsynet-udtaler-alvorlig-kritik-i-sag-om-nedbrud-af-nemid>

## Datatilsynet udtaler alvorlig kritik af Københavns Kommune i sag om håndtering af oplysninger angående 3.7 millioner personer

Det danske Datatilsyn (»Datatilsynet«) traf den 7. maj 2024 afgørelse i en sag med journalnummer 2024-442-4149. Sagen angik Københavns Kommune som i forbindelse med flytning af en større mængde data gav 37.500 medarbejdere uberettiget adgang til oplysninger om 3.7 millioner personer i knap to måneder.

Den dataansvarlige skal identificere risici og træffe passende sikkerhedsforanstaltninger, der beskytter de registrerede mod disse risici, efter GDPR artikel 32, stk. 1.

Datatilsynet lagde i deres afgørelse vægt på, at Københavns Kommune havde et set-up, hvor en enkelt medarbejders fejl resulterede i et nedbrud, der omfattede 3.7 millioner personer. Desuden forelå der ikke protokoller, der sikrede, at det umiddelbart efter flytningen af oplysningerne blev testet, hvem der havde adgang til oplysningerne. Datatilsynet udtalte yderligere, at

der i systemer med et stort antal fortrolige oplysninger om et stort antal brugere, stilles store krav til sikkerhedsniveauet ved behandlingen af oplysningerne. Datatilsynet forklarede særligt om diskswapping, at den dataansvarlige skal indføre foranstaltninger til at verificere, at rettigheder på mapper og filer på den nye disk er identiske med rettighederne på den tidligere disk.

Blot fordi de fleste af dataene krævede en SAS-installation for at blive læsbare, var der ikke efter Datatilsynets opfattelse sikret et passende sikkerhedsniveau, da en SAS-installation nemt ville kunne hentes på nettet.

På baggrund af ovenstående udtalte Datatilsynet alvorlig kritik af, at Københavns Kommunes behandling af personoplysninger var sket i strid med GDPR artikel 32, stk. 1.

Læs Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/maj/koebenhavns-kommune-faar-alvorlig-kritik-for-manglende-sikkerhedsforanstaltninger>

## Datatilsynet udtaler kritik af politikredsens manglende procedurer for anvendelse af logkontrol

Det danske Datatilsyn (»Datatilsynet«) afsluttede den 17. maj 2024 tilsynssagen med journalnummer 2023-813-0003 om tre politikredsens anvendelse af logkontrol.

Politiet behandler i forbindelse med deres arbejde store mængder af personoplysninger i deres sagsstyringssystem POLSAS, herunder fortrolige oplysninger om strafbare forhold. Politiet skal føre løbende logkontrol med brugernes adgang til personoplysninger i POLSAS for at sikre, at oplysninger kun tilgås i forbindelse med arbejdsmæssigt relevante formål.

Datatilsynet indledte i 2021 et tilsyn med Nordjyllands Politi, Fyns Politi og Bornholms Politi, for at sikre, at politikredsene overholdte

kravene til logkontrol og brugeradgang.

Det følger af lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger (»den danske retshåndhævelseslov«) § 27, at den dataansvarlige skal træffe passende tekniske og organisatoriske foranstaltninger, der skal sikre et tilstrækkeligt sikkerhedsniveau. Datatilsynet kom i den forbindelse frem til, at det ikke var tilstrækkeligt udelukkende at føre logkontrol ved konkret mistanke om misbrug. Det forventedes derimod, at der som minimum foretages en halvårlig stikprøvekontrol. Datatilsynet uddyber, at implementering af stikprøvekontroller ligeledes har en præventiv effekt.

Datatilsynet fandt på den baggrund, at der var grundlag for at udtale kritik af politikredsens manglende procedurer for løbende logkontrol.

Det bemærkes, at passende procedurer for stikprøvekontroller efterfølgende er blevet implementeret.

Læs Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/maj/tre-politikredse-faar-kritik-for-manglende-behandlings-sikkerhed-nordjyllands-politi>

## Datatilsynet offentliggør nye skabeloner til gennemførelse af konsekvensanalyser

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 22. maj 2024 to nye skabeloner til gennemførelse af konsekvensanalyser.

Enhver dataansvarlig skal efter GDPR artikel 35 foretage en konsekvensanalyse, inden en given behandling igangsættes, hvis behandlingen udgør en særlig høj risiko for den registrerede.

Datatilsynet konstaterede, at det for mange virksomheder og myndigheder kan være udfordrende at foretage konsekvensanalyserne, herunder i forbindelse med udviklingen og anvendelsen af kunstig intelli-

gens. De nye skabeloner skal bidrage til, at virksomheder og myndigheder i fremtiden skal have lettere ved at gennemføre konsekvensanalyserne.

Den ene skabelon kan benyttes til konsekvensanalyser af mere generisk karakter, hvor den anden fokuserer på udviklingen og anvendelsen af kunstig intelligens.

Skabelonerne indeholder en række konkrete eksempler på, hvilke risici og foranstaltninger virksomheder og myndigheder skal tage stilling til, når en konsekvensanalyse udarbejdes.

Skabelonerne er ikke udtømmende, hvorfor det er den enkelte virksomhed- eller myndigheds eget ansvar at vurdere, om konsekvensanalysen er i overensstemmelse med reglerne i GDPR.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/maj/nye-skabeloner-til-gennemfoerelse-af-konsekvensanalyser>

Læs skabelonen til konsekvensanalyser vedrørende databeskyttelse her: <https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.datatilsynet.dk%2FMedia%2F638519770150276707%2FSkabelon%2520til%2520konsekvensanalyse%2520ved%2520AI.xlsx&wdOrigin=BROWSELINK>

Læs skabelonen til konsekvensanalyser vedrørende databeskyttelse til AI-løsninger her: <https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.datatilsynet.dk%2FMedia%2F638519770150276707%2FSkabelon%2520til%2520konsekvensanalyse%2520ved%2520AI.xlsx&wdOrigin=BROWSELINK>

## Datatilsynet afslutter den sidste tilsynssag om behandlingssikkerheden i AULA og udtaler kritik til Københavns Kommune

Det danske Datatilsyn (»Datatilsynet«) traf den 23. maj 2024 afgørelse i tilsynssagen med journalnummer 2023-423-0005 vedrørende



Københavns Kommunes behandling af personoplysninger på kommunikationsplatformen AULA.

Datatilsynet har tidligere truffet fem afgørelser i tilsynssagen med Københavns Kommune.

Det følger af GDPR artikel 35, at enhver dataansvarlige skal foretage en konsekvensanalyse, inden en behandling igangsættes, hvis behandlingen udgør en særlig høj risiko for den registrerede. Datatilsynet vurderede, at Københavns Kommune ikke havde gennemført en fyldestgørende konsekvensanalyse, da den ikke opfyldte mindstekravene. Datatilsynet udtalte på denne baggrund kritik af Københavns Kommunes behandlingssikkerhed.

Afgørelsen indeholder desuden anbefalinger til kommunens videre arbejde med opdateringen af konsekvensanalysen. Især blev det anbefalet, at kommunen i deres reviderede risikovurdering strukturerer oplysningerne, så risikovurderingerne kan sammenlignes før og efter implementeringen af relevante foranstaltninger, og at sammenhængen mellem foranstaltninger og risici tydeliggøres.

Det bemærkedes endvidere, at Københavns Kommune har arbejdet på at reducere risici med særlig fokus på risikoen ved brug af UNI-login.

Læs Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/maj/koebenhavns-kommune-faar-kritik-i-tilsynssag-om-aula>

## Datatilsynet offentliggør vejledende tekst om underretning ved brud på persondatasikkerheden

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 27. maj 2024 en vejledende tekst om kravene til underretning af registrerede i forbindelse med brud på persondatasikkerheden efter GDPR artikel 34. Den vejledende tekst er baseret på konkrete tilsyn, som Datatilsynet har ført med en række danske virksomheder og myndigheder.

Datatilsynet konstaterede i flere tilfælde, at flere af underretningerne var utilstrækkelige, idet de manglede at inkludere samtlige de påkrævede oplysninger. En underretning om brud på persondatasikkerheden skal blandt andet omfatte beskrivelser af bruddets karakter og sandsynlige konsekvenser i et klart og forståeligt sprog, eventuelle relevante anbefalinger for at mindske mulige skadevirkninger samt en beskrivelse af de foranstaltninger, som den dataansvarlige selv har truffet for at håndtere bruddet.

Læs Datatilsynets vejledende tekst her: <https://www.datatilsynet.dk/bvaad-siger-reglerne/vejledning/sikkerhed/haandtering-af-brud-paa-persondatasikkerheden/underretning-af-den-registrerede-ved-brud-paa-persondatasikkerheden>

## Nordiske datatilsynsmyndigheder vedtager principper for at styrke børns databeskyttelse i online spil

De nordiske datatilsynsmyndigheder (»Datatilsynene«) vedtog den 30. maj 2024 på det årlige nordiske møde et sæt fælles principper, der skal sikre en øget beskyttelse af børns personoplysninger i forbindelse med online spil.

Princip-kataloget fokuserer på fire databeskyttelsesretslige principper, navnlig rimelighed, gennemsigtighed, dataminering og ansvarlighed. Kataloget henvender sig primært til spiludviklere, der agerer som dataansvarlige, og har til formål at gøre spiludviklerne opmærksomme på persondataretlige overvejelser, der kan være med til at fremme beskyttelsen af brugernes personoplysninger.

Kataloget kan være et effektivt værktøj til virksomheder, der udbyder onlinespil til mindreårige.

Læs Datatilsynenes principper her: <https://www.datatilsynet.dk/Media/638544622578121029/Princip-le%20on%20Children%20and%20Online%20Gaming%20june24.pdf>

## Datatilsynet omgør langvarig praksis, om at retten til indsigt ikke omfatter sikkerhedslogs, på baggrund af EU-dom

Det danske Datatilsyn (»Datatilsynet«) traf den 6. juni 2024 afgørelse i sagen med journalnummer 2024-32-0283, hvor en borger havde klaget over, at Indenrigs- og Sundhedsministeriet (»ISM«) havde afvist at give borgeren indsigt i CPR's sikkerhedslog. Med denne afgørelse ændrer Datatilsynet sin tidligere praksis, som udelukkede retten til indsigt i sikkerhedslogs.

Datatilsynet modtog den 3. oktober 2023 en klage fra Folketingets Ombudsmand, hvoraf det fremgik, at ISM med reference til Datatilsynets hidtidige praksis havde afvist at give indsigt i historiske logs fra CPR. Datatilsynet sendte klagen til revurdering i ISM, som fastholdte afslaget i en afgørelse den 4. januar 2024 med henvisning til den lovbekendtgørelse nr. 289 af 8. marts 2024 (»den danske databeskyttelseslov«) § 22, stk. 2. Bestemmelsen indeholder en undtagelse fra den registreredes ret til indsigt i, hvilke personoplysninger der behandles om vedkommende.

Den 22. juni 2023 afsagde EU-Domstolen dom i sagen C-579/21 og fastslog, at logfiler, herunder information om søgninger i en persons personoplysninger samt datoerne for og formålet med disse søgninger, er omfattet af retten til indsigt i henhold til GDPR artikel 15, stk. 1 (se dommens præmis 83).

På baggrund af denne dom konkluderede Datatilsynet i den aktuelle afgørelse, at GDPR artikel 15 også omfatter information om, hvilke virksomheder og myndigheder der historisk set har abonneret på oplysninger om registrerede i CPR. Datatilsynet fandt desuden, at hensynet til den dataansvarliges økonomiske interesse i at undgå ressourceforbrug på at opfylde indsigtsanmodninger ikke er omfattet

# NYTT OM PERSONVERN

af undtagelserne i den danske databeskyttelseslov § 22, stk. 2.

Dermed ændrer Datatilsynet sin langvarige praksis, som udelukkede retten til indsigt i sikkerhedslogs, ved at fastslå, at ISM ikke kunne afvise klagen.

Læs Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jun/hvad-gaelder-for-indsigt-i-logfiler>

## Datatilsynet lancerer GDPR-univers for små foreninger

Det danske Datatilsyn (»Datatilsynet«) lancerede den 19. juni 2024 et vejledningsunivers om GDPR rettet mod små foreninger. Universet indeholder råd og konkrete eksempler, særligt tilpasset foreningers udfordringer, med det formål at vejlede og sikre overholdelse af databeskyttelsesreglerne.

Universet indeholder blandt andet en 7-trins guide til overholdelse af GDPR og nyttige links til information, såsom en FAQ. Ind-

holdet er struktureret under tre hovedkategorier, navnlig boligforeninger, frivillige foreninger og nonprofitorganisationer, og er skræddersyet udfordringer, som disse kategorier af foreninger hyppigt møder.

Besøg Datatilsynets GDPR-univers for små foreninger her: <https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/gdpr-univers-for-smaa-foreninger>

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



Illustration: Colourbox.com



## Bird & Bird

Gunnar Hjalt

### Fastställt fängelsestraff för grovt upphovsrättsintrång (IPTV)

Patent- och marknadsöverdomstolen (PMÖD) har fastställt fängelsestraff 2,5 år för två tilltalade som tillhandahållit ett nätverk för utsändning av IPTV under perioden september 2017 – oktober 2021. Dessutom har PMÖD fastställt en solidarisk skadeståndsskyldighet om ca 114 000 000 SEK, vilket var en sänkning från underrättens belopp som byggde på fler användare (8 303) än vad PMÖD slutligt kom fram till (5 000). Vidare skulle ett antal beslagtagna IPTV-boxar förverkas.

Det grova upphovsrättsbrottet avsåg intrång i den till upphovsrätten närstående rättigheten signalrätten, i 48§ upphovsrättslagen. Rubriceringen grovt upphovsrättsbrott infördes i svensk rätt den 1 september 2020 och straffskalan är densamma för intrång i de närstående rättigheterna som för intrång i upphovsrättigheter.

Se avgörandet i dess helhet här:

<https://www.domstol.se/globalassets/filer/domstol/patentochmarknadsoverdomstolen/avgoranden/2024/pmb-14039-23.pdf>

### Svårt vilandeförklara svensk varumärkesansökan med hänvisning till pågående ogiltigförklaring av EU-varumärken

Patent- och marknadsdomstolen har avslagit en begäran om vilande-

förklaring av överklagad varumärkesansökan, samt även avslagit själva överklagandet, mot bakgrund av att vilandeförklaringen tog sikte på en pågående ogiltigförklaring av motanförda hinder i form av EU-varumärkesregistreringar där ansökningarna om ogiltighetsförklaring hade initierats först efter ansökningsdagen för den överklagade varumärkesansökan. Domstolen ansåg inte att bestämmelsen om vilandeförklaring i Rättegångsbalken 35 kap 5§, som enligt avgörandet i Högsta domstolen NJA 2010 s. 609 är analogt tillämplig vid hand-

läggning av domstolsärenden, var tillämplig i ärendet eftersom det inte förelåg synnerlig vikt för prövningen att frågan om ogiltigförklaring prövades först. Sökanden var enligt domstolen oförhindrad att på nytt ansöka om registrering, om dennes ansökningar om ogiltigförklaring skulle visa sig framgångsrika. *Varumärket 2022-03489 Marrybrown ./. MARY BROWN'S och Mary Brown's Famous Chikken & Taters! (fig).*

Gunnar Hjalt, Senior Counsel,  
Bird & Bird Advokat.



Illustration: Colourbox.com



## Gorrissen Federspiel

Tue Goldschmieding

### PET skulle ikke udlevere eller destruere dagbogskopier

Den danske Højesteret afsagde den 18. april 2024 dom i sagen BS-49623-HJR mellem Dansk Forfatterforening som mandatar for en forfatter over for Rigspolitiet og Rigsarkivet.

Sagen handlede om forfatteren, der i 1981 fik beslaglagt nogle dagbøger, fordi myndighederne mente, at forfatteren havde samarbejdet med sovjetiske agenter. Sagen blev dengang afgjort med et tiltalefråfald, og forfatteren fik sine dagbøger tilbage, men blev senere klar over, at PET havde taget en kopi af dem.

Forfatteren mente, at denne handling krænkede både hans privatliv efter EMRK samt ophavsretten til dagbøgerne.

Vedrørende spørgsmålet om ophavsretskrænkelsen fastslog Højesteret, at lovbekendtgørelse nr. 1093 af 20. august 2023 (»den danske ophavsretslov«) fastslår, at det ikke er i strid med ophavsretten, når statslige arkivalier gøres tilgængelige i overensstemmelse med arkivlovgivningen.

Vedrørende spørgsmålet om privatlivskrænkelsen kom Højesteret indledningsvist frem til, at der ved selve beslaglæggelsen forelå et indgreb i forfatterens ret til privatliv, men at indgrebet under hensyn til PET's efterretningsmæssige arbejde var lovligt og proportionalt efter EMRK artikel 8, stk. 2.

Den efterfølgende arkivering udgjorde ifølge Højesteret ligeledes et indgreb i forfatterens ret til privatliv efter EMRK artikel 8, stk. 1. Efter en samlet vurdering fandt

Højesteret, at også arkiveringen var lovlig, idet formålet med arkiveringen var omfattet af hensynene opregnet i EMRK artikel 8, stk. 2.

Spørgsmålet var herefter, om arkiveringen kunne anses for nødvendig i et demokratisk samfund til varetagelse af de nævnte hensyn. Højesteret vurderede, at det efter praksis fra Menneskerettighedsdomstolen var lovligt og proportionalt at foretage mere generelle og automatiserede indgreb i individers ret til privatliv, såfremt disse byggede på samfunds- og ressourcemæssige hensyn.

Højesteret konkluderede således, at der ikke var grundlag for at udlevere eller destruere dagbogskopierne og stadfæstede dermed Landsrettens dom.

Læs dommen her: [https://domstol.fe1.tangora.com/media/-300016/files/49623-2023\\_Anonymiseret\\_dom\\_til\\_hjemmesiden.pdf](https://domstol.fe1.tangora.com/media/-300016/files/49623-2023_Anonymiseret_dom_til_hjemmesiden.pdf)

### Forvekslingsrisiko mellem babysutter

Sø- og Handelsretten afsagde den 26. april 2024 dom i sagen BS-33118/2021-SHR, hvor AH Licens ApS og Bibs Danmark ApS (samlet »Bibs«) over for FB Trading ApS, Frigg Production ApS, Sundesutter.dk ApS og FB Group ApS (samlet »Frigg«) gjorde gældende, at der forelå en krænkelse af rettighederne til sutterne af type »Bibs Colour« og »Bibs De Lux« efter lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«).

Retten fastslog indledningsvist, at Bibs sutter »Bibs Colour« og »Bibs De Lux« havde en sådan markedsposition og hver for sig sådanne

udtryksmæssige karakteristika, at de på det tidspunkt, hvor Frigg lancerede sutterne af typen »Frigg«, var beskyttet mod nærgående efterligninger i medfør af den danske markedsføringslovs § 3, stk. 1.

Frigg sutterne »Frigg Classic« og »Frigg Color Blocks« fremstod designmæssigt med en del ligheder i forhold til Bibs sutterne. Retten fremhævede særligt ligheden i sutternes farve, materialer, form og det overordnede udtryk, og fandt, at der forelå en nærliggende forvekslingsrisiko mellem produkterne.

Alene vedrørende sutton »Frigg Daisy« kom retten frem til, at der vare tale om design, der havde en tilstrækkelig grad af særpræg, hvorfor denne ikke krænkede rettighederne til Bibs sutterne.

Frigg blev forbudt at producere, markedsføre og sælge sutterne »Frigg Classic« og »Frigg Color Blocks«.

Læs dommen her: [https://domstol.fe1.tangora.com/media/-300011/files/Dom\\_BS-33118-2021-SHR.pdf](https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-33118-2021-SHR.pdf)

### Visningen af YouTube-, TikTok og Facebookvideoer uploadet af udenlandske brugere var ikke omfattet af den danske markedsføringslov

Sø- og Handelsretten afsagde den 16. april 2024 dom i sagen BS-27666/2022-SHR mellem VKR Holding AS (»VKR«) og Fakro sp. z o.o (»Fakro«).

Sagen handlede om, hvorvidt Fakro var ansvarlig for visningen af visse videoer på udenlandske profiler på sociale medier, samt om visningerne krænkede VKR's rettigheder efter lovbekendtgørelse nr. 866

af 15. juni 2022 (»den danske markedsføringslov«).

Det første spørgsmål var således, om den danske markedsføringslov fandt anvendelse på visningen, da der var tale om videoer uploadet af udenlandske brugere. Det var lagt til grund, at sagen alene vedrørte visningernes virkninger i Danmark. Retten fandt det ikke godtgjort, at videoerne havde en sådan virkning i Danmark, at de kunne siges at være rettet mod danske forbrugere. Retten lagde blandt andet vægt på, at videoerne ikke fandtes med dansk tekst og tale.

Da visningerne ikke var omfattet af den danske markedsføringslovs anvendelsesområde, blev Fakro fri-fundet.

Læs dommen her: [https://domstol.fe1.tangora.com/media/-300011/files/Dom\\_BS-27666-2022-SHR.pdf](https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-27666-2022-SHR.pdf)

## Mondelez krænkede Toms' rettigheder ved at sælge chokoladeæsker med betegnelsen »Alladin«

Sø- og Handelsretten afsagde den 26. april 2024 dom i sagen BS-14884/2023-SHR mellem Toms Gruppen A/S (»Toms«) og Mondelez Danmark ApS (»Mondelez«).

Sagen handlede om, hvorvidt Mondelez, der blandt andet er kendt for »Marabou« chokolade, krænkede Toms' rettigheder efter lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) og lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) ved at have markedsført og solgt chokolade med betegnelsen »Aladdin«.

Toms har siden 1945 haft rettighederne til ordmærket »Aladdin«, og retten vurderede indledningsvist, at denne ret var gyldigt stiftet. Spørgsmålet var dernæst, hvorvidt retten til ordmærket var fortabt som følge af manglende brug. Med udgangspunkt i markedsføringsmaterialer fandt retten, at Toms havde brugt ordmærket »Aladdin« for chokoladeæg til bland-selv-slik, og bemær-

kede samtidig, at også salg til grossister udgør reel brug af varemærket.

Følgelig udgjorde Mondelez' salg af chokolade i Danmark under betegnelsen »Aladdin« en krænkelse af Toms' rettigheder efter den danske markedsførings- og varemærkelov, da der var lighed mellem såvel betegnelsen og varetypen.

Toms havde ikke dokumenteret tab som følge af krænkelsen, hvorfor der ikke blev tilkendt erstatning herfor. Retten fandt dog, at Mondelez skulle betale en skønsmæssigt vederlag på 20.000 kr. for den uberegtigede brug af ordmærket. Retten lagde herved vægt på, at Mondelez havde solgt over 2.000 chokoladeæsker med betegnelsen »Aladdin«.

Mondelez blev endvidere forbudt at gøre erhvervsmæssigt brug af betegnelsen »Aladdin« for chokolader i Danmark samt påbudt at tilbagekalde og fjerne alle fortsat eksisterende varer med betegnelsen »Aladdin«.

Læs dommen her: [https://domstol.fe1.tangora.com/media/-300011/files/Dom\\_BS-14884-2023-SHR.pdf](https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-14884-2023-SHR.pdf)

## Råstoff kaffelikør mindede for meget om Kaluha

Sø- og Handelsretten afsagde den 29. april 2024 dom i sagen BS-26618/2023-SHR, hvor The Absolut Company AB (»Absolut«) over for Spritfabrikken Danmark ApS og Premium Productions ApS (»Spritfabrikken«) gjorde gældende, at emballagen til kaffelikøren Råstoff Coffee Liqueur udgjorde en retsstridig produktetfærligning af kaffelikøren Kaluha efter lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«).

Retten fastslog indledningsvist, at Kaluha med en markedsandel på mere end 90 % og det designmæssige karakteristiske gule udtryk havde en sådan markedsposition, at de var beskyttet mod nærgående efterligninger i medfør af den danske markedsføringslovs § 3, stk. 1.

Efter at have foretaget en visuel sammenligning af de to likørflasker

fandt retten, at designet af Råstoff kaffelikørs emballage udgjorde en illoyal markedsforstyrrelse. Retten konkluderede, at Spritfabrikken forsøgte at drage økonomisk fordel af Kaluha ved at skabe associationer til Kaluha og udnytte den markedsføringsindsats og det indarbejdede kendskab, som Kaluha har opnået hos forbrugerne. Der blev lagt særligt vægt på, at Spritfabrikken havde anvendt farvenuancer, der mindede meget om den som anvendtes hos Kaluha, og specifikt for kaffelikøren havde afvejet fra et beige design, som anvendtes for deres øvrige likører.

Spritfabrikken blev forbudt at producere, markedsføre og sælge Råstoff Coffee Liqueur i den specifikke emballage. Spritfabrikken blev tillige påbudt at tilbagekalde og fjerne alle produkter med den specifikke emballage.

Læs dommen her: [https://domstol.fe1.tangora.com/media/-300011/files/Dom\\_BS-26618-2023-SHR.pdf](https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-26618-2023-SHR.pdf)

## Virksomheder opfordres til at konkret beskrive, hvordan de kompenserer for CO<sub>2</sub>-udledning

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) oplyste den 7. maj 2024 i en pressemeddelelse, at der i samarbejde med de nordiske søstermyndigheder opfordres til at droppe generelle udsagn som »CO<sub>2</sub>-neutral« på baggrund af klimakompensationsordningen.

Efter § 13 i lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) skal rigtigheden af oplysninger om faktisk forhold kunne dokumenteres. Det betyder, at en erhvervsdrivende skal kunne dokumentere, at klima- og miljøsagn anvendt i markedsføringen er korrekte.

Flere virksomheder benytter sig af kompensationsordninger, hvor klimakreditter købes uden om det markedsførte produkts værdikæde.

Forbrugerombudsmanden mener, at denne type klima- og miljø-

udsagn kan vildlede forbrugere til at tro, at selve det markedsførte produkt er klimaneutralt. Det er derfor Forbrugerombudsmandens opfattelse, at det skal fremgå, at der er tale om en klimakompensationsordning uden for det markedsførte produkts værdikæde.

Forbrugerombudsmanden bemærkede yderligere, at udsagn der hævder klimaneutralitet eller reduceret eller positiv indvirkning på miljøet, der bygger på klimakompensationsordninger, efter alle omstændigheder vil være ulovlige efter implementeringen af ændringerne af Europa Parlamentets og Rådets direktiv 2005/29 om urimelig handelspraksis, der træder i kraft i september 2026.

Konkret anbefalede Forbrugerombudsmanden, at virksomheden i stedet beskriver, hvad de gør. Et udsagn kunne eksempelvis være »For hver solgte [produkt] støtter vi [plantning af nye træer] gennem [klimaprojekt], hvorved der over de næste 20 år bliver bundet [antal kg/ tons] CO<sub>2</sub>«.

Læs pressemeddelelsen her: <https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2024/20240507-nordiske-forbrugermyndigheder-klimandsagn-base-ret-paa-kompensationsordninger-er-nemt-vildledende/>

## Størstedel af YouTube-videoer havde karakter af anmeldelser og var ikke misrekommanderende

Sø- og Handelsretten afsagde den 8. maj 2024 dom i sagen BS-63297/2023-SHR, hvor Nviro A/S ("Nviro") over for Siky Energy ApS, Palle de Groot-Poulsen og Siky Ejendomme v/Palle de Groot Poulsen ("Siky") gjorde gældende, at en række YouTube-videoer uploadet af Siky udgjorde en misrekommandering af Nviro's omdømme og dermed var i strid med lovbekendtgørelse nr. 866 af 15. juni 2022 ("den danske markedsføringslov").

Siky havde på sin YouTube kanal uploadet en række videoer, der handlede om forskellige isoleringsløsninger og i enkelte tilfælde direkte henviste til Nviro's produkter.

For så vidt angik de videoer, hvor der ikke direkte blev henvist til Nviro, men papirisolering blot blev kommenteret generelt, kom retten frem til, at videoerne havde karakter af anmeldelser og gennemgang af en række krav til installationen. Retten vurderede således, at det ikke var sandsynliggjort, at disse videoer var i strid med den danske markedsføringslov.

For så vidt angik de videoer, hvor Nviro's produkter specifikt nævnes fandt retten, at størstedelen af videoerne har karakter af anmeldelser af produkterne, der beskriver produkternes egenskaber og anvendelighed, og således ikke i strid med den danske markedsføringslov.

Kun tre videoer vurderedes af retten at være i strid med den danske markedsføringslov. Her drejede det sig om to videoer, hvor Siky udtalte, at Nviro's produkter under ingen omstændigheder kunne installeres, hvilket retten ikke mente var faktisk korrekt. Den sidste video, som retten vurderede værende i strid med den danske markedsføringslov, omhandlede den igangværende retssag og sidestillede Nviro med Nazityskland.

Siky blev meddelt forbud mod offentligt at tilgængeliggøre de ovenfor tre nævnte videoer, men blev frifundet for de øvrige påstande.

Læs dommen her: [https://domstol.fe1.tangora.com/media/-300011/files/Kendelse\\_-\\_BS-63297-2023-SHR.pdf](https://domstol.fe1.tangora.com/media/-300011/files/Kendelse_-_BS-63297-2023-SHR.pdf)

## Obi Sport havde ikke fortabt rettighederne til ordmærket »Sport Direct«

Sø- og Handelsretten afsagde den 10. maj 2024 dom i sagerne BS-13516/2022-SHR og BS-40762/2022-SHR, der blev sambehandlet.

I den førstnævnte sag bestod parterne af Sportsdirect.com Retail Limited («Sportsdirect»), der er en kendt sport- og detailhandel ejet af Fraser Group-koncernen, og Obi Sport A/S («Obi»), der også sælger sportstøj og blandt andet er involveret i Intersport-kæden.

Her gjorde Sportsdirect gældende, at Obi havde fortabt rettighederne til det registrerede ord- og figurmærke »Sport Direct« som følge af manglende brug. »Sport Direct« er et velkendt mærke i dansk fodbold, som leverer blandt andet drikkedunke, taktiktavler og tasker til adskillige danske foreninger. For så vidt angik brug af ordmærket kom retten frem til, at brugen fandtes dokumenteret for beklædningsgenstande, legetøj, gymnastik- og sportsartikler og for reklame- og annoncevirksomhed, mens der ikke var sket reel brug for fodtøj, hovedbeklædning og julepynt. Retten ophævede derfor registreringen af ordmærket for fodtøj, hovedbeklædning og julepynt.

Vedrørende figurmærket konkluderede retten, at det ikke var brugt i sin originale form. Spørgsmålet for retten blev derfor, om den reelle brug var sket i en form, der ikke forandrede varemærkets særpræg, og dermed ikke afveg fra den form, hvori varemærket var blevet registreret, jf. lovbekendtgørelse nr. 88 af 29. januar 2019 («den danske varemærkelov») § 10c, stk. 4, nr. 1.

Retten fandt efter en visuel sammenligning af det originale og det anvendte figurmærke, at det anvendte mærke i den relevante 5-årsperiode havde et væsentligt anderledes særpræg end det registrerede varemærke, hvorfor det afveg i en sådan grad fra den form, hvori det blev registreret, at det ikke kunne betragtes som brug af det registrerede varemærke, jf. den danske varemærkelovs § 10 c, stk. 4, nr. 1.

Retten tog således Sportsdirects påstand om ophævelse af figurmærket til følge.

I den anden af de to sambehandlede sager var spørgsmålet, om Sportsmaster Danmark ApS (»Sportsmaster«), der ligeledes er en del af Fraser Group-koncernen, havde krænket Obi's fortsat eksisterende rettigheder til ordmærket »Sport Direct«.

Sportsmaster havde solgt og markedsført en stor sort taske/pose med betegnelsen »Sports Direct«. Selvom Obi's ordmærke ikke var registreret for tasker, vurderede retten, at tasken tilhørte det samme sportsunivers, og at der forelå en reel risiko for forveksling.

Sportsmaster blev forbudt at anvende betegnelsen »Sports Direct« ved salg og markedsføring som sket i sagen.

*Læs dommen her: [https://domstol.fe1.tangora.com/media/-300011/files/Dom\\_BS-13516-2022-SHR\\_og\\_BS-40762-2022-SHR.pdf](https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-13516-2022-SHR_og_BS-40762-2022-SHR.pdf)*

## »Kopi-ris« skulle tilintetgøres

Sø- og Handelsretten afsagde den 17. maj 2024 dom i sagen BS-27864/2023-SHR mellem Nadi Holding GmbH (»Nadi«) og Euro Foods ApS (»Euro Foods«), der handlede om, hvorvidt Euro Foods ved import af 27,5 tons ris krænkede varemærkerettigheder tilhørende Nadi.

Toldstyrelsen havde i maj 2023 tilbageholdt 27,5 tons ris, der var påført »Nadi« mærket. Retten kom frem til, at tilbageholdelsen var lovlig, idet der gjort erhvervsmæssig brug af varemærket uden rettighedshaverens samtykke jf. lov-bekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) § 4 og Europa Parlamentets og Rådets Forordning 2017/1001 af 14. juni 2017 (»Varemærkeforordningen«) art. 9, stk. 2.

Euro Foods gjorde **gældende, at alene emballagen for risene skulle destrueres**, og at risene kunne ompakkes. Selvom retten ud fra en proportionalitetsvurdering mente, at en ompakning var en mindre indgribende foranstaltning, var der

ikke forelagt tilstrækkelig dokumentation for mulighederne for ompakningen og risenes fysiske forhold under lageropbevaringen. Retten bestemte således, at risene skulle tilintetgøres uden erstatning eller kompensation til Euro Foods, jf. den danske varemærkelovs § 44, stk. 1, nr. 3.

Retten kom afslutningsvist frem til, at Euro Foods ikke havde handlet uagtsomt eller forsætligt, da de ikke var involveret i pakningen af risene, hvorfor der ikke var grundlag for at tilkende Nadi et vederlag for varemærkekrænkelsen.

*Læs dommen her: [https://domstol.fe1.tangora.com/media/-300011/files/Dom\\_BS-27864-2023-SHR.pdf](https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-27864-2023-SHR.pdf)*

## Musiker måtte ikke optræde som »ADHD«

Sø- og Handelsretten afsagde den 21. maj 2024 dom i sagen BS-52670/2023-SHR mellem H1t-makers v/ Jacob Nørhave Simonsen (»Jacob Simonsen«) og Fretz Music v/ Frederik Skærbæk Dyrby Nielsen (»Frederik Skærbæk«), der i perioden fra 2016 til 2022 tilsammen udgjorde duoen »ADHD«.

Sagen handlede om gyldigheden af det registrerede ordmærke »ADHD« og brugen af kunstnernavnet »ADHD«.

Parterne havde i fællesskab komponeret, produceret og optrådt med musik under navnet ADHD, og derved udøvet erhvervsmæssige aktiviteter, hvorfor varemærket »ADHD« ansås som stiftet i lige sameje ved ibrugtagning jf. lov-bekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) § 3, stk. 1, nr. 3. Der var ikke dokumenteret noget formelt ophør af samejet af varemærket. Retten fandt således, at Frederik Skærbæk gjorde uretmæssig brug af navnet »ADHD« til at promovere sine solooptrædere. Det var derfor også ugyldigt, da Frederik Skærbæk registrerede »ADHD« som ordmærke, da varemærket allerede var stiftet i lige sameje ved ibrugtagning.

Med udgangspunkt i omsætningen fra før samarbejdets ophør blev Frederik Skærbæk tilpligtet at betale Jacob Simonsen en skønsmæssig erstatning og et rimeligt vederlag på samlet 250.000 kr. jf. den danske varemærkelovs § 43, stk. 1 og 2, og lov-bekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 24, stk. 2 og 3 for indtægter genereret under navnet ADHD efter samarbejdets ophør.

Der var intet til hinder for, at Frederik Skærbæk kunne markedsføre sig og optræde som »Frederik fra ADHD« uden Jacob Simonsens forudgående samtykke.

*Læs dommen her: [https://domstol.fe1.tangora.com/media/-300011/files/Dom\\_BS-52670-2023-SHR.pdf](https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-52670-2023-SHR.pdf)*

## Forenings brug af betegnelsen »legal tech« var beskrivende for dens aktiviteter

Sø- og Handelsretten afsagde den 22. maj 2024 dom i sagen BS-19511/2023-SHR mellem Copenhagen Legal Tech ApS (»Copenhagen Legal Tech«) og Foreningen Copenhagen Legal Tech.

Sagen handlede om, hvorvidt Foreningen Copenhagen Legal Techs brug af navnene eller foreningskendetegnene »Foreningen Copenhagen Legal Tech« og »Copenhagen Legal Tech« var i strid med Copenhagen Legal Tech ApS' rettigheder til selskabsnavnet LEGALTECH ApS og til det registrerede varemærke LEGALTECH.

Retten bemærkede under henvisning til Østre Landsret dom af 28. juni 2023, at begrebet legal tech har et bredt anvendelsesområde, og at Patent- og Varemærkestyrelsen afviste at registrere varemærket for teknologiske og juridiske ydelser, da varemærket kunne være beskrivende for ydelser i disse klasser.

Retten lagde til grund, at Foreningen Copenhagen Legal Tech ved dets virke søger at fremme udviklingen af og interessen for legal tech blandt danske studerende og udvalgte virksomheder. Retten

fandt således, at foreningens brug af betegnelsen legal tech måtte anses som værende beskrivende for foreningens aktiviteter.

Foreningen Copenhagen Legal Tech blev frifundet.

Læs dommen her: [https://domstol.fe1.tangora.com/media/-300011/files/BS-19511-2023-SHR\\_Dom.pdf](https://domstol.fe1.tangora.com/media/-300011/files/BS-19511-2023-SHR_Dom.pdf)

## TV 2-dokumentar »Den sorte svane« var af samfundsmæssig interesse

Østre Landsret afsagde den 27. maj 2024 kendelse i sagen BS-22906/2024-OLR om nedlæggelsen af et forbud mod offentliggørelsen af TV2 dokumentaren »Den Sorte Svane«, der skulle sendes dagen efter afsigelse af kendelsen. Sagen foregik for store dele for lukkede døre, og rettens begrundelse er pseudonymiseret.

I dokumentaren følger man en kvindelig jurist, der agerer som muldvarp i bandemiljøet. Hun bistår bandemedlemmer, forretningsmænd og advokater med hvidvask, svindel med forurenede jord og anden kriminalitet. Formålet med dokumentaren er at belyse, hvordan profilerede aktører inden for advokat- og forretningsverden bidrager til og dækker over grov kriminalitet i bandemiljøet.

Muldvarpen ønskede ikke dokumentaren offentliggjort, da hun mente, at den udgjorde en trussel mod hendes liv, helbred og velfærd.

Retten kom indledningsvist frem til, at den indgående kontrakt og projektaftale mellem muldvarpen og TV2 ikke muliggjorde en vetoret for muldvarpen.

Spørgsmålet var således, om der forelå så alvorlige trusler mod muldvarpens liv, helbred, velfærd, og om de sikkerhedsforanstaltninger, hun måtte underkaste sig, udgjorde et sådant indgreb i hendes almindelige livsudfoldelse, at hun ansås for berettiget til at tilbagekalde sit samtykke til offentliggørelsen som følge af bristende forudsætninger. Alternativt skulle retten

tage stilling til om aftalen skulle tilsidettes i medfør af § 36 i lov-bekendtgørelsen nr. 193 af 2. marts 2016 (»den danske aftalelov«) eller lov nr. 11000 af 15. april 1683 (»Danske Lov«) 5-1-2, herunder til-lige henset til statens positive for-pligtelser til at sikre hendes liv og sikre hendes privatliv efter Den Europæiske Menneskerettigheds-konvention artikel 2, stk. 1, og arti-kel 8, stk. 1.

Retten bemærkede, at et forbud mod offentliggørelse af optagelser som de foreliggende udgør et indgreb i ytrings- og informations-friheden, som kun kan foretages, hvis tungtvejende grunde taler her-for. Retten henviste i den forbindel-se til principperne bag den danske grundlovs § 77 samt artikel 10, stk. 2, i Den Europæiske Menneske-rettighedskonvention.

Da TV2 allerede havde forelagt optagelserne for de i dokumentaren viste personer herunder bandemedlemmer, var det allerede kendt i de kriminelle miljøer, at den kvindelige jurist havde ageret som muldvarp. Politiets iværksatte foranstaltninger fandtes ikke at overskride, hvad muldvarpen måtte have accepteret at tåle.

Retten fandt det således ikke sandsynliggjort, at muldvarpen kunne forbyde offentliggørelsen, og lagde særligt vægt på at hensynet til ytringsfriheden og samfundets inte-resse vejede tungere end muldvar-pens interesse i at dokumentaren ikke skulle offentliggøres.

Læs dommen her: <https://domsdata-basen.dk/#sag/5587/6686>

## Biogen havde gyldig markedsføringsbeskyttelse for lægemidlet Tecfidera – Dimethyl fumarat

Sø- og Handelsretten afsagde den 29. maj 2024 dom i sagen BS-62147/2023-SHR mellem Biogen Netherlands B.V. og Biogen (Denmark) A/S (»Biogen«) overfor Sandoz A/S (»Sandoz«).

Sagen handlede om, hvorvidt Sandoz kunne forbydes at markedsføre lægemidlet Dimethyl fumarate »Hexal«, som følge af en markedsføringsbeskyttelse tilhørende Bio-gen.

Biogen blev den 2. maj 2023 tildelt en markedsføringsbeskyttelse for lægemidlet Tecfidera – Dimethyl fumarat ved gennemførelsesafgørelse af EU Kommissionen. Sandoz mente, at denne gennemførelsesafgørelse var behæftet med fejl, da den byggede på et faktisk forkert grundlag, og allerede af den årsag var ugyldig. Påstanden byggede sær-ligt på, at gennemførelsesafgørelsen, ifølge Sandoz, byggede på forælde-de data og ikke tog en rapport udar-bejdet af Committee for Medicinal Product for Human Use (CHMP) med i vurderingen. Retten vurderede dog, at Kommissionen på trods af kendskab til rapporten ikke var forpligtet til at inddrage CHMP's rapport, hvorfor der ikke forelå nogen klar fejl eller mangel ved gennemførelsesafgørelsen.

Da Sandoz ikke havde sandsyn-liggjort, at markedsføringsbeskyttel-sen var ugyldig, betød det samtidig, at Sandoz markedsføring af Dime-thyl fumarate »Hexal« krænkede Biogens rettigheder og var i strid med lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske mar-kedsføringslov«) § 3.

Sandoz blev meddelt et midlerti-digt forbud mod markedsføring af lægemidlet Dimethyl fumarate »Hexal« mod sikkerhedsstillelse af et beløb på 75 mio. kr. fra Biogen.

Læs dommen her: [https://domstol.fe1.tangora.com/media/-300011/files/Kendelse\\_BS-62147-2023-SHR.pdf](https://domstol.fe1.tangora.com/media/-300011/files/Kendelse_BS-62147-2023-SHR.pdf)

## Mærkningsordning for strøm fra vedvarende energi ophæves

Den danske Forbrugerombuds-mand (»Forbrugerombudsmanden«) oplyste den 3. juni 2024 i en presse-meddelelse, at retningslinjerne for elhandelsvirksomheders brug af klimamæssige udsagn ved markeds-føring af strøm ophæves.



Ordningen var i 2020 blevet indført for at gøre det mere gennemskueligt for forbrugere at forholde sig til, hvor klimavenlige elprodukter var i forhold til hinanden. Elprodukterne kunne således opnå op til to grønne blade, der afspejlede deres klimaaftryk.

I januar 2023 skulle mærkningsordningen revideres. Retningslinjerne blev i den forbindelse i en forhandlingsgruppe diskuteret, og det var ikke muligt at nå til enighed om enkelte punkter. Mærkningsordningen blev derfor ophævet med virkning fra den 1. september 2024. Elhandelsvirksomheder skal således sikre sig at have fjernet alle grønne blade fra deres markedsføring inden denne dato.

Læs pressemeddelelsen her: <https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2024/20240603-forbrugerombudsmanden-ophaever-groen-maerkningsordning-for-stroem-fra-vedvarende-energi/>

## Markedsføring af »Becker«-maling var i strid med IP-rettigheder, da forhandleraftale var ophørt ved konkurs

Sø- og Handelsretten afsagde den 3. juni 2024 dom i sagen BS-32198/2023-SHR mellem PPG Coating Danmark A/S (»PPG«) over for M. Beckmann ApS, Beckmann Invest A/S og Martin Claudi Beckmann (»Beckmann«).

PPG er datterselskab til det amerikanske selskab PPG Industries, Inc., der producerer maling, og ejer rettighederne til varemærket »Beckers«. PPG indgik forhandleraftale med Beckmann A/S om salg af maling under mærket »Beckers«. Beckmann A/S gik i februar 2023 konkurs. Selvom det fremgik af forhandleraftalen, at denne skulle ophøre ved konkurs, fortsatte Beckmann salget og markedsføring af Beckers maling i Beckmann ApS. Beckmann solgte blandt andet for gammel Beckers maling og blandede malingen med andre produkter. Retten kom herefter frem til, at

Beckmann havde krænket PPG's rettigheder efter lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) og lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«).

Beckmann havde tillige anvendt PPG's farvedatabase efter konkurens indtræden. Farvedatabasen var oparbejdet over en længere årrække og indeholdt omkring 46.000 unikke farvekoder. Udviklingen af farvedatabasen var således resultatet af en væsentlig økonomisk og arbejdsmæssig investering, og dermed omfattet af sui generis beskyttelsen i lovbekendtgørelse nr. 1093 af 20. august 2023 (»den danske ophavsretslov«) § 71, stk. 1. Retten fandt, at Beckmann havde handlet i strid med PPG's enerettigheder efter den danske ophavsretslov ved at benytte farvedatabasen efter ophør af forhandleraftalen.

Farvedatabasen udgjorde ligeledes en forretningshemmelighed, da oplysningerne i databasen ikke var almindeligt kendte. Da det fremgik af forhandleraftalen, at forretningshemmeligheder ikke på noget tidspunkt måtte videregives, kom retten frem til, at tilrådighedsstillelsen af databasen for Beckmann ApS udgjorde en ulovlig brug af forretningshemmeligheder jf. lov nr. 309 af 25. april 2018 om forretningshemmeligheder (»den danske lov om forretningshemmeligheder«) § 4, stk. 1 og stk. 2, nr. 1, 2 og 3, og stk. 4, jf. § 2.

Beckmann blev forbudt at anvende betegnelsen »Beckers« i erhvervsmæssig sammenhæng samt at anvende materiale omfattet af forhandleraftalen. Retten fastsatte erstatning og et rimeligt vederlag til 1 mio. kr. samt en bødestraf på 50.000 kr.

Læs dommen her: [https://domstol.fe1.tangora.com/media/-300011/files/Dom\\_BS-32198-2023-SHR.pdf](https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-32198-2023-SHR.pdf)

## Power fodbold-reklamer krænkede ikke DBU's rettigheder til fodboldherrelandsholdet

Østre Landsret afsagde den 4. juni 2024 dom i sagen BS-22133/2023-OLR mellem Dansk Boldspil-Union (»DBU«) og Power A/S (»Power«).

Power havde under EM-slutrunden i 2021 bragt tre reklamer, der blandt andet viste en animeret fodboldspiller i en orange fodboldtrøje på et fodboldstadion og teksten »Den store fodboldfest«. DBU mente, at reklamerne krænkede rettighederne til det danske fodboldherrelandsholds navn og kendetegn.

Sø- og Handelsretten kom i sagen BS-26458/2022-SHR frem til, at reklamerne i højere grad skabte associationer til fodbold som sport og til EM-slutrunden end til det danske herrelandshold. Retten lagde herved vægt på, at reklamerne var påført et Power-logo (og ikke DBU), og at reklamerne blev vist i forbindelse med en national begivenhed.

Landsretten kom, ligesom Sø- og Handelsretten, frem til, at DBU's rettigheder ikke var krænket, og stadfæstede derfor Sø- og Handelsrettens dom i det omfang, den var anket.

Læs Sø- og Handelsrettens dom her: [https://domstol.fe1.tangora.com/media/-300011/files/Dom\\_\(Power\\_mod\\_DBU\).pdf](https://domstol.fe1.tangora.com/media/-300011/files/Dom_(Power_mod_DBU).pdf)

Læs Østre Landsrets dom her: <https://domstol.dk/media/cojpxi5/bs-22133-2023-olr.pdf>

## Betegnelsen »Himmerlands Pejsecenter« vare beskyttet efter den danske markedsføringslov

Sø- og Handelsretten afsagde den 17. juni dom i sagen BS-53492/2023-SHR mellem Himmerlands Pejsecenter ApS (»Himmerlands Pejsecenter«) over for Ecoteck A/S (»Ecoteck«) og Brændeovns Finans ApS (»Brændeovns Finans«).

Sagen handlede om, hvorvidt Ecoteck og Brændeovns Finans handlede i strid med Himmerlands

Pejsecenters rettigheder ved at anvende betegnelsen »Himmerlands Pejsecenter« på deres fælles hjemmeside skiftpejs.dk.

Retten fastslog indledningsvist, at betegnelsen »Himmerlands Pejsecenter« blandt andet som følge af den mangeårige anvendelse havde opnået den fornødne markedsføringsretlige beskyttelse, selvom ordene hver især er af beskrivende karakter.

Betegnelsen »Himmerlands Pejsecenter« var identisk med Himmerlands Pejsecenters forretningskendetegn, da både »Himmerland« og »Pejsecenter« anvendtes sammensat og var skrevet med versaler. Retten tilføjede desuden, at parterne opererede indenfor samme branche og geografiske område, hvilket understøttede den øgede risiko for forveksling.

Retten fandt derfor, at Ecoteck og Brændeovns Finans anvendte Himmerlands Pejsecenters forretningskendetegn på en måde, der var egnet til at fremkalde risiko for forveksling. Ecoteck og Brændeovns Finans handlede derfor i strid med lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 3, stk. 1 og § 22 og blev forbudt at anvende Himmerlands Pejsecenters kendetegn.

Retten kom afslutningsvist frem til, at Himmerlands Pejsecenter manglede dokumentation til at sandsynliggøre et erstatningsberettiget tab, hvorfor retten ikke kunne foretage et skøn over opgørelsen af erstatning eller et rimeligt vederlag, jf. den danske markedsføringslovs § 24, stk. 2 & stk. 3.

Læs dommen her: [https://domstol.fe1.tangora.com/media/-300011/files/Dom\\_BS-53492-2023-SHR.pdf](https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-53492-2023-SHR.pdf)

## Licenstager var ikke berettiget til at registrere udvalgte varemærker i eget navn

Sø- og Handelsretten afsagde den 18. juni 2024 dom i sagen BS-28714/2020-SHR mellem Henrik Klimek og J.J. Jacobsen L.P. (»Jacobsen«) over for A. H. Riise Spirits ApS (»Riise Spirits«).

Jacobsen havde den 14. juni indgået en licensaftale om kommerciel udnyttelse af en række produkter og varemærker med selskabet Riise Spirits (tidligere B Rum ApS). Det fremgik af licensaftalen, at der alene var tale om en udnyttelsesret, og at alle rettighederne til varemærkerne tilhørte Jacobsen. Der var udarbejdet en procedure, hvorefter Riise Spirits kunne registrere de licenserede varemærker i andre lande. Varemærkerne skulle registreres i licensgiveren, Jacobsens navn. Retten fandt således, at Riise Spirits i henhold til licensaftalen ikke var berettiget til at registrere de respektive varemærker i licenstageren, Riise Spirits, navn. Riise Spirits blev tilpligtet at overdrage varemærkerne.

Da Riise Spirits ikke havde betalt royalties som bestemt i licensaftalen, udmålte retten erstatning og et rimeligt vederlag til et samlet beløb på 5 mio. kr.

Læs dommen her: [https://domstol.fe1.tangora.com/media/-300011/files/OF-FENTLIG\\_VERSION\\_af\\_dommen\\_BS-28714-2020-SHR.pdf](https://domstol.fe1.tangora.com/media/-300011/files/OF-FENTLIG_VERSION_af_dommen_BS-28714-2020-SHR.pdf)

## Indførsel af 50 kopivarer fra Tyrkiet var ikke privat brug

Østre Landsret afsagde den 26. juni 2024 dom i de sambehandlede ankesager BS-101/2023-OLR, BS-102/2023-OLR og BS-103/2023-OLR, der handlede om indførslen

af mere end 50 kopivarer af mærkerne Prada, Chanel, Louis Vuitton, Moncler og Balenciaga.

Det var i sagen ubestridt, at der var tale om kopivarer. Spørgsmålet var derimod, hvorvidt indførslen af kopivarerne var sket til personlig brug eller havde erhvervsmæssig karakter og dermed i strid med lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«).

Landsretten vurderede, at der allerede som følge af antallet af indførte kopivarer ikke kunne være tale om privat brug, hvorfor man ikke tog stilling til de fremlagte materialer, der viste en korrespondance mellem appellanten (tidligere sagsøgte) og vedkommendes familie.

Landsretten stadfæstede således Sø- og Handelsrettens dom med den ændring, at vederlaget til Balenciaga forhøjedes til 30.000 kr. ud fra et afskrækkelses- og forebyggelsesprincip jf. Parlamentets og Rådets direktiv af 29. april 2004 om håndhævelsen af intellektuelle ejendomsrettigheder 2004/48 (»rets-håndhævelsesdirektivet«), artikel 13, stk. 1.

Læs Sø- og Handelsrettens dom her: [https://domstol.fe1.tangora.com/media/-300011/files/Dom\\_BS-1073-2022-SHR\\_m.fl..pdf](https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-1073-2022-SHR_m.fl..pdf)

Læs Østre Landsrets dom her: <https://domsdata.basen.dk/#-sag/5790/6914>

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



# Selmer

Thea Kjølø, Øystein Kolstad Kvalø og Eilert Midttun Rostrup

## Statens standardavtaler er oppdatert

I juni 2024 ble flere av Statens standardavtaler (SSA) oppdatert (SSA-B (Bistandsavtalen), SSA-D (Driftsavtalen), SSA-K (Kjøpsavtalen), SSA-O (Oppdragsavtalen), SSA-T (Utviklings- og tilpasningsavtalen) og SSA-V (Vedlikeholdsavtalen)). Standardavtalene brukes i stor utstrekning ved anskaffelse av IT- og konsulenttjenester i både privat og offentlig sektor. Innholdet i standardavtalene er stort sett videreført, men det er gjort viktige endringer i ansvarsfordelingen mellom leverandør og kunde, samt presiseringer av partenes rettigheter og plikter i kontrakten. Avtalene er også bedre harmonisert. Disse endringene bidrar til økt klarhet, forutsigbarhet og en mer rettferdig balanse mellom leverandører og kunder.

### En mer balansert ansvarsfordeling mellom kunde og leverandør

Standardavtalene har blitt kritisert for å legge mye ansvar på leverandøren til fordel for kunden. Leverandørene har etter SSA-K, -V og -T vært ansvarlig ved mislighold fra alle underleverandører, også de som kun leverer standardprogramvare. I de oppdaterte avtalene er produsent av standardprogramvare ikke ansett som underleverandør, forutsatt at produsentens standardvilkår er inntatt som bilag til avtalen. Leverandørene bærer dermed ikke risikoen ved mislighold fra produsent av standardprogramvare i like

stor grad som tidligere. Dette er en velkommen endring for leverandørene, som ofte står uten mulighet til å kreve regress fra produsenter av standardprogramvare på grunn av produsentenes omfattende ansvarsbegrensninger.

Crowdstrike-hendelsen i juli illustrerer betydningen av denne endringen. Datasystemer over hele verden stanset som følge av en feiloppdatering fra leverandøren Crowdstrike. En rekke norske IT-selskaper som har levert Crowdstrikes antivirusprogram som en del av egne tjenester, ofte med godkjenning fra kunden, har blitt møtt med erstatningskrav. Spørsmålet er om konsekvensene av de oppdaterte standardavtalene er at kundene må bære tapet ved slike hendelser. I tilfeller der kunden har godkjent bruk av programvaren, er det ikke nødvendigvis mer rimelig at leverandøren alene bærer tapet. Derfor kan denne endringen bidra til en bedre balanse mellom partene. Det er likevel sannsynlig at vi i tiden fremover vil møte nye og komplekse juridiske spørsmål knyttet til definisjonen av standardprogramvare.

Avtalene er også oppdatert med en rekke mindre endringer som er positive for leverandørene. I SSA-B og -O har leverandøren nå rett til å si opp avtalen etter at det har gått 120 dager siden kunden stanset oppdraget eller bistanden. Den særegne bestemmelsen i SSA-D som gir kunden rett til å bytte ut leveran-

dørens personell, er også fjernet. I SSA-D, -V, -T og -O har leverandøren nå rett til å nekte å samarbeide med tredjeparter engasjert av kunden der dette er en «vesentlig ulempe» for eksisterende underleverandører eller «vesentlig forretningsmessig ulempe» for leverandøren.

I SSA-T har kunden fått rett til å forlange endringer av leveransen som er «nødvendige som følge av endrede rettslige krav». Formålet er trolig å sikre at kunden mottar programvare som kan brukes til tross for at de rettslige rammebetingelsene endrer seg underveis utviklingsløpet. Endrede rettslige krav er imidlertid ikke forhold leverandøren har kontroll over, og endringen medfører derfor en betydelig risiko for leverandørene.

Av øvrige endringer i SSA-T, kan nevnes at garantiperioden for utstyr er økt fra to til tre år.

I SSA-D, -O og -T er det presisert at leverandørene har ansvar for egen bruk av underleverandører. Selv om denne endringen ikke utvider det eksisterende kontraktsmedhjelperansvaret, bidrar den til å tydeliggjøre ansvarsforholdene mellom partene.

Til tross for endringene som er gjort, kan det fremdeles gjøres mer for å bedre risikofordelingen mellom kunde og leverandør. SSA-O (Oppdragsavtalen), som forsøker å være en avtale for konsulentoppdrag der leverandøren har et resul-

tatansvar, har ikke et godt regime for godkjenning av leveransen. Et akseptanseregime er en grunnforutsetning for resultatansvarskontrakter, og dette er en stor mangel ved avtalen. Oppdragsavtalen mangler også et system for klar og detaljert spesifikasjon av leveransen, samt grundig regulering av utviklingsprosessen.

Ved mislighold krever avtalen en abstrakt og krevende vurdering av om leverandøren har levert «i samsvar med de funksjoner, krav og frister som er avtalb». Samtidig er ikke avtalen tydelig nok på hvordan leveransen skal spesifiseres ved kontraktsinngåelsen. Samlet legger disse forholdene en betydelig del av risikoen på leverandøren, og øker risikoen for tvister i tilfeller der sluttresultatet ikke er i tråd med hva kunden forventer.

## Harmonisering av standardavtalene for enklere bruk

Direktoratet for forvaltning og økonomistyring (DFØ) har oppnådd en større grad av harmonisering ved å anvende en mer enhetlig kapittelinndeling og ved å standardisere formuleringene i bestemmelsene som gjentas på tvers av avtalene. For leverandører og kunder som gjerne inngår flere IT- og tjenestekontrakter er dette gunstig. Bedre harmoniserte avtaler gjør det enklere å drive kontraktsforvaltning og ha kontroll på egne rettigheter og plikter i kontraktsforholdene. Overgangen til andre standardavtaler i nye prosjekter blir også enklere.

Harmoniseringen bør likevel ikke gå for langt. Standardavtalene dekker et bredt spekter av tjenester, inkludert levering, utvikling, drift, bistand og vedlikehold av teknologi og IT-tjenester. Det er derfor essensielt at de ulike standardavtalene tar hensyn til bredden i leveransene. De siste endringene reflekterer DFØs bevissthet om dette aspektet.



Illustrasjon: Colourbox.com

## Presisering av generelle kontraktsbestemmelser

Flere av kontraktsbestemmelsene har fått nødvendige presiseringer og oppklaringer, blant annet ved at flere ord og uttrykk er definert. Uttrykket «vesentlig mislighold» fra leverandørens side definert i SSA-D, -V og -T, og hvem som anses å være «utenforstående» i relasjon til taushetsplikten er definert i samtlige standardavtaler.

En særlig viktig endring er klargjøringen av leverandørens ansvar for sine leveranser i SSA-D og -V. I de tidligere versjonene av avtalene sto det at «[L]everandørens ytelser skal på en helhetlig måte dekke de funksjoner og krav som er spesifisert i avtalen». Hva en «helhetlig måte» betyr for leverandørens leverings- og tjenesteplikt, er uklart.

Formuleringen er nå endret. Etter SSA-V skal leveransen nå være «gjennomført med tilstrekkelig kvalitative og kvantitative ressurser og kompetanse, ut fra kravene i avtalen», og etter SSA-D har leverandøren nå «ansvar for at den samlede leveransen (den helhetlige løsningen) dekker de funksjoner og krav som er spesifisert i avtalen». Endringene bidrar til å sikre kontroll over ytelsespliktene og redusere risikoen for tvister.

## Nye rangordning for databehandleravtalen

I samtlige av de nye avtalene er rangordningsbestemmelsen oppdatert. I den nye bestemmelsen går

databehandleravtalen foran den generelle avtaleteksten og samtlige bilag når det gjelder «bestemmelser knyttet klart og utvetydig til regulering av personvern». Dermed unngår leverandøren å måtte oppfylle plikter i avtalen som kommer i konflikt med leverandørens personvernrettslige plikter.

## Forventninger til neste revisjon

SSAene blir aldri ferdigutviklet, og må kontinuerlig ajourholdes og forbedres for å sikre balanse mellom partene, samt holde tritt med utviklingen både i teknologisektoren og i samfunnet for øvrig. Det er avgjørende med et godt samarbeid mellom DFØ og interesseorganisasjoner som IKT Norge, og det er gledelig at IKT Norge spesielt påpeker behovet for å forbedre SSA-L og SSA-Sky i fremtiden.<sup>1</sup> Vi ser frem til neste oppdatering!

*Thea Kjølo. 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*

*Eilert Midttun Rostrup. Trainee.*

<sup>1</sup> «Nye versjoner av Statens Standardavtaler lansert.», 27.juni.2024, IKT-Norge.no, (Nye versjoner av Statens Standardavtaler lansert. | IKT Norge (ikt-norge.no))



## Gorrissen Federspiel

Tue Goldschmieding

### Trusselvurdering for destruktive cyberangreb hæves fra lav til middel

Det danske Center for Cybersikkerhed (»CFCS«) offentliggjorde den 4. juni 2024 en ny trusselvurdering, der hævdede trusselsniveauet for destruktive cyberangreb fra lav til middel.

Den nye vurdering bygger på, at de danske efterretningstjenester anser det for tiltagende sandsynligt, at Rusland vil anvende hybride virkemidler i fremtiden. Hybrid krigsførelse handler ikke udelukkende om militære mål, men indbefatter blandt andet politiske, informationsmæssige eller økonomiske virkemidler, der kan påvirke samfundet i de pågældende lande.

CFCS opfordrer derfor danske myndigheder og virksomheder til at vurdere og om nødvendigt styrke deres cybersikkerhed. Særligt sikkerheden imod angreb, der har til formål at destruere data eller forårsage systemnedbrud, bør styrkes. Som eksempel på sådanne angreb nævnes specifikt Wiper-angreb, falsk ransomware eller DDoS-angreb.

Læs trusselvurderingen her: <https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselvurderinger/-cfcs-haver-trussel-fra-destruktive-cyberangreb-.pdf>

### Nyt inspirationskatalog til anvendelse af AI i den offentlige sektor

Den danske Digitaliseringsstyrelse (»Digitaliseringsstyrelsen«) offentliggjorde d. 20. juni 2024 et nyt inspirationskatalog til anvendelsen af AI i den offentlige sektor.

Inspirationskataloget henvender sig til medarbejdere i den offentlige

sektor og har til formål at demonstrere, hvor og hvordan AI kan benyttes til at effektivisere og kvalitetssikre den daglige arbejds-gang.

I inspirationskataloget præsenteres syv forskellige cases, hvor AI allerede har været med til at skabe værdi i hverdagen. Casene dækker blandt andet, hvordan AI kan bruges i den daglige kommunikation med borgere, og hvordan AI kan medvirke til udarbejdelse af hørings svar eller journaler.

Digitaliseringsstyrelsen fremhæver, at det er meget vigtigt at afklare tekniske og juridiske forhold med organisationen forinden AI benyttes.

Læs inspirationskataloget her: [https://digst.dk/media/31720/inspirationskatalog-syv-eksempler-med-generativ-ai-i-den-offentlige-sektor-webtilgaengelig\\_final.pdf](https://digst.dk/media/31720/inspirationskatalog-syv-eksempler-med-generativ-ai-i-den-offentlige-sektor-webtilgaengelig_final.pdf)

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



Illustration: Colarbox.com

