

Lov & Data

Juni 2025

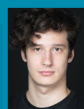
Nr. 162 2/2025

Innhold

Leder 2

Artikler

Victoria Jakobsen Digital Operational Resilience: A Guide for crypto- asset service providers under DORA and MiCA	4
Otto Lindholm Can Database Rights Prohibit Training AI on Finnish Laws?	7
Martin Brinnen Högsta domstolen sammanjämkar svenska mediegrundlagarna med dataskyddsförordningen . . .	9
Annelin Sødal Etterretningstjenestens nye «overvåkningshjemler» – et svekket kommunikasjonsvern?	14
Nicholas Foss Barbantonis og Henning Wahlberg Birkenstock-sandaler er ikke beskyttet av opphavsrett . .	19
Ove A. Vanebo KI-forordningens krav om å sikre kompetanse innenfor kunstig intelligens	22
Aras Nazarovas When Wellness and Security Apps Betray Your Trust . .	26
Øystein Blymke «Planseksjonen» – et fremmedord for Justisdepartementet i 1975	28
Kristian Foss og Christer Berg Johannesen NIS2: Hvilke konkrete sikkerhetskrav gjelder? Del 2 i artikkelserien om cybersikkerhet og NIS2 . .	31
Steinar Skagemo Hva sier forslaget til ny forvaltningslov om samtykkebasert deling?	39
Stein Schjøllberg State sovereignty in cyberspace regulating global technology companies	43
JusNytt	49
Halvor Manshaus Kunstig intelligens og ærekrenkelser: Avgjørelse fra USA trekker linjer overfor ChatGPT og OpenAI	
Aktuell i dag.	55
Peter Wahlgren Peter Seipel 1939–2025	
Rettsinformatisk litteratur med mer.	57
Nytt om personvern	60
Nytt om immaterialrett.	65
Nytt om IT-kontrakter.	75
Annet nytt	78



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, advokat, VP Legal & Compliance i LINK Mobility Group.

Medredaktør er Trine Shil Kristiansen, Lovdata.

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

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

Redaktør for Finland er Viveca Still, senior ministerial adviser, legal affairs, at Ministry of Finance.

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

Juristen og AI

Utvecklingen inom det området som brukar benämnas artificiell intelligens (AI) är intensiv. På kort sikt gör den nuvarande hypen att det finns en betydande risk för besvikelser och bakslag, men på längre sikt råder det knappast någon tvekan om att samhällspåverkan kommer att bli kraftig.

Utvecklingen ställer krav på jurister på åtminstone tre sätt.

- **Det finns ett behov av att förstå tekniken och dess egenskaper.** Det är inte möjligt att tillämpa rättsregler, utforma avtal och utföra andra rättsliga oppgifter på ett korrekt sätt utan att förstå hur olika AI-tekniker fungerar och vilka särskilda risker de för med sig. När AI-tillämpningarna blir allestädes närvarande måste kretsen av jurister med dessa kunskaper breddas kraftigt. Utmaningen är att tekniken är komplex, utvecklas snabbt och kan implementeras på skilda sätt.
- **Fler jurister behöver vara in-satta i den rättsliga reglering som styr utvikling och användning av AI.** I takt med att AI-lösningar tas i bruk på allt fler områden krävs ökad kunskap om den relevanta rättsliga regleringen. I praktiken handlar det både om ny komplex specialreglering (t.ex. AI-förordningen) och om kunskap om hur generellt utformade rättsregler kan appliceras på AI. AI-juridiken måste gå från ett smalt specialistområde till ett område som många behärskar.



Daniel Westman

- **Jurister måste i första hand vara bra på att utföra de rättsliga arbeidsmoment som inte bättre utförs av AI-verktyg.** De juridiska AI-tjänster som finns idag är på många sätt imponerende, men for den som är ekspert på ett visst område är det ofta lätt att upptäcka fel og brister. Samtidig er vi bare i början av utviklingen og tekniken kommer fortsätta att förbättras og anpassas till rättsliga behov. Mycket tyder på att jurister i framtiden endast kommer att utföra arbeidsoppgifter som AI-verktyg inte utför bättre eller som av principella skäl kan anses kräva mänskligt utförande. Användning av AI är visserligen inget självändamål,

men det är inte heller befintliga arbetssätt – och faktiskt inte heller jurister.

De tre kraven hänger samman. Viktiga arbetsuppgift för jurister blir att ställa krav på utformningen av nya AI-verktyg och att bedöma deras arbetsresultat, något som förutsätter

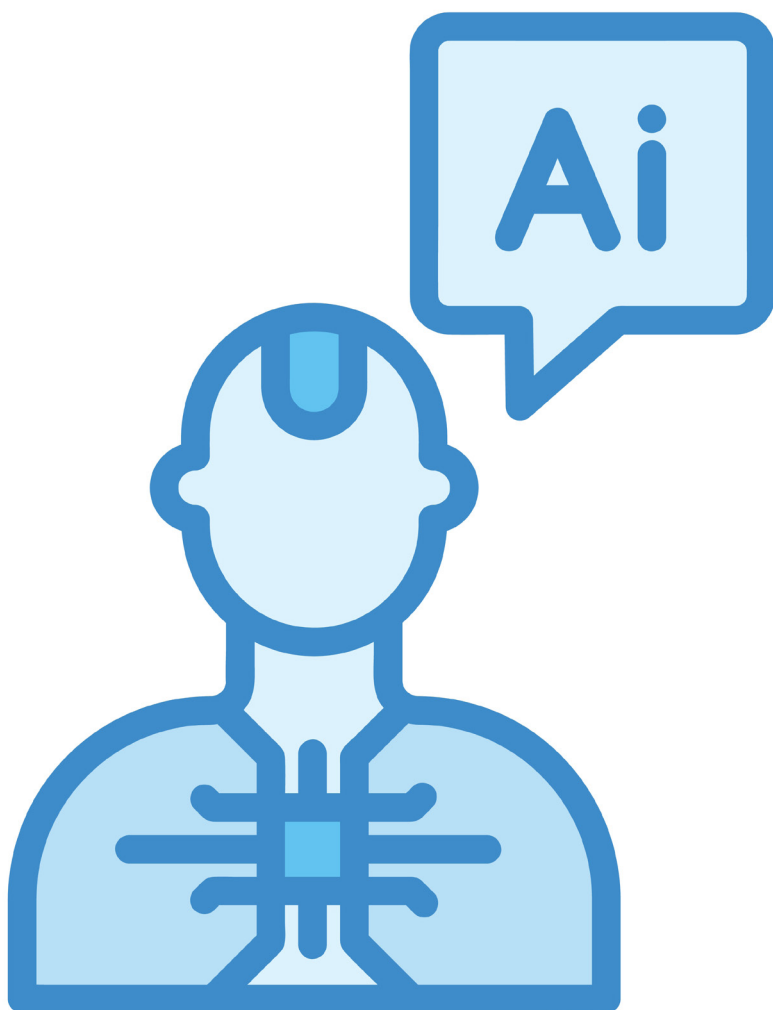
kunskap såväl om hur tekniken fungerar som om de rättsliga förutsättningarna för verktygens användning. Samtidigt kan AI-tekniken i sig bidra till att det blir lättare att förvärva nödvändig kunskap.

Det faktum att vi inte vet exakt hur genomgripande förändringarna kommer att bli är inte ett argument

för att vi ska vänta med att utbilda yrkesverksamma jurister och juriststudenter om AI-tekniken, AI-juridiken och det praktiska rättsliga arbetet med AI. Trycket på att tekniken ska komma till användning är redan idag stort och kompetensen behövs därför omgående. Utan en juristkår med relevanta kunskaper föreligger det både en risk för olaglig och olämplig AI-användning och att positiv användning begränsas i onödan. Exempelvis är det lätt att bli utlämnad till vad marknaden för tillfället erbjuder, vilket riskerar att leda till bristande rättslig kvalitet och rena rättsförluster.

Ny teknik förstås ofta initialt i ljuset av befintlig teknik och etablerade arbetssätt. Det är lätt att se möjligheterna att automatisera och på annat sätt effektivisera befintliga moment i arbetet. Men AI-tekniken har potential att leda till mer djupgående förändringar av samhället och mer specifikt av juridikens roll och funktionssätt. Exakt vad framtiden för med sig är svårt att säga, men helt klart är att det finns ett stort behov av jurister som aktivt kan vara med och påverka utvecklingen och kvalitetssäkra arbetet.

Daniel Westman



Illustrasjon: Colourbox.com

Digital Operational Resilience: A Guide for crypto-asset service providers under DORA and MiCA

Av Victoria Jakobsen

1. Introduction

1.1. The regulatory landscape

The increasing adoption and popularity of cryptocurrencies highlight the need for robust security measures and resilience – this is not merely an individual concern but becoming a matter of preserving trust and preventing systemic risks in the financial market as a whole.¹ As the technology advances in this field its increasingly important to have legislative measures who effectively captures the unique threat landscape for crypto-asset service providers, such as private key theft and smart contract vulnerabilities.

The European Union has recognized the need for stringent security measures in the financial sector through the implementation of Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA). While DORA set forth the most detailed legal framework for cybersecurity in the Union, it is not the only framework that applies to crypto asset service providers (CASP).

The implementation of Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA) highlights the critical role of DORA in ensuring digital operational resilience for CASPs, see article 68 (7). MiCA covers all crypto



Victoria Jakobsen

assets that are not already regulated by existing EU financial service regulation, such as E-money tokens, asset-referenced tokens, utility tokens and unbacked crypto-assets that doesn't qualify as financial instruments under MiFID II.

Note that because the scope of application for DORA and MiCA are different, it is important to do a case-by-case assessment of the applicable rules and regulations for the entity in question.

1.2. Aspects of difference between traditional financial entities and CASPs

CASPs enjoy several advantages that enable them to address both operational resilience and compliance in ways that traditional financial entities may struggle to replicate. A key advantage is their low technical debt. Most CASPs operate on modern, cloud-based infrastructure paired with blockchain technology. Generally speaking, this results in a lower technical debt than the

legacy systems that dominate traditional financial entities.

For example, the decentralized nature of many crypto architectures enables scalable and flexible solutions, such as decentralized identity management or automated risk monitoring tools. These solutions can improve resilience by enhancing security and ensuring that compliance requirements are met more efficiently.

” Note that because the scope of application for DORA and MiCA are different, it is important to do a case-by-case assessment of the applicable rules and regulations for the entity in question.

Another distinct advantage for CASPs is their ability to leverage automation and new technologies. The automation of tasks like monitoring, reporting, and auditing can help to reduce human error and increases the overall efficiency of compliance. This flexibility makes it easier for them to integrate tools like machine learning for anomaly detection, AI-based fraud prevention, and blockchain analytics. Additionally, tools that automatically audit smart contracts for vulnerabilities help prevent security flaws before the contracts are deployed.

¹ As an example Binance tried offering the Binance debit card offering european residents to convert and spend crypto currencies in online and physical stores. For various reasons the services closed in EEA in 2023 (Binance, 2022)

On the other hand, the need for transparency is greater because CASPs don't leverage the general trust that traditional financial entities have struggled to build over years. Incidents could therefore have a greater impact on the reputational damage of CASPs. Furthermore, decentralisation and innovation can also imply greater reliance on third parties and less capacity for reintegrating ICT services back into the CASPs internal environment. Meaning that while vendor security and third-party risk management also is a priority for traditional financial entities, it should be one of the top priorities for CASPs that heavily rely on outsourced ICT services.

2. Requirements under DORA

2.1. Introduction to DORA

MiCA article 68 (7) and (8) underscores the importance of a comprehensive risk management framework to safeguard ICT systems, focusing on reliance on third-party service providers, availability, authenticity, integrity and confidentiality. Nevertheless, MiCA must also be read in correlation with DORA, which provides a detailed description of such risk management frameworks.

DORA consists of four chapters of material requirements for the cybersecurity of financial entities. Chapter II gives an in-depth legal framework for ICT risk management frameworks, building on the principles of identification, protection, detection, response and recovery.² Chapter III gives detailed requirements on ICT-related incident management, classification and reporting. Chapter IV focuses on digital operational resilience testing and Chapter V covers ICT third party risk. All of which are important to have a holistic and comprehensive outlook on digital opera-

tional resilience for CASPs.

However, as previously mentioned, the unique nature of CASPs may result in different focuses, and different priorities than for the more traditional financial entities.

2.2 ICT risk management framework and proportionality

DORA mandates that financial entities need to develop and document comprehensive ICT security policies, procedures, protocols, and tools to protect information assets and ICT assets, see article 6 (1). Paragraph 2 of article 6 further elaborates that the ICT risk management framework needs content that is "necessary to duly and adequately protect all information asset and ICT assets...". The wording clearly nodding to a principle of proportionality as is highlighted in DORA art.4.

The specific material content of the ICT risk management framework is further elaborated in DORA as well as the several Commission Delegated regulations, also called regulatory technical standards (RTS) under the regulation.³

The RTS 2024/1774 on the ICT risk management framework stipulate that financial entities subject to DORA encompass a diverse array of sizes, structures, internal organizations, and levels of complexity, as highlighted in Recital 1.

Article 2 of the RTS 2024/1774 contains a detailed list of what the entities ICT risk management framework needs to achieve. The goals spanning from ensuring the security of networks in *litra a*, to

guaranteeing business continuity in *litra d*. By phrasing the goal of the ICT risk management framework like this, the regulator to some extent allows the entities a discretion in determining how to best achieve this. Especially for CASPs operating in the boundaries of the traditional financial sector this discretion is important to tailor an ICT risk management framework to their needs.

We can see the same nod to proportionality when RTS 2024/1774 uses known principles of information security such as "risk tolerance levels" and "residual risk". The RTS balances the need for visibility on these topics but doesn't specify the minimum tolerance level for the entities, see article 3. Still, RTS 2024/1774 contains several requirements regarding the responsibility and organisation of the ICT risk management framework, see article 2 (2).⁴

RTS 2024/1774 goes into detail when discussing specific policies and procedures for asset management in article 4 and 5. The balance of proportionality is further pushed by even elaborating on specific controls regarding encryption and cryptographic controls. While both asset management and encryption are key aspects to ensure availability and confidentiality, and it is understandable why the regulator chooses to emphasise these topics, it also affects the CASPs ability to determine and tailor the content of their own ICT management framework.

2.3 Connection with MiCA

On February 15 of 2025, RTS 2025/299 was introduced as a supplement to MiCA. Appropriately, it references Articles 11 and 12 of DORA in its opening paragraph. The RTS 2025/299 introduces fur-

² Building upon recognized frameworks such as NIST (Pascoe, 2024)

³ See especially Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework (RTS 2024/1774)

⁴ For example specific requirement regarding overarching strategy, formal approvals by management bodies, as well as responsibilities and consequences of staff.

ther obligations specifically aimed at ensuring the continuity and consistency in the delivery of crypto-asset services. While business continuity is emphasized in several clauses of DORA, including articles 11, 24, and 25, RTS 2025/299 provides additional, detailed specifications tailored specifically for CASPs.

RTS 2025/299 emphasizes the differences between traditional financial entities and entities operating in crypto assets, such as CASPs. Focusing again on business continuity and proportionality the goal of the RTS is clearly to ensure operational resilience in the services that CASPs provide. Not only do the RTS emphasize the business continuity plans for CASPs, but it also underscores the need for information distribution to clients and customers in the event of business disruptions involving permissionless distributed ledgers, see article 4 (2) and (3).

Additionally, there is a focus on continuous improvement, and CASPs must also perform periodic testing of their business continuity plans, note article 5 of the RTS 2025/299. For CASP, scenario based crypto-specific tests are perhaps even more important. Threats such as smart contract exploits, private key theft, and blockchain consensus attacks can all impact business continuity for CASPs in various ways. RTS 2025/299 also contain the requirement to document testing activity in writing and submitting it to the management, see article 5(3). Subsequently also making it subject for supervisory authorities review during audits.

3. Summary

While most financial entities encounter challenges in complying with DORA, crypto-asset service providers face these challenges somewhat differently given their



Illustrasjon: Colourbox.com

nature. Their challenges include DORAs integration with distributed ledger technologies, as well as scalability and proportionality of the regulation

DORA mandates the development of comprehensive ICT security policies and procedures, emphasizing principles like identification, protection, detection, response, and recovery. The regulation also highlights the importance of proportionality, allowing CASPs to tailor their ICT risk management frameworks to their specific needs. RTS 2024/1774 and RTS 2025/299 provide detailed requirements and additional specifications for CASPs, focusing on business continuity, periodic testing, and continuous improvement.

While it is noteworthy that the RTS 2025/299 focuses on business continuity in the face of permissionless distributed ledgers, it's important to emphasize that to succeed regarding business continuity

one should maintain a holistic approach to ICT risk management as a whole. Thus, ensuring that the overall ICT risk management framework can leverage and address unique the benefits and the risks that CASPs face.

Works Cited

- Binance. (2022, 05 27). *FAQ: An Overview of the Binance Card*. Opgehaald van Binance.com: <https://www.binance.com/en/support/faq/detail/7258c9d01cd04e58b4269ae5a86acb6d>
- Pascoe, C. . (2024). *The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Papers (CSWP)*. Gaithersburg, MD: National Institute of Standards and Technology. doi: <https://doi.org/10.6028/NIST.CSWP.29>

Victoria er utdannet jurist ved UiT og arbeider for tiden som Rådgiver ved KPMG i Brussel for deres Cyber & Privacy avdeling.

Can Database Rights Prohibit Training AI on Finnish Laws?

Av Otto Lindholm

Background:

Finlex is a public source of Finnish laws, but backed by a commercial database

Finlex is Finland's official legal information service – essentially a comprehensive online database of laws, regulations, and case law. It's operated by the Ministry of Justice and offered as a free public resource.

Edita, on the other hand, is a private legal publisher involved in maintaining and publishing Finlex materials.

In the past few years, as generative AI and particularly large language models have made their way into the general public's knowledge and use, a question has arisen about whether the Finnish government could use Finlex content to train AI, particularly to help the legislative branch in preparing laws.

This legal question came into the spotlight during a 2023 pilot project by Finland's Ministry of Transport and Communications. When the ministry began to explore the possibility of AI-assisted legislative drafting, they discovered that this would not be possible due to alleged restrictions placed by Edita, the maker of the database which provides the index and structure for Finlex.

A legally crucial question follows: Can a database maker exercise control over the database and its data such that the use of the data for the purposes of AI development could be prohibited?

It turns out, the extent and nature of legal control and ownership



Otto Lindholm

over data, and particularly the extent of rights that pertain to databases, are not well understood in the EU and Finland.

No Copyright in Laws or Decisions

First, it's crucial to clarify that the content of Finlex – Finnish laws, statutes, and official decisions – is not protected by copyright. Section 9 of the Finnish Copyright Act explicitly excludes such official materials from copyright protection. In Finland, as in many jurisdictions, you cannot claim copyright over the text of an Act of Parliament, decisions of official bodies, or a court judgment. These texts are outside of copyright protection by law because the law is public information, and everyone must be free to read and use it.

So, if the dispute were simply about feeding the texts of laws from Finlex to an AI, copyright law wouldn't pose a barrier.

However, what about the way Finlex organizes or presents that content? This is where database rights come in.

Sui Generis Database Rights

Finlex is essentially a database, a structured collection of legal documents. Even though the individual laws and decisions have no copyright, the database as a whole could be protected by a sui generis database right. Under Section 49 of the Finnish Copyright Act (implementing the EU Database Directive (96/9/EC)), a person or entity that has made a database with a substantial investment has the exclusive right to control the extraction or re-utilization of substantial parts of that database.

This right was originally introduced to protect investments in the compilation and structuring of vast amounts of data. But what is crucial is that the right is actually narrowly framed: the database maker can exercise control over the entirety of the database as a whole, or its "substantial parts". However, the right does not give the maker any control over the pieces of data in the database.

But if the Finnish government were to use the contents of the entire Finlex to train AI, surely that would amount to "substantial part"?

Most likely. But there's more to it in the case law.

The CV-Online Case: Introducing the "Adverse Effect" Test

This brings us to the CJEU's CV-Online Latvia v. Melons case (Case C-762/19).

In this case, a company (CV-Online) had a public database of job listings, and another company (Melons) ran a specialized search engine that indexed those listings and pro-

vided links to them. CV-Online sued, claiming that Melons was extracting and reusing substantial parts of its database without permission. The dispute made it to the European Court of Justice, which had to interpret the Database Directive – essentially clarifying what counts as prohibited “extraction” or “re-utilization” of a database.

While the Court agreed that Melons did use substantial portions of CV-Online’s database, it ended up concluding that this alone was not enough to prohibit CV-Online from running its search engine.

In fact, an “adverse effect on investment” test was introduced for database right infringement. The Court (echoing the Advocate General’s opinion) held that a database maker can only prevent extraction or reuse under the *sui generis* right *if the act in question undermines the investment that went into creating the database*. In other words, not every technical reuse is an infringement – it has to be something that poses a real risk to the database maker’s ability to recoup their investment (for example, by threatening their revenue streams or business model).

This “adverse effect” criterion is not explicitly written in the statute; it’s a pragmatic gloss by the Court. The rationale is to strike a balance: database rights shouldn’t stifle useful services and further innovation on the back of data if they don’t actually harm the database owner’s economic interests.

In CV-Online, the service provided by Melons was a job aggregator that linked back to the original site. The Court noted that CV-Online’s site was still the one doing the “heavy lifting” – users ultimately landed there, meaning CV-Online wasn’t losing out in a way that jeopardized its investment. The database right exists to prevent free-riding that cripples the incentive to invest. Rather, the right is not meant to grant absolute control over how others may use the database.

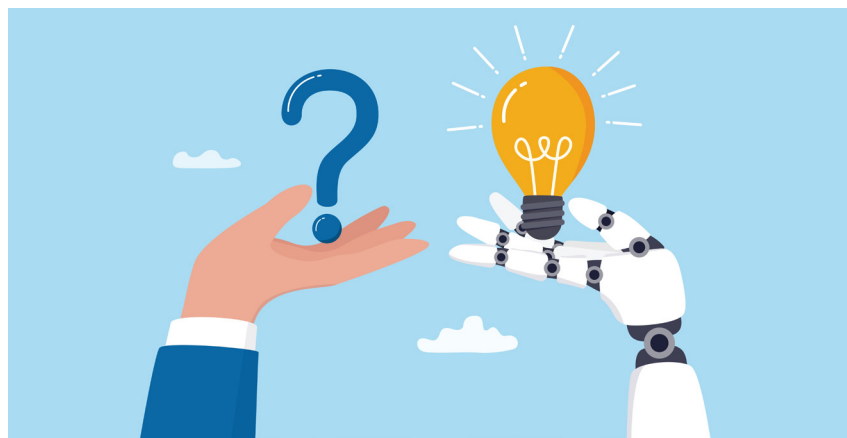


Illustration: Colourbox.com

This standard is critical when evaluating claims against AI developers or legal tech platforms that might train machine learning models on structured legal data.

So, Can Edita Prohibit AI Training on Finlex or not?

Applying the *CV-Online* ruling here, any argument that training an AI model on Finlex data constitutes unlawful re-use must meet the adverse effect standard. This seems like a high bar.

Finlex is not monetized. It’s publicly funded and free to access. Historically, Edita’s role, while important for the development of a functional service that is Finlex, was not based on a revenue model endangered by AI reuse. The original investment made in organizing Finlex was not made with an aim for Edita to invest in AI development. Therefore, it can be argued that using Finlex data to train AI cannot reasonably be said to “undermine” the original investment in the database.

Conclusion: Database Rights Cannot Justify Blocking AI Innovation

In early 2025, Finlex was updated, and the restrictions on the data use were removed. This change reflects both legal compliance and policy alignment: Finlex is now structurally and legally open by design. However, there is an argument to be

made that the restriction should not have been there to begin with.

” Database rights cannot be used to prohibit the training of AI, unless such reuse causes real economic harm to the rights holder.

The combined force of Finnish and EU law, along with judicial interpretation in *CV-Online*, points to a clear conclusion: database rights cannot be used to prohibit the training of AI, unless such reuse causes real economic harm to the rights holder.

By ruling on the CV-Online Latvia case, the European Court of Justice made a move towards favouring open data over proprietary in quite a fundamental manner, which has been largely ignored by the field.

It is up to the future to demonstrate whether this status quo of the law will become reality, or whether the case will be forgotten and stumped by companies and organizations not recognizing the potential for the use of available databases.

*Otto Lindholm, Partner,
Dottir Attorneys Ltd.*

Högsta domstolen sammanjämkar svenska mediegrundlagarna med dataskyddsförordningen

Av Martin Brinnen

Inledning

Högsta domstolen har i två ärenden den 25 februari 2025 tagit ställning till hur offentlighetsprincipen enligt 2 kap. tryckfrihetsförordningen (TF) ska sammanjämkas med dataskyddsförordningen vid utlämnande av brottnömsdomar från domstolarna till rättsdatabaser som omfattas av grundlagsskydd enligt yttrandefrihetsgrundlagen (YGL).

Högsta domstolens beslut (Å 3457-24 och Å 3169-24) innebär att de aktuella massuttagen av brottnömsdomar omfattas av s.k. dataskyddssekretess enligt 21 kap. 7 § offentlighets- och sekretesslagen, 2009:400 (OSL) men att brottnömsdomarna får lämnas ut med sekretessförbehåll som i korthet innebär att domarna inte får tillhandahållas eller göras sökbara för allmänheten eller betalande kunder.

” En troligen konsekvens av besluten är att de allmänt tillgängliga rättsdatabaser som används av journalister, jurister och för bakgrunds-kontroller inte längre kommer att kunna tillhandahållas i dess nuvarande form.

En troligen konsekvens av besluten är att de allmänt tillgängliga rättsdatabaser som används av journalister, jurister och för bakgrunds-



Martin Brinnen

kontroller inte längre kommer att kunna tillhandahållas i dess nuvarande form.

Det ena målet gällde nyhetsbyrån Siren, vars kärnverksamhet enligt beslutet består i att identifiera och samla in underlag för nyheter och att förmedla sådant underlag till andra massmedier. Eftersom Siren är en nyhetsbyrå omfattas den databas (siren.se) där bland annat brottnömsdomar tillhandahålls av grundlagsskydd enligt 1 kap. 4 § YGL.

Det andra målet gällde företaget Trobar AB som enligt beslutet tillhandahåller en rättsdatabas med domar, beslut, protokoll, dagboksblad, beslut om strafföreläggande och åtalsunderlåtelser. Handlingarna har hämtats ut från domstolar och myndigheter. Rättsdatabasen tillhandahålls företag och organisationer som ägnar sig åt bl.a. bakgrunds-kontroller, journalistik och forskning. Tjänsten innefattar även en möjlighet att få en avisering ifall ett person- eller organisationsnummer förekommer i nytillkomna hand-

lingar. Rättsdatabasen har ett utgivningsbevis och omfattas därmed av grundlagsskydd.

Bakgrund

Rättsdatabaser har i flera decennier med stöd av den grundlagsskyddade rätten till allmänna handlingar enligt 2 kap. TF begärt och fått ut brottnömsdomar från i stort sett samtliga svenska domstolar. Brottnömsdomarna har därefter tillhandahållits till allmänheten eller betalande kunder via internet. Databaserna har använts av bl.a. journalister för research och av företag, organisationer och myndigheter för bakgrunds-kontroller men även av jurister för rättsutredningar.

Utlämnandet från domstolarna har ansetts kunna ske eftersom domar som utgångspunkt är offentliga inklusive personuppgifter som framgår av domarna. Eventuell sekretess som har gällt under handläggningen av målet upphör i regel när domen publiceras. Brottnömsdomarna har därför lämnats ut av domstolarna även när det gällt massuttag. Därtill kommer att den efterföljande publiceringen av domarna i rättsdatabaserna omfattas av grundlagsskyddet enligt 1 kap. 4 § YGL, antingen för att tillhandahållaren av databasen är ett sådant massmedieföretag som driver annan grundlagsskyddad verksamhet eller för att tillhandahållaren har ansökt och erhållit utgivningsbevis för databasen. De svenska mediegrundlagarna har således ansetts omfatta både domstolarnas utlämnande och rättsdatabasernas publicering av brottnömsdomarna.

Den svenska lagstiftarens uppfattning har varit att TF och YGL (mediegrundlagarna) har företrädde framför EU-rätten inklusive dataskyddsförordningen. Denna tolkning har även lagts fast i 1 kap. 7 § första stycket dataskyddslagen där det framgår att dataskyddsförordning och dataskyddslagen inte ska tillämpas i den utsträckning det skulle strida mot TF eller YGL. I andra stycket görs undantag från huvuddelen av bestämmelserna i dataskyddsförordningen och dataskyddslagen för behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande. Bestämmelserna i 1 kap. 7 § dataskyddslagen stödjer sig på det utrymme som medlemsstaterna har enligt artiklarna 85 och 86 dataskyddsförordningen att sammanjämka skyddet för den personliga integriteten med yttrande- och informationsfriheten.

Det har därför inte ansetts varit aktuellt att tillämpa dataskyddsförordningen varken för behandlingen som består av domstolarnas utlämnande till grundlagsskyddade verksamheter eller för rättsdatabasernas tillhandahållande av databaserna. Under våren 2024 började emellertid flera domstolar ifrågasätta praxisen att lämna ut brottmålsdomar till rättsdatabaserna. Domstolarna menade bl.a. att brottmålsdomarna omfattas sekretess enligt 21 kap. 7 § OSL (här kallad för dataskyddsssekretess) och att dataskyddsförordningen måste ges företräde framför de svenska mediegrundlagarna.

Enligt bestämmelsen i 21 kap. 7 § OSL gäller sekretess för en personuppgift om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med dataskyddsförordningen, dataskyddslagen eller etikprovningsslagen. Enligt bestämmelsen ska således den utlämnande myndigheten ta hänsyn till vad som kan antas om den kommande behandlingen och dess karaktär. En bedömning behö-

ver, enligt förarbetena, göras endast om det finns konkreta omständigheter som indikerar att mottagaren kommer att behandla uppgifterna på ett sätt som strider mot dataskyddsregleringen, t.ex. att det är fråga om ett massuttag eller selekterade uttag. Någon fullständig bedömning av om behandlingen kommer att strida mot dataskyddsförordningen eller dataskyddslagen behöver inte göras (jfr prop. 2017/18:105 s. 135 f.).

Högsta domstolens bedömning

Högsta domstolen har i de två aktuella målen gjort samma bedömning av den rättsliga bakgrunden och beslutat om i stort sett likalydande sekretessförbehåll. Hänvisningar nedan gäller i första hand beslutet som gäller Siren.

Inledningsvis gör Högsta domstolen bedömningen att det ”får sägas ha varit” lagstiftarens avsikt att dataskyddsförordningen och dataskyddslagen över huvud taget inte ska tillämpas på det grundlagsskyddade området. Det innebär att förordningen inte inskränker myndigheters skyldigheter att lämna ut personuppgifter. Därav följer enligt domstolen att sekretess enligt 21 kap. 7 § OSL inte är tillämplig om mottagarens verksamhet omfattas av mediegrundlagarna. Det kan ju inte antas att mottagaren kommer att behandla de utlämnade personuppgifter i strid med dataskyddsförordningen eftersom förordningen inte ska tillämpas på mottagarens verksamhet, enligt 1 kap. 7 § dataskyddslagen (p. 35-37).

Högsta domstolen bedömer dock ”att det inte kan anses förenligt med unionsrätten att ha en ordning som innebär att brottmålsdomar i stor omfattning lämnas ut med följd att en betydande mängd personuppgifter rörande lagöverträdelser därefter kan behandlas i en databas och göras tillgängliga för andra. I princip finns då inte något annat skydd för integritetsintresset än det som kan ligga i ingripanden med stöd av mediegrundlagarna och brottsbalken. En sådan ordning under-

gräver närmast helt det skydd vid behandling av uppgifter om lagöverträdelser som dataskyddsförordningen syftar till att ge och kan inte anses innebära att det har fastställts lämpliga skyddsåtgärder för de registrerades rättigheter och friheter på det sätt som förutsätts enligt artikel 10 i dataskyddsförordningen. Bedömningen att detta inte är godtagbart gäller även i förhållande till behandling som sker för journalistiska ändamål eller andra ändamål som avses i artikel 85” (p. 42).

Mot den bakgrunden konstaterar Högsta domstolen att det inte är möjligt att förena den svenska regleringen med dataskyddsförordningen på det sätt som lagstiftaren får antas ha avsett (p. 43). Högsta domstolen finner dock att det finns ett utrymme att tolka 1 kap. 7 § första stycket dataskyddslagen så att bestämmelsen inte hindrar att dataskyddsförordningens krav beaktas vid tillämpningen av sekretessbestämmelsen i 21 kap. 7 § OSL även på det grundlagsskyddade området (p. 51).

Myndigheter ska därför enligt domstolen pröva sekretessfrågan enligt 21 kap. 7 § OSL ”utan att ta ställning till i vilken mån den svenska regleringen innebär att förordningen inte ska tillämpas i den verksamhet som bedrivs av den som har begärt att få ut uppgifterna.” Dataskyddsförordningen kan därvid ”närmast ses som en fristående måttstock för när sekretess råder för uppgifter som annars skulle ha varit offentliga” (p. 52).

Vad gäller utlämnande till verksamhet som omfattas av journalistiska ändamål (jfr artikel 85.2 dataskyddsförordningen) konstaterar Högsta domstolen att bestämmelsen i 1 kap. 7 § andra stycket dataskyddslagen inte rimligen kan ge ett mer långtgående undantag från dataskyddsförordningen än det undantag som avser det grundlagsskyddade området (p. 56). Även i sådana fall anser Högsta domstolen att myndigheter inte behöver ta ställning till om de undantagna artiklarna i dataskyddsförordningen

ska tillämpas vid behandling i mottagarens verksamhet.

Sammantaget finner således Högsta domstolen att 1 kap. 7 § dataskyddslagen bedömd i ljuset av unionsrätten inte hindrar att dataskyddsförordningen beaktas vid tillämpningen av sekretessbestämmelsen i 21 kap. 7 § OSL (p. 58).

Högsta domstolen konstatera därefter att både Siren och Trobar har begärt att få ut ett stort antal brottmålsdomar m.m. med uppgifter om lagöverträdelse och andra uppgifter av känslig natur. Vidare beaktar domstolen att företagen återkommande har begärt ut handlingar på motsvarande sätt. Mot denna bakgrund och den omfattande behandling av personuppgifter som sker hos företagen kan det, enligt Högsta domstolen, antas att personuppgifter som finns i de begärda handlingar kommer att behandlas på ett sätt som är oförenligt med artikel 10 dataskyddsförordningen. Högsta domstolen anser därför att sekretess gäller för de personuppgifter som finns i de begärda handlingarna (p. 60). Handlingarna kan dock lämnas ut med sekretessförbehåll.

Högsta domstolen ansåg att en rimlig balans mellan integritetsintresset och de journalistiska ändamålen kan uppnås genom ett sekretessförbehåll som tar sikte på att förhindra att handlingar tillhandahålls eller görs sökbara för andra än bolagen själva. Förbehållet ska dock inte förhindra att personuppgifterna i handlingar används i t.ex. nyhetstexter eller nyhetsunderlag som Siren eller Trobar producerar (p. 65).

Högsta domstolens beslutade sekretessförbehåll innebär i korthet att de begärda handlingarna får lämnas ut men med förbehållet att handlingarna inte får tillhandahållas till, eller göras för sökbara för, allmänheten eller betalande kunder om de därigenom får del av personnamn, personnummer eller adresser för enskilda personer. Handlingarna

får inte heller användas för att avisera allmänheten eller betalande kunder om en viss person förekommer i handlingarna.

Av de sju justitieråd som deltog i avgörandena var tre skiljaktiga. Två av de skiljaktiga justitieråden ansåg att det inte var i strid med unionsrätten att låta grundlagarna gälla på det sättet som lagstiftaren avsett vad gäller utlämnande till Siren. Däremot ansåg de skiljaktiga justitieråden att det fanns anledning att bortse från grundlagsskyddet för Trobars databas. Det tredje skiljaktiga justitierådet ansåg att det inte var möjligt att med ett sekretessförhåll undanröja att uppgifterna kommer att behandlas i strid med dataskyddsförordningen.

Högsta domstolen utgår från ett antagande om lagstiftarens syfte

I de båda målen har Högsta domstolen för första gången bedömt konflikten mellan mediegrundlagarna och dataskyddslagstiftningen – en problematik som har gäckat rättstillämparen under flera decennier. Men det är tveksamt om det verkligen har funnits ett sådan konflikt i de aktuella målen dvs. frågan om mediegrundlagarna förhindrar tillämpningen av bestämmelsen om s.k. dataskyddssekretess när mottagarens verksamhet omfattas av mediegrundlagarnas tillämpningsområde.

Enligt ordalydelsen i 1 kap. 7 § dataskyddslagen framgår, såsom också Högsta domstolen konstaterar (p. 48), att dataskyddsförordningen får vika först när det råder en konflikt mellan förordningen och mediegrundlagarna. HD bedömer dock aldrig på vilket sätt tillämpningen av dataskyddsförordningen kommer i konflikt med mediegrundlagarna.

I stället utgår Högsta domstolens bedömningar i de båda målen från ett antagande om lagstiftarens avsikt med bestämmelsen i 1 kap. 7 § dataskyddslagen. Högsta domstolen uttalar således att lagstiftarens syfte

med bestämmelsen i 1 kap. 7 § dataskyddslagen ”får sägas ha varit” att dataskyddsförordningen och dataskyddslagen över huvud taget inte ska tillämpas på det grundlagsskyddade området (p. 34-35). Något stöd för ett sådant antagande tycks dock inte gå att finna i förarbetena.

Antagandet om lagstiftarens avsikt bygger troligen på en missuppfattning

Högsta domstolens antagande om lagstiftarens avsikt avspeglar den ordning som har etablerats bland domstolarna om grundlagarnas företräde vid utlämnande till grundlagsskyddade medier. Bakgrunden är troligen den tolkning som etablerades med anledning av den tidigare lydelse av 21 kap. 7 § OSL (och dess föregångare i 7 kap. 16 § sekretesslagen, 1980:100) och den diskussion som tidigare fördes om bestämmelsen om dataskyddssekretess innefattade en bedömning av myndigheternas behandling av personuppgifter inför utlämnandet och inte enbart vad som kunde antas om mottagarens behandling av personuppgifter (se kommentar till 21 kap. 7 § OSL i Sören Öman, Kommentarer till dataskyddsförordningen (GDPR) m.m. JUNO version 3).

När lagstiftaren har uttalat sig i denna fråga har uppfattningen varit att grundlagarna ska ha företräde och att dataskyddsregleringen inte får begränsa myndigheternas skyldigheter att lämna ut allmänna handlingar enligt 2 kap. TF. Denna inställning kom också till uttryck i 8 § personuppgiftslagen där det angavs att lagen inte ska tillämpas i den utsträckning det skulle ”inskränka en myndighets skyldighet” enligt 2 kap. TF. Bestämmelsen fick som bekant en annan förenklad lydelse i 1 kap. 7 § dataskyddslagen. I sammanhanget bör noteras att myndigheterna endast har skyldighet att lämna ut allmänna handlingar på papper (enligt det s.k. utskriftsundantaget i 2 kap. 16 § TF) och att när utlämnande frivilligt görs elek-

troniskt gäller dataskyddsförordningen även för myndigheternas behandling (se den nämnda kommentaren av Öman).

Lagstiftarens avsikt har således varit att dataskyddsförordningen inte ska påverka myndigheternas i grundlagen fastställda skyldighet att lämna ut personuppgifter. Data-skyddsförordningen ska därför inte tillämpas på myndigheternas behandling av personuppgifter vid utlämnande av allmänna handlingar. Detta ställningstagande ska inte sammanblandas med dataskyddssekretess som gäller bedömning av mottagarens behandling av personuppgifter. Mot den bakgrunden och med anledning av att den senare frågan aldrig tycks ha varit föremål för lagstiftarens bedömning framstår det som svårt att tala om lagstiftarens avsikt på det sättet som Högsta domstolen gör.

Finns det någon konflikt med mediegrundlagarna?

Bestämmelsen om dataskyddssekretess innebär som nämnts att sekretess gäller för personuppgift om det kan antas att personuppgiften kommer att hanteras i strid med dataskyddsförordningen efter utlämnandet. Den uppfattning som har etablerats har varit att eftersom mediegrundlagarna inte gäller på det grundlagsskyddade området kan således behandling som utförs av grundlagsskyddade verksamheter aldrig komma i konflikt med dataskyddsförordningen. Denna ordning bygger, som nämnts ovan, troligen på en missuppfattning.

Mediegrundlagarna är visserligen avsedda att vara exklusiva inom sina tillämpningsområden men för att grundlagsskyddet ska aktiveras krävs att en åtgärd från det offentliga kommer i konflikt med någon av de grundläggande principerna i grundlagarna såsom censurförbudet, förbud mot hindrande åtgärder, exklusivitetprincipen, meddelar- och anskaffarfriheten. Det framgår bl.a. av bestämmelsen i 1 kap. 7 § data-

skyddslagen där det anges att dataskyddsförordningen och dataskyddslagen inte ska tillämpas ”i den utsträckning” som det skulle strida mot TF eller YGL. Att det ska föreligga en konflikt mellan regelverken är något som även HD konstaterar (p. 48). HD anger dock aldrig vari denna konflikt består.

Det är således inte tillräckligt att en verksamhet omfattas av mediegrundlagarnas tillämpningsområde. Det krävs en åtgärd som från det offentliga som kommer i konflikt med de grundläggande principerna. Den åtgärd som ska bedömas i de aktuella målen är de sekretessförbehåll som domstolarna har beslutat. Frågan som ska ställas är således på vilket sätt denna åtgärd strider med någon av de grundläggande principerna i TF och YGL.

Inledningsvis kan konstateras att tillämpningen av sekretessbestämmelser inte kan vara i strid med 2 kap. TF eftersom allmänhetens tillgång till allmänna handlingar får begränsas med hänsyn till bl.a. skyddet för enskildas personliga eller ekonomiska förhållanden. Detta konstaterar även Högsta domstolen (p. 49). Ett sekretessförbehåll skulle möjligen kunna betraktas som en form av hindrande åtgärd eller ingripande i strid med exklusivitetsprincipen men mycket talar för att förbud mot hindrande åtgärder och övriga principer inte är avsedda att tillämpas vid utlämnande av allmänna handlingar vid sidan av sekretessbestämmelserna. En annan tolkning skulle innebära att all sekretess vid utlämnande till grundlagsskyddade medier skulle strida mot grundlagarna.

Mycket talar därför för att Högsta domstolens bedömning bygger på en missuppfattning om lagstiftarens avsikt och att någon konflikt mellan mediegrundlagarna och dataskyddsförordningen inte finns i de aktuella målen. Det är förtur dock inte prejudikatvärdet av Högsta domstolens bedömning när domstolen bedömer att dataskyddsse-

kreteess kan tillämpas utan hinder av mediegrundlagarna (p. 52).

Varför utgör dataskyddsförordningen endast en ”fristående måttstock”?

Det är något oklart vad som är skälet till att Högsta domstolen anger att dataskyddsförordningen ska användas som en ”fristående måttstock” vid bedömning av sekretess enligt 21 kap. 7 § OSL i stället för att tillämpas direkt. En möjlig förklaring är att det är ett sätt att ge ett visst utrymme för att beakta att mottagarens verksamhet omfattas av grundlagsskydd och därmed använda det utrymme för nationell sammanjämkning som artikel 85.1 dataskyddsförordningen ger. Att någon fullständig bedömning av mottagarens verksamhet inte ska göras framgår redan av äldre förarbeten, vilket även nämns i Högsta domstolens beslut (p. 14).

Högsta domstolens tolkning av undantag för journalistiska ändamål är svårförståelig

Utöver bedömningen att undantaget i 1 kap. 7 § första stycket dataskyddslagen och artikel 85.1 inte medger utlämnande till grundlagsskyddade verksamheter gör Högsta domstolen bedömningen att undantaget för journalistiska ändamål enligt 1 kap. 7 § andra stycket och artikel 85.2 inte rimligen kan göras mer långtgående än undantaget för grundlagsskyddad verksamhet (p. 56). Denna tolkning framstår som svår att förstå; i vart fall utifrån ett unionsrättsligt perspektiv.

I Satakunna-målet (C-73/07) till vilket Högsta domstolen hänvisar till i slutet (p. 22), konstaterade EU-domstolen att även behandling av personuppgifter (taxeringsuppgifter) som har samlats in från offentliga handlingar hos skattemyndigheter och som i oförändrad form tillhandahålls under kommersiella förhållanden i en databas till allmänheten, kan utgöra behandling av journalistiska ändamål. Mot den

bakgrunden är det inte uteslutet att tillhandahållande av offentliga handlingar kan omfattas av undantaget för journalistiska ändamål i artikel 85.2 dataskyddsförordningen, t.ex. vidareförmedling av enstaka brottnålsdomar till andra medie-företag.

Förhållandet mellan bestämmelserna i artikel 85.1 och 85.2 är inte helt klar. Mycket talar dock för att artikel 85.2 avser den särskilt skyddsvärda yttrande- och informationsfriheten för vilken vissa minimikrav uppställs genom krav på undantag i nationell lagstiftning från dataskyddsförordningen. I sådana fall är Högsta domstolens tolkning än mer svårörförståelig. Se min artikel ”Utgivningsbevisen och de svenska mediegrundlagarna utmanas” i SvJT 2024 s. 287 och det kommandet avgörandet från EU-domstolen i det s.k. Lexbase-målet (C-199/24).

Slutet för rättsdatabaserna?

Högsta domstolen har genom de aktuella besluten, åtminstone delvis, hanterat den konflikt mellan svenska

mediegrundlagarna och EU:s dataskyddsreglering som har varit känd sedan flera decennier. Högsta domstolens bedömning att den ordning som har etablerats med stöd av mediegrundlagarna – som innebär att privata rättsdatabaser med omfattande mängder brottnålsdomar m.m. från domstolarna tillhandahålls allmänheten – innebär stora integritetsrisker och inte är förenlig med unionsrätten, framstår som obestridlig.

Även om ett utlämnande till verksamheter som omfattas av grundlagsskydd eller av undantaget för journalistiska ändamål eller av andra skäl är förenlig med dataskyddsförordningens materiella reglering, kan vara godtagbar när det gäller enstaka brottnålsdomar lär det vara svårt, troligen uteslutet, att finna stöd i dataskyddsförordningen för utlämnande till en privat aktör som regelbundet begär ut brottnålshandlingar och med hjälp av dessa bygger upp sådana omfattande rättsdatabaser som i de aktuella målen. Inte ens medie företag torde ha stöd i unionsrätten för att bygga

upp sådana obegränsade databaser i sin journalistiska verksamhet.

Det återstår att se om utformningen av de av Högsta domstolen beslutade sekretessförbehållen får avsedd effekt för integritetsskyddet. Det är dock troligen inte det sista avgörande i förhållandet mellan integritetsintresset och mediegrundlagarna. Det kommande avgörandet från EU-domstolen i det s.k. Lexbase-målet (C-199/24) och de svenska domstolarnas bedömningar med anledning av EU-domstolens avgörande kommer att få stor betydelse.

Det ska också noteras att journalistik inte är det enda berättigade intresset som kan motivera behandling av brottnålsdomar. Behovet av att kontrollera brottnålsdomar för bakgrundskontroller växer snabbt. Det är dock lämpligt att detta behov regleras och tillgodoses på annat sätt än utnyttjande av offentlighetsprincipen i 2 kap. TF.

Martin Brinnen är fristående juridisk rådgivare som samarbetar med advokatfirman Kahn Pedersen.



Illustrasjon: Colourbox.com

Etterretningstjenestens nye «overvåkningshjemler» – et svekket kommunikasjonsvern?

Av Annelin Sødal

Innledning

I 2020 vedtok Stortinget ny lov om Etterretningstjenesten (e-loven).¹ Loven gir adgang for Etterretningstjenesten («E-tjenesten») til såkalt tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon (heretter i denne artikkelen bare kalt «TI»), på folkemunne bedre kjent som «digitalt grenseforsvar» eller «digital masseovervåkning».

TI er en moderne metode for innhenting av etterretningsinformasjon, som på nærmere vilkår gir E-tjenesten tilgang til «masselagring (såkalt bulklagring) av metadata om elektronisk kommunikasjon som passerer den norske landegrensen».² Det innebærer at E-tjenesten kan bruke TI til å få innsyn i store mengder kommunikasjonsdata mellom norske og utenlandske borgere. På nærmere vilkår kan E-tjenesten ta i bruk bulklagrede data til målsøking, målrettet innhenting av innholdsdata og videre analyse og behandling av data for etterretningsformål.³ Formålet med TI er å modernisere E-tjenestens metoder for utenlandsetterretning, i lys av nasjonale sikkerhetsinteresser i dagens digitale trusselbilde, jf. e-loven § 1-1.

Selv om formålet om utenlandsetterretning er legitimt, kan TI innebære alvorlige inngrep i personvern, kommunikasjonsvern og pres-



Annelin Sødal

sens ytringsfrihet (kildevern). Årsaken er at verktøyet innhenter og lagrer store mengder norsk innenlands elektronisk kommunikasjon. Den Europeiske menneskerettighetsdomstol (EMD), som har vurdert lignende systemer i flere naboland, har treffende beskrevet bulklagring for sikkerhetsformål som et dilemma hvor «*a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it.*»⁴

” Selv om formålet om utenlandsetterretning er legitimt, kan TI innebære alvorlige inngrep i personvern, kommunikasjonsvern og pressens ytringsfrihet (kildevern).

Som følge av konsekvensene av TI har lovendringen vekket reaksjoner fra flere hold. Stiftelsen Tinius og Varden-redaktør Tom Erik Thorsen, anla i mars 2024 søksmål mot staten med påstand om at staten er uberettiget til å innhente, lagre og behandle elektronisk kommunikasjon og begrunnet dette med at lovreglene var i strid med grunnleggende rettigheter etter Grunnloven, EMK og EØS-retten. Store deler av mediebransjen har engasjert seg som partshjelpere. Saken ble behandlet i desember 2024, og Oslo Tingrett avsa dom i mars 2025. Stiftelsen fikk ikke medhold, og har nylig anket avgjørelsen til lagmannsretten.

Artikkelen tar først for seg tilretteleggingsplikten innhold, hvem som er pliktsubjekter etter lovverket og konsekvenser for aktørene som rammes. Deretter gis en overordnet oversikt over konsekvensene for enkeltindividers personvern, kommunikasjonsvern og ytringsfrihet (kildevern). Avslutningsvis kommenteres Oslo Tingretts avgjørelse i søksmålet mot staten.

Hvilke konsekvenser har TI for aktører som pålegges tilretteleggingsplikt?

Innhenting av kommunikasjonsdata gjennom TI skjer ved at ekomtilbydere pålegges en plikt til å speile og tilgjengeliggjøre utvalgte kommunikasjonsstrømmer for E-tjenesten, jf. e-loven § 7-2. Innhenting og lagring av kommunikasjonsdataene er en form for midtpunktinnhenting, det vil si innhenting av kommunikasjon

1 Lov 19. juni 2020 nr. 77 om Etterretningstjenesten (etterretningstjenesteloven). Loven ble endelig vedtatt, med noen endringer, i 2023.

2 Prop. 92 L (2022–2023) s. 22.

3 Prop. 80 L (2019–2020) s. 92.

4 Big Brother Watch m.fl. mot Storbritannia [GC] avsnitt 339.

i transitt mellom to endepunkter.⁵ TI skiller seg fra annen midtpunktinnhenting ved at datainnhenting er avhengig av tilrettelegging fra ekomtilbydere som E-tjenesten utpeker. Det betyr at gjennom e-lovens nye tilretteleggingsplikt kan E-tjenesten pålegge ekomtilbydere å tilrettelegge for at utvalgte kommunikasjonsstrømmer som ekomtilbyrder kontrollerer skal tilgjengeliggjøres for E-tjenestens speiling. Tilretteleggingsplikten kan i tillegg innebære å gjøre data tilgjengelig for utvalg, filtrering, testing, innhenting, lagring og søk, jf. § 7-2. Tilrettelegging kan blant annet skje på de ulike måtene § 7-2 angir, for eksempel ved å gi informasjon om dataene, tillate at E-tjenesten installerer teknisk utstyr for speilingen, bidra til teknisk drift og vedlikehold av TI og sikre at dataene ikke er underlagt kryptering som tilbyrder kontrollerer. For eksempel kan E-tjenesten pålegge Telenor å tilgjengeliggjøre kabler til utlandet ved å tillate at E-tjenesten installerer utstyr for speiling av transporterte kommunikasjonssignaler i sanntid. Listen i § 7-2 over medvirkningsplikter er ikke uttømmende, jf. ordlyden «blant annet». Rekkevidden av tilretteleggingsplikten er dermed vidt angitt og gir potensielt E-tjenesten en inngripende adgang til store mengder data hos tilretteleggeren og en tilsvarende nokså ubegrenset plikt for tilretteleggere til å bistå i E-tjenestens datainnhenting.

Pliktsubjekter etter regelen om tilrettelegging er tilbydere som omfattes av ekomloven § 1-5 og tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten.⁶ Det betyr at tilretteleggingsplikt kan pålegges tradisjonelle ekomtilbydere og tilbydere av kommunikasjonstjenester så vel som tilbydere av internettbaserte over the top-tjenester

(OTT) for kommunikasjon. Det vil si alt fra leverandører av telefoni og nett til sosiale medier og meldingsapplikasjoner. Typiske eksempler på tilbydere er Telenor, Snapchat og Messenger (Meta/Facebook). Også andre virksomheter som tilbyr digitale kommunikasjonstjenester er omfattet, og regelen skiller ikke mellom enveis- og toveiskommunikasjon. Det betyr at ordlyden ikke hindrer E-tjenesten fra å be om tilrettelegging fra andre aktører som via relevante nett leverer plattformer for digitale ytringer, for eksempel digitale fora eller nettaviser med digitale kommentarfelt. Slik regelen er utformet, er det grunn til å tro at tilretteleggingsplikten vil kunne ramme bredt.

Tilretteleggingsplikt utløses gjennom pålegg fra E-tjenesten i tråd med prosedyrene gitt i § 7-3. For det første kan tilretteleggingsplikt bare brukes når det er nødvendig for å etablere et informasjonsgrunnlag for etterretningsformål. For det andre skal pålegg om tilrettelegging gis av sjefen for E-tjenesten, men bare etter tillatelse fra retten. Det betyr i praksis at E-tjenesten må innhente forhåndstillatelse fra retten for å pålegge tilretteleggingsplikt etter § 7-2. Kravet om rettens tillatelse innebærer at tilretteleggingsplikt i ethvert tilfelle er underlagt forutgående domstolskontroll av om lovens vilkår for datainngrep er oppfylt. Det betyr at retten skal foreta en konkret vurdering av enhver forespørsel fra E-tjenesten om å innhente data fra en tilrettelegger, være seg bulklagring av metadata, målsøking i rådata, målrettet innhenting av innholdsdata, eller bruk av data til nærmere analyse. Denne domstolskontrollen utgjør en viktig rettssikkerhetsgaranti for ekomtilbydere og andre aktører som rammes av plikten.

Brudd på pålegg om tilrettelegging etter § 7-3 kan medføre straff etter § 11-8, for eksempel i form av foretaksstraff etter straffeloven §§ 27 og 28. Ekomtilbydere kan ikke

inngi innsigelse ved avgjørelser om tilretteleggingsplikt, da beslutning om tilrettelegging avgjøres bak lukkede dører for retten (§ 8-3) og uten at den som avgjørelsen berører får mulighet til å uttale seg (§ 8-1). Deres ekomtilbyder ønsker å angripe pålegg om tilrettelegging, er alternativet å benytte seg av klageadgangen etter § 11-7. Klage behandles av EOS-utvalget, som er E-tjenestens uavhengige kontrollorgan. Klageadgangen etter § 11-7 gjelder for «enhver». I praksis er det imidlertid vanskelig å se for seg at andre enn aktører som er direkte adressat for vedtak om tilrettelegging har reell mulighet til å benytte seg av klageadgangen. Faktiske eiere av kommunikasjonsdata som innhentes gjennom tilrettelegging, herunder brukere av kommunikasjonstjenestene (deg og meg), informeres ikke om at våre kommunikasjonsdata havner i E-tjenestens besittelse.

Hvilke konsekvenser har tilretteleggingsplikt for personvern, kommunikasjonsvern og pressens ytringsfrihet (kildevern)?

Formålet med E-tjenestens datainnsamling er utenlandsetterretning, og E-tjenesten skal som hovedregel ikke innhente data om norske borgere, jf. e-loven § 4-1. Ved bulkinnhenting gjennom TI, skal E-tjenesten søke å hindre å lagre data om kommunikasjon mellom personer i Norge, jf. § 7-6. All innhenting, lagring og videre behandling av data må dessuten oppfylle grunnvilkår i lovens kapittel 5, deriblant krav om forholdsmessighet, jf. § 5-4. Pålegg om tilrettelegging, målrettet innhenting, målsøking og analyse/behandling av data skal i alle tilfeller, som nevnt, forhåndsgodkjennes av en domstol, jf. § 8-1.

Et problem med TI, og bakgrunnen for søksmålet mot staten, er at det norske elektroniske kommunikasjonsnett i stor grad er tilknyttet servere/databaser i utlandet. De

⁵ Prop. 80 L (2019–2020) s. 103.

⁶ E-loven § 7-2, se nærmere i Prop. 80 L (2019–2020) s. 214

fleste kommunikasjonskanaler nordmenn bruker i det daglige, passerer dermed landegrensen som følge av infrastrukturens oppbygning. Selv om E-tjenestens datainnsamling er underlagt lovens begrensninger og kontrollmekanismer, er det alminnelig anerkjent at det ikke er mulig med dagens teknologi å hindre lagring av store mengder innenlands kommunikasjon.⁷

I tillegg til at ekomtilbydere har tilretteleggingsplikt, vil TI gjennom speiling og tilrettelegging av kommunikasjonsdata innebære omfattende innsamling av dataene til mennesker som kommuniserer med hverandre i det daglige, som medfører inngrep i berørte individers kommunikasjon.

Bulkinnhenting og -lagring av kommunikasjonsdata utgjør for det første inngrep i retten til privatliv, herunder personvern og kommunikasjonsvern. Det innebærer at alle personer i Norge som kommuniserer via tradisjonelle eller digitale kommunikasjonskanaler, er utsatt for en uoverskuelig risiko for E-tjenestens innsyn i personlig kommunikasjonsdata. For eksempel vil allerede bulklagring av metadata om en person kunne si noe om personens adresse, bevegelse eller handlingsmønster.

For det andre innebærer TI inngrep i pressens ytringsfrihet, herunder kilders rett til å forbli anonyme i møte med journalister (kildevern). I prinsippet kan hvem som helst være en journalistisk kilde, slik at kildevern henger tett sammen med personvern. Kildevernets begrunnelse har bakgrunn i samfunnshensyn; EMD har gjentatte ganger beskrevet kildevern som en hjørnestein for demokratiet og en åpen, opplyst offentlig debatt.⁸ Av den grunn skal det være en høy terskel

for inngrep i kildevernet.⁹ Uten et sterkt kildevern vil viktige bidrag til det offentlige ordskiftet kunne gå tapt, fordi kilder vegrer seg for å kommunisere med pressen. Innføringen av et system som TI vil i seg selv medføre risiko for at individer blir mer tilbakeholdne enn før med å gi informasjon til pressen over digitale plattformer – en såkalt nedkjølingseffekt. Det betyr at TI på lengre sikt vil kunne få negative konsekvenser for bidrag til den offentlige debatt, for eksempel i form av redusert kildetilfang hos medi-
evirksomheter og andre aktører som besitter fortrolig kommunikasjonsdata.

Inngrep gjennom TI kan i praksis være mange og ulikartede, alt etter hva E-tjenestens ønsker å foreta seg, fra bulklagring av metadata til målsøking, målrettet innhenting og eventuelt behandling/analyse av etterretningsrelevante data. Befatning med både innholdsdata og metadata kan anses som inngrep.¹⁰ For eksempel vil bulkinnhenting av metadata kunne gi informasjon om individers geolokasjon, mens målrettet innhenting av innholdsdata kan gi tilgang til fortrolig tekstinnhold i en chat. Sistnevnte er mer inngripende enn førstnevnte, men begge representerer like fullt inngrepsituasjoner. I mange tilfeller vil kombinasjonen av disse kunne gi omfattende informasjon om et individs bevegelser eller handlingsmønstre. TI kan forklares som en trinnvis prosess, hvor graden av inngrep i individets rettigheter øker etter hvert som prosessen skrider frem.¹¹

Retten til personvern, fortrolig kommunikasjon og pressens kildevern er grunnleggende rettigheter beskyttet under Grunnloven § 102 og § 100, EMK Artikkel 8 og 10 og EUs kommunikasjonsvern direktiv.

Retten til privatliv og kildevern etter Grunnloven henger nært sammen, og Grunnloven må tolkes i lys av de parallelle folkerettslige reglene. Lignende systemer som TI har vært innført i andre land og vært gjenstand for prøving i internasjonale domstoler. EMD og EU-domstolen har i disse sakene anerkjent på prinsipielt grunnlag at statlig bulkinnhenting av kommunikasjonsdata i seg selv ikke er i strid med hhv. EMK og EUs kommunikasjonsversdirektiv.¹² Men på grunn av den risiko et statlig system for bulkinnhenting og -lagring representerer, oppstiller EMD og EU-domstolen strenge materielle og prosessuelle skranke for myndighetenes befatning med vernet kommunikasjon. Dersom regelverket som skal beskytte mot inngrep inneholder en eller flere svakheter, viser praksis at en totalbedømmelse av regelverket vil kunne resultere i at bulkagringsregimet utgjør et ulovlig inngrep i berørte rettigheter. Avgjørende er om regelverket som tillater bulklagring samlet angir tilstrekkelige garantier for å hindre misbruk. Nettopp dette var derfor sentralt da Oslo Tingrett behandlet søksmålet mot staten i desember 2024.

Oslo Tingrett mener E-tjenestens «overvåkningshjemer» er lovlige

Oslo Tingrett avsa 26. mars 2025 avgjørelse i søksmålet mot staten om lovligheten av E-tjenestens nye regler om TI. Oslo tingretts konklusjon var at reglene om TI er i samsvar med de krav som oppstilles for ivaretagelse av berørte rettigheter etter Grunnloven § 102, EMK Artikkel 8 og 10 og EUs kommunikasjonsvern direktiv. Avgjørelsen er på 67 sider og er tilgjengelig i sin helhet *her*. Dommen er ikke rettskraft-

7 Dette ble også lagt til grunn av Oslo Tingrett i 24-038001TVI-TOSL/04 på s. 7.

8 Se for eksempel Big Brother Watch mot Storbritannia [GC] avsnitt 442.

9 Se for eksempel Goodwin mot Storbritannia [GC] avsnitt 39–40.

10 Prop. 80 L (2019–2020) s. 96.

11 Big Brother Watch mot Storbritannia [GC] avsnitt 325.

12 Se for eksempel Big Brother Watch mot Storbritannia [GC] avsnitt 322–323 og de forente sakene C-511/18, C-512/18 og C-520 (Quadrature du Net).

tig. Saksøker innga anke over lovanvendelsen mandag 5. mai 2025.

Det faller utenfor artikkelens rammer å gjennomgå avgjørelsen i sin helhet. Gjennomgangen i det videre er derfor begrenset til en overordnet kommentar til rettens vurderinger av TI i lys av Grunnloven og EMK, som er regelsettet som får størst fokus i dommen. Jeg vil også benytte anledningen til å påpeke noen svakheter ved avgjørelsen.

Sentralt ved vurderingen etter EMK er om e-loven inneholder tilstrekkelige rettsikkerhetsgarantier («end-to-end safeguards») for å sikre berørte rettigheter og hindre misbruk, blant annet klart definerte rammer for innhenting, formålsbegrensning, domstolskontroll og etterfølgende kontroll. I denne vurderingen tar retten utgangspunkt i 8 forhåndsdefinerte kriterier som EMD har oppstilt for å vurdere om nasjonal lovgivning fremstår betryggende ut fra en samlet vurdering («global assessment»)¹³. Det er imidlertid bare fem av momentene som gis en nærmere vurdering. Begrunnelsen er at retten legger til grunn at det ikke er innsigelser fra saksøker mot de øvrige kriteriene. Dette gjør retten basert på disposisjonsprinsippet (tvisteloven § 11-2), som innebærer at retten er bundet av påstandene som partene fremsetter. Ved en abstrakt prøving av e-lovens lovliggheit i lys av EMK, vil imidlertid en vurdering begrenset til 5 av 8 kriterier som EMD har oppstilt for bulklagringsregimers lovliggheit, innebære at rettens samlede vurdering metodisk taper av syne viktige hensyn. En reell samlet vurdering («global assessment») av TI etter EMK forutsetter en vurdering av alle relevante momenter som EMD har

oppstilt.¹⁴ Metodisk kommer avgjørelsen dermed skjevt ut fra start, noe som kan ha fått uheldige innvirkninger på rettens materielle vurderinger.

I lys av partenes anførsler vurderer retten om kontrollmekanismene e-loven gir for beskyttelse av berørte rettigheter er betryggende, og det vises til det grundige lovarbeidet som ble gjort av myndighetene i forbindelse med vedtagelse av e-loven i 2020 og frem til endelige endringer ble vedtatt i 2023 med hensyn til utvikling i internasjonal rettspraksis om bulklagring. En sentral rettsikkerhetsgaranti som kom inn i loven i 2023 var krav om domstolskontroll som forutsetning for E-tjenestens inngrep, herunder bulkinnhenting og -lagring, målsøking, målrettet innhenting eller videre behandling. Retten understreker at E-tjenesten skal innhente forhåndstilatelse fra retten i to omganger: først må rettens tillatelse innhentes for tilrettelegging og speiling av metadata i bulk, og for å få nærmere tilgang til dataene gjennom søk og videre bruk må E-tjenesten på nytt innhente tillatelse.¹⁵ Det betyr at tillatelse skal gis av retten for E-tjenestens konkrete formål med databefatningen. Dette er en viktig presisering for reell domstolskontroll med enkeltstående inngrep, og må tolkes dithen at domstolskontroll som hovedregel skal gjennomføres separat og forut for hvert stadiet i prosessen av TI. Konkret domstolskontroll for enkeltstående inngrep som databefatningen representerer er en viktig rettsikkerhetsgaranti, da det begrenser E-tjenestens adgang til å be om en samlet adgang til bulkinnhenting, målrettet innhenting og videre bruk av data til analyse/behandling.

I den samlede vurderingen påpeker retten at e-lovens kontrollordning inneholder en svakhet i form av manglende adgang til effektivt rettsmiddel (EMK Artikkel 13), herunder at «en klager har begrensede muligheter til å få bekreftet om det har skjedd en rettighetskrenkelse».¹⁶ Dette tillegges tilsynelatende lite eller ingen vekt i helhetsvurderingen, uten nærmere begrunnelse enn at «[d]et er summen av de nasjonale rettsmidlene som avgjør hvorvidt det foreligger tilstrekkelige garantier mot misbruk».¹⁷ Premisset er riktig, men forutsetter at svakheten ved manglende rettsmiddel er uvesentlig og at alle relevante hensyn har vært vurdert i «summen» av kontrollmekanismer. Det er et problem at avgjørelsen etterlater tvil om begge deler.

Retten anerkjenner for eksempel at EOS-utvalget mangler kapasitet som uavhengig kontrollorgan for regelverket, men understreker at det er opp til statens skjønn å vurdere hvilke ressurser som skal tilføres organet.¹⁸ Selv om ressursfordeling i utgangspunktet tilfaller statens skjønnsmargin, ville EMD neppe tillatt denne type ansvarsfraskrivelse; Statens positive forpliktelser etter EMK er også administrative. I praksis er det vanskelig å se forbi at EOS-utvalget potensielt er hindret fra å utføre sitt arbeid som kontrollorgan på grunn av ressursmangel. Kombinert med mangelen på effektivt rettsmiddel, er det betenkelig at tingretten ikke benytter anledningen til å reise kritikk mot kontrollordningen, for eksempel ved å understreke at staten er forpliktet etter EMK til å sikre forsvarlige ressurser for håndhevelse av menneskerettighetene som lovverket skal beskytte. Et lovverk med gjennomtenkte formuleringer har ikke større verdi enn dets mekanismer for å håndheve det.

13 Se Oslo Tingrett i 24-038001TVI-TOSL/04 på s. 24-25 og Big Brother Watch mot Storbritannia [GC] avsnitt 361.

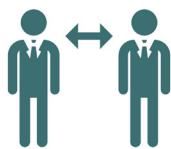
14 Se til sammenligning EMDs metode i Big Brother Watch mot Storbritannia [GC] og Centrum for Rättvisa [GC].

15 24-038001TVI-TOSL/04 på s. 5 og 49.

16 24-038001TVI-TOSL/04 på s. 48.

17 Ibid.

18 24-038001TVI-TOSL/04 på s. 44.



Illustrasjon: Colourbox.com

Det er ellers uheldig at retten underspiller hvilken nedkjølingseffekt TI vil kunne ha for pressens ytringsfrihet (kildevernet). Slik dommen er skrevet, fremstår det som rettens vektlegging av kildevernhensyn er begrenset til den konkrete forholdsmessigheten av enkeltstående inngrep. På denne måten mister retten av syne at TI, som et system for masselagring av kommunikasjonsdata, i seg selv vil ha en nedkjølende effekt på ytringsfriheten i det digitale rom, fordi folk flest er klar over at kommunikasjonsdata innhentes og lagres i bulk. Det er den langsiktige nedkjølingseffekten på ytringsfriheten kildevernet først og fremst skal hindre, og som er særlig problematisk ved innføringen av TI som etterretningsverktøy.

Det samme kan sies om rettens underspilling av risikoen for mis-

bruk av TI, for eksempel formålsutglidning eller skadepotensialet ved et fremtidig udemokratisk maktskifte. Innføring av et datainnsamlingssystem av denne dimensjonen bærer med seg en åpenbar iboende risiko for misbruk. Jeg stiller meg undrende til at denne risikoen ikke får større plass i avgjørelsen, for eksempel gjennom strengere krav til løpende og etterfølgende kontroll. Kanskje ville Oslo Tingrett vurdert lovgivningen strengere dersom systemets misbrukspotensiale ble løftet frem i større grad. På grunn av langsiktige konsekvenser for grunnleggende rettigheter, blir det desto viktigere at lovens kontrollmekanismer er betryggende, og at kontrollorganer utstyres med nok ressurser til å håndheve rettighetene.

Siste ord er ikke sagt i spørsmålet om det norske TI-regelverket gir

tilstrekkelige garantier mot misbruk. Tiden vil vise om behandlingen blir annerledes når lagmannsretten skal foreta en ny, uavhengig vurdering av e-lovens mekanismer for å beskytte berørte aktører, personer og fortrolige kilder. Avgjørende i praksis blir uansett hvordan involverte aktører tar i bruk systemet i tråd med den teknologiske utviklingen. Det er ikke mulig å forutse alle utfordringer som kan true systemet i fremtiden. Et system av denne karakter er demokratisk avhengig av at det føres kontinuerlig kontroll for å sikre at grunnleggende verdier etterleves.

Annelin Sodal, advokatfullmektig, arbeider i Advokatfirmaet Wiersholms avdeling for teknologi, media, telekom og immaterialrett.

Birkenstock-sandaler er ikke beskyttet av opphavsrett

Av Nicholas Foss Barbantonis og Henning Wahlberg

Tysk høyesterett med ny avgjørelse som nyanserer verkshøydekravet for kunst-håndverk/brukskunst

Tysklands føderale høyesterett for sivil- og straffesaker, Bundesgerichtshof («BGH»), har nylig konkludert med at Birkenstocks populære sandalmodeller «Madrid» og «Arizona» ikke nyter opphavsrettslig vern.¹ Sandalene oppfylte ikke kravet om original og individuell skapende åndsinnsett (kravet om verkshøyde/originalitet).

Avgjørelsen er interessant da den, sammen med øvrig nyere rettspraksis fra EU-domstolen, bidrar til å nyansere og videreutvikle sondringen mellom funksjonelle og ikke-funksjonelle (eller kunstneriske) elementer i såkalt kunsthåndverk (eller «brukskunst»), jf. åndsverkloven § 2 annet ledd bokstav j (og i forlengelsen Direktiv 2001/29/EF art. 2(a)).

Det finnes begrenset med rettspraksis om opphavsrettsbeskyttelse for brukskunst i Norge. Fra EU-domstolen har det de siste årene vært en utvikling innen tematikken. BGHs avgjørelse har naturligvis ingen direkte virkning utenfor Tyskland, men nasjonale domstoler i både EØS og EU skal legge opphavsrettsdirektivene til grunn for å oppnå såkalt direktivkonformitet. Avgjørelsen fra BGH kan dermed bidra til å klarlegge grensene for opphavsrettsbeskyttelse for brukskunst etter opphavsrettsdirektivet.



Nicholas Foss Barbantonis



Henning Wahlberg

I tråd med gjeldende EU-domstolspraksis understreket BGH at åndsverk må være originalt og gjenspeile opphaverens personlighet gjennom frie og kreative valg. Videre bekreftet BGH at rent tekniske eller funksjonelle verk ikke nyter beskyttelse. Ved anvendelse av disse prinsippene på Birkenstocks sandaler fant BGH at eventuelle kreative bidrag i designene var for beskjedne til å oppnå det nødvendige nivået av kunstnerisk originalitet. Birkenstock-avgjørelsen er enda et eksempel på at det i praksis kan være utfordrende å sannsynliggjøre at det kreative handlingsrommet er benyttet i tilstrekkelig grad for brukskunst. Den kan også bidra til å presisere prinsippene tidligere fastsatt av EU-domstolen i C-683/17 (Cofemel).²

I Cofemel, som omhandlet klær, forela Portugals høyesterett EU-domstolen spørsmål om originalitetsnivået som kreves for at brukskunst skal kunne nyte vern etter

opphavsretten, altså den nærmere terskelen for verkshøydevurderingen. Som i Norge, var det ikke i Portugal noen fullstendig klar eller enhetlig rettspraksis på forholdet mellom funksjonelle og ikke-funksjonelle verk, herunder klare retningslinjer for hvordan den konkrete vurderingen skal foretas. I tråd med etablert rett, jf. også C-145/10 (Painer), bekreftet EU-domstolen at det første kravet er at verket må reflektere opphaverens personlighet, som et uttrykk for dennes frie og kreative valg. For det andre vil opphavsretten kun omfatte de elementer i verket som nettopp gir uttrykk for kunstnerens frie og kreative valg. EU-domstolen presiserte at konseptet av et verk nødvendigvis innebærer at det finnes en gjenstand som er identifiserbar med tilstrekkelig presisjon og objektivitet. Dette er en forutsetning for å kunne håndheve rettigheten. EU-domstolen har videre understreket at man ikke vil oppfylle kravet om presisjon og objektivitet dersom disse elementene hovedsakelig baseres på opphaverens individuelle og subjek-

¹ I ZR 16/24, åpent tilgjengelig her: <https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&Sort=12288&nr=140774&anz=1209&pos=29&Blank=1.pdf>.

² Big Brother Watch m.fl. mot Storbritannia [GC] avsnitt 339.

tive opplevelser. Verket vil heller ikke oppfylle originalitetskravet dersom verket er diktet av tekniske hensyn, regler eller begrensninger, som ikke gir rom for kreativ frihet.

Dersom verket oppfyller karakteristikkene omtalt ovenfor, vil det ifølge Cofemel oppfylle verkshøydekravet. Ved vurderingen av beskyttelsesomfanget er det ikke avgjørende om verket er brukskunst eller annen type åndsverk. I Cofemel var det liten tvil om at klærne genererte en «*spesifikk og estetisk signifikant visuell effekt*». Dette var imidlertid ikke tilstrekkelig. Den visuelle effekten bidro i liten grad til at verket kunne karakteriseres som identifiserbart med tilstrekkelig presisjon og objektivitet. Når verket, her klærne, har et klart funksjonelt formål, må det noe mer til enn å vise til en spesifikk og estetisk signifikant visuell effekt. Verket må også påvise opphaverens personlighet, som uttrykk for dennes frie og kreative valg. Det var ikke tilfellet i Cofemel. Klærne oppfylte dermed ikke originalitetskravet/verkshøydekravet.

I Birkenstock gjentar BGH flere av vurderingene i Cofemel, og presiserer videre at et verk ikke nyter opphavsrettslig vern dersom det utelukkende består av teknisk nødvendige, valgfrie eller utskiftbare, men tekniske betingede trekk, og ikke viser noen kunstnerisk prestasjon. Den blotte utnyttelse av et teknisk-konstruktivt spillerom eller utskiftning av et teknisk trekk med et annet oppfyller ikke verkshøydekravet.

Birkenstock-avgjørelsen illustrerer den grunnleggende forskjellen mellom kunstneriske og funksjonelle elementer i et verk. Spørsmålet var om verkets kunstneriske elementer var diktet av dets funksjon, og om denne utformingen nådde et nivå som berettiger opphavsrettslig beskyttelse. BGH konkluderte med at sandalene ikke nøy opphavsrettslig vern. I saken var det ikke omstridt at sandalene formidlet et konsistent og karakteristisk helhetsinn-

trykk, og var objektivt identifiserbare.

Problemet var at de ikke oppfylte verkshøydekravet som følge av at de ikke var originale, i den forstand at de var opphaverens egne intellektuelle verk. Birkenstock hadde ikke sannsynliggjort en *tilstrekkelig utnyttelse av det kunstneriske spillerommet*. Det kunne ikke godtgjøres at Birkenstock-sandalene skilte seg kunstnerisk fra den ordinære utformingen av ergonomiske sandaler som allerede var kjent på 1960- og 1970-tallet, som er tidspunktet de aktuelle modellene ble skapt. Opphaveren hadde holdt seg til det kjente og innenfor det håndverksmessige området til en ordinær skomaker eller ortopedisk skomaker. Det var ikke mulig å utlede utfra dette at Birkenstock hadde utnyttet de eksisterende designmulighetene på en slik kreativ måte som reflekterte vedkommendes personlighet. Tvert imot fant BGH det bevist at sandalene i første rekke var innrettet mot å skape et produkt som var særlig «sunt» for foten, men som også samtidig var salgbart. Dette harmonerer langt på vei med norsk rettspraksis, men Birkenstock-avgjørelsen innebærer en nærmere konkretisering av forholdet mellom funksjonelle og ikke-funksjonelle elementer (formelementer) i brukskunst.

Verkshøydekravet for brukskunst har vært behandlet av Høyesterett i Rt. 1962 s. 964 (Wegner), Rt. 2012 s. 1062 (Tripp Trapp), Rt. 2013 s. 822 (Ambassadør) og HR-2017-2165-A (Il Tempo Gigante). Rt. 2013 s. 822 (Ambassadør) gjaldt bygningskunst og berørte også forholdet mellom funksjonalitet og verkshøydekravet.

I Il Tempo Gigante presiserte Høyesterett at ordet «originalt» ikke innebærer et krav om nyhet, men at det må være skapt noe som har en viss grad av individualitet og kreativitet, og at det ved «*originalitetsbedømmelsen skal tas hensyn til både enkeltelementer i verket og til verket bedømt som en helhet*», samtidig som «*[o]gså en ori-*

ginal sammenstilling av kjente enkeltelementer kan oppfylle verkshøydekravets». Beskyttelse forutsetter, i henhold til EU-domstolens avgjørelse i C-145/10 (Painer), at opphaverens intellektuelle frembringelse er uttrykk for dennes frie og kreative valg. Generelt er det lagt til grunn en relativt lav terskel for å oppfylle verkshøydekravet, likevel er det også klart at det skal trekkes en nedre grense for hva som kan anses som et opphavsrettslig verk. EU-domstolen har i C-5/08 (Infopaq I) kommet til at et lite tekstutdrag på 11 ord fra avisartikler var tilstrekkelig. Dette eksemplet skiller seg imidlertid fra Birkenstock-eksempelet ettersom førstnevnte gjelder tekst (ikke-funksjonelt verk), mens sistnevnte gjelder brukskunst (funksjonelt verk).

I Ambassadør har Høyesterett fastslått at det ikke gjelder noen strengere norm for verkshøydevurderingen for bygningskunst isolert sett. At dette likevel fort kommer på spissen skyldes at det for funksjonelle verk ofte er utfordrende å skille mellom de funksjonelle og ikke-funksjonelle elementene ved verkshøydevurderingen. Dersom det viser seg at det faktisk er de funksjonelle elementene som utelukkende utgjør verkets originalitet, så skal i utgangspunktet konklusjonen bli at det ikke foreligger verkshøyde i opphavsrettslig forstand.³ I så tilfelle er rettighetshaver bedre stilt ved å gå veien om designregistrering, alternativt (og som siste skanse) hevde etterlikningsvern etter markedsføringslovens bestemmelser.

I Tripp Trapp konkluderte Høyesterett med at Stokkes barnestol oppfylte verkshøydekravet. I tråd med en sakkyndiguttalelse i saken ble dette beskrevet som «*et harmonisk, rytmisk og 'musikalsk' preg, med en utforming som formidler trygghet og*

³ Dette har vært ansett som rimelig sikker rett, se bl.a. Opphavsrett, 2. utg., 2019 s. 110 flg.

soliditet». Høyesterett vektla det faktum at Tripp Trapp-stolen på introduksjonstidspunktet på 1970-tallet «*var original og god – konseptet var egnet til å vekke oppsikt*». I sin vurdering henviste Høyesterett til utenlandske rettsavgjørelser vedrørende Tripp Trapp-stolen, inkludert danske Højesterets dom U 2001 747 H hvor det følger at stolen har «*et banebrytende helt usedvanlig egenartet design*». Lagmannsrettens vurdering, som Høyesterett også tilsluttet seg, var at stolens formelementer «*... gir et helhetspreg av originalitet, som er resultat av en selvstendig, skapende innsats. Formgivningen fremstår som særpreget og med stor grad av nyskapning sammenlignet med eksisterende stoler. Kravene til åndsverk er etter dette klart oppfylt*». Tilsvarende konkluderte Høyesterett i Ambassadør at det aktuelle typehuset hadde oppfylt kravet til verkshøyde. I dommen bekreftet Høyesterett at funksjonelle elementer ikke er vernet. Vernet omfattet utelukkende «*den særlige utformingen/uttrykket som huset har fått*». Som det fremgår i Opphavsrett, 2. utg., 2019 s. 115, kan det antas at Høyesterett i Tripp Trapp har «*ment at stolens funksjonalitet kan oppnås på flere forskjellige måter, og at [designeren] ved sin design har utnyttet de valgmuligheter som finnes i så henseende*». Tilsvarende bør også kunne legges til grunn for Ambassadør.

Birkenstock bryter ikke fundamentalt med tidligere rettspraksis, men den trekker en noe strengere og klarere ramme for vurderingen av verkshøyde i brukskunst. De tidligere ovennevnte avgjørelser vektlegger opphaverens frie og kreative valg som grunnlag for opphavsrettslig vern. Det Birkenstock-avgjørelsen tilfører, er en mer presis sondering mellom kunstneriske og funksjonelle elementer, og en tydeligere definisjon av hva som kreves for at et verk skal oppnå beskyttelse.

Birkenstock fremhever at kunstnerisk originalitet må gå utover det estetisk tiltalende og representere en unik og individuell skapende innsats som ikke er diktet av funksjonelle



Illustrasjon: Colourbox.com

krav. Dette innebærer at elementer som er nødvendige for verkets funksjon, eller som kan byttes ut med andre tekniske løsninger, ikke kan danne grunnlag for opphavsrettslig vern. Et verk som primært består av slike elementer, vil derfor ikke oppfylle verkshøydekravet.

Videre understreker avgjørelsen viktigheten av at opphaveren har utnyttet et kreativt spillerom i utformingen av verket. Det må være en demonstrasjon av opphaverens personlighet gjennom valg som ikke er begrenset av tekniske eller funksjonelle hensyn. Selv om et verk kan ha et konsistent og karakteristisk helhetsinntrykk, må det også kunne identifiseres som opphaverens intellektuelle frembringelse, og ikke bare som en funksjonell gjenstand. I dette ligger også at det ikke er tilstrekkelig at det forelår et kreativt handlingsrom ved skapelsen av verket – utnyttelse av kreativ frihet er ikke isolert sett tilstrekkelig for å oppfylle verkshøydekravet. Det må kunne påvises at valgene som ble tatt innenfor dette handlingsrommet var frie og kreative, og ikke bestemt av tekniske behov.

I avgjørelsen ble det også vurdert om etterfølgende momenter skal få betydning for vurderingen av verkshøyde, herunder verkets presentasjon på utstillinger eller kunsthaglig

anerkjennelse. Slike bevis hadde blitt lagt frem for å underbygge at sandalene oppfylte verkshøydekravet. Hvorvidt slike etterfølgende bevis er relevante er forelagt EU-domstolen i forbindelse med en annen sak som verserer for BGH (USM Haller).⁴ I Birkenstock konkluderte BGH uansett at slik dokumentasjon ikke endret konklusjonen om at sandalene mangler verkshøyde.

Birkenstock-avgjørelsen bidrar til å utpensle den nærmere grensedragningen for verkshøyde og brukskunst. Dommen kan potensielt betraktes som «streng», og kan bidra til å heve terskelen for å oppnå opphavsrettsbeskyttelse til brukskunst.

Av Nicholas Foss Barbantonis, assosiert partner, Advokatfirmaet Simonsen Vogt Wiig AS. Nicholas arbeider i firmaets prosedyreavdeling, med fokus på teknologi, media, telekom og immaterialrett, og Henning Wahlberg, advokat i Advokatfirmaet Simonsen Vogt Wiig AS. Henning arbeider i firmaets teknologi- og medieavdeling, med fokus på immaterialrett.

⁴ EU-domstolen har p.t. ikke tildelt saksnummer; I ZR 96/22 (USM Haller).

KI-forordningens krav om å sikre kompetanse innenfor kunstig intelligens

Av Ove A. Vanebo

1. Innledning

Kunstig intelligens («KI») er i ferd med å bli nærmere regulert gjennom forordning om kunstig intelligens («KI-forordningen»), populært kalt «AI Act».¹ EU-rettsakten skal etter planen bli gjennomført i norsk rett sommeren/høsten 2026.

Et krav som allerede er tredd i kraft innenfor EU, erplikten til å sørge for tilstrekkelig kompetanse (engelsk: «AI literacy») for nærmere bestemte personer, som lyder slik i den danske oversettelsen:

Artikel 4 AI-færdigheder

Udbydere og idriftsættere af AI-systemer træffer foranstaltninger til i videst muligt omfang at sikre et tilstrækkeligt niveau af AI-færdigheder hos deres personale og andre personer, der er involveret i drift og anvendelse af AI-systemer på deres vegne, og tager herved hensyn til disse personers tekniske viden, erfaring og uddannelse og den kontekst, hvori AI-systemerne skal anvendes, og de personer eller grupper af personer, som AI-systemerne skal anvendes på.

Artikkelen har ingen parallell i norsk lovgivning i dag. Målet om KI-kompetanse er begrunnet i tre ulike formål.² For det første skal kravene sørge for størst mulig fordel ved bruk av KI-systemer, ved at «den brede gjennomførelse af foranstaltninger vedrørende AI-færdigheder og indførelsen af passende opfølgende tiltag [kan] bidrage til at forbedre arbejdsvilkårene og i sidste ende understøtte konsoliderings- og innovasjonsstien for troværdig AI i Unionen». For det annet skal



Ove A. Vanebo

kompetansen beskytte «de grundleggende rettigheder, sundheden og sikkerheden». Til sist skal kompetansen «muliggjøre demokratisk kontroll», trolig for å unngå at «big tech» og andre mektige aktører skal få ubegrenset spillerom.

På mange måter kan man anse kravet som en del av allmennutdanningen, der man både skal tilegne seg ferdigheter og kunne bli et selvstendig, tenkende menneske.³ Samtidig er kravet begrenset til en nærmere krets.

KI-forordningens krav om KI-kompetanse er imidlertid nokså uklart, og i litteraturen er det påpekt at: «The reality is that AI literacy remains a novel and fuzzy concept which, despite receiving some attention from researchers, has yet to be fully elaborated or to have consensus.»⁴

Målsettingen med min artikkel er derfor å tydeliggjøre hva kravet til KI-kompetanse innebærer i praksis.

Siden det ennå ikke finnes en norsk oversettelse, vil jeg henvide til den danske og engelske oversettelsen for å belyse innholdet i bestemmelsen. Språklige nyanser kan også illustrere hva som ligger i artikkelens krav.

2. Hva er KI-kompetanse?

KI-kompetanse omfatter en rekke ulike aspekter ved å håndtere KI på en forsvarlig måte. I Norge har departementet først og fremst fokusert på oppnåelse av tilstrekkelig *kunnskap*.⁵ Den danske oversettelsen viser til «ferdigheter» – mens den engelske språkdrakten bruker uttrykket «literacy», dvs. en form for «alfabetisme», som trolig henspiller på både teoretisk og praktisk kyndighet.

KI-kompetanse er definert i artikkel 3(56):

«færdigheder, viden og forståelse, der giver udbydere, idriftsættere og berørte personer mulighed for under hensyntagen til deres respektive rettigheder og forpligtelser i forbindelse med denne forordning at idriftsætte AI-systemer på et informeret grundlag samt at øge bevidstheden om muligheder og risici ved AI og den mulige skade, som den kan forvolde»

1 Europaparlaments- og rådsforordning (EU) 2024/1689.

2 KI-forordningen fortalepunkt 20, jf. fortalepunkt 91.

3 Elora Fernandes, Wayne Holmes og Sopio Zhgenti, «Article 4 AI Literacy», 2024, punkt 1 Purpose. I: Ceyhun Necati Pehlivan, Nikolaus Forgó og Peggy Valcke, *The EU Artificial Intelligence (AI) Act: A Commentary*.

4 Fernandes, Holmes og Zhgenti (2024) punkt 3.2 Defining AI Literacy.

5 Se Regjeringens EØS-notatbase, som påpeker at «Art. 4 angir et særlig krav til 'AI literacy', som kan forstås som kunnskap om KI-systemer.» Lest 5. mai 2025: <https://www.regjeringen.no/no/no/sub/eos-notatbasen/notatene/2021/juni/forslag-til-forordning-om-kunstig-intelligens-ki-forordning/id2884935/>

Definisjonen tydeliggjør at KI-kompetanse vil kreve at leverandører, profesjonelle brukere og berørte personer i vid forstand må forstå hvordan KI «fungerer» og kunne bruke det på en forsvarlig måte. Dette er også påpekt i fortalepunkt 20:

«Disse begreber kan variere med hensyn til den relevante kontekst og kan omfatte forståelse af den korrekte anvendelse af tekniske elementer i AI-systemets udviklingsfase, de foranstaltninger, der skal anvendes under dets anvendelse, passende måder at fortolke AI-systemets output på, og i tilfælde af berørte personer den viden, der er nødvendig for at forstå, hvordan beslutninger truffet med hjælp fra AI vil have indvirkning på dem.»

Med «færdigheder» siktes trolig til at relevante personer skal rent *faktisk* kunne bruke kunstig intelligens på en tilfredsstillende måte. Kunnskap, «viden», innebærer nok at personer som bruker KI-systemer må vite hva som skjer i systemet, og hvordan det (overordnet) fungerer. Trolig betyr «forståelse» at brukeren får innsikt og kan se sammenhenger, f. eks. klarer å utlede/tolke hva en frembringelse uttrykker (med svakheter og styrker), og forstår hva slags virkning bruken av kunstig intelligens kan ha både direkte og mer indirekte.

I praksis vil dette bety at de som oppnår KI-ferdigheter skal kunne håndtere varierende tekniske, juridiske og etiske problemstillinger som kan oppstå, kanskje (særlig) i utviklingsfasen, bl.a. i forbindelse med å identifisere problemer, data-innsamling, databehandling, valg av modeller, trening osv.⁶

3. Hvem er omfattet av plikten til å sørge for tilstrekkelige KI-ferdigheter?

3.1 Generelt

To ulike aktører er pliktsubjekter:

«Udbydere» i den danske språkdrakten kan oversettes til «leverandøren» på norsk. Dette er aktøren som «*udvikler eller får udviklet et AI-system eller en AI-model til almen brug og bringer dem i omsætning eller ibrugtager AI-systemet under eget navn eller varemærke, enten mod betaling eller gratis*».⁷

Kategorien «idriftsættere» er oversatt til «deployer» på engelsk, og vanligvis omtalt som «bruker» på norsk (selv om den endelige betegnelsen neppe er avklart for Norges vedkommende, og trolig blir avgjort først i lovproposisjonen). Definisjonen i KI-forordningen artikkel 3(4) fastslår at dette er den «*der anvender et AI-system under sin myndighed*». Litt enkelt sagt er det altså aktøren som benytter KI-systemer i profesjonell sammenheng. Det avgrenses m.a.o. mot bruk der «*AI-systemet anvendes som led i en personlig ikkeerhvervsmessig aktivitet*», jf. samme artikkel.

3.2. Må også leverandører og brukere av KI-systemer med liten eller lav risiko følge kravet?

Ordlyden i forordningen tilsier at leverandører og alle brukere av KI-systemer, uavhengig av risikonivå, er omfattet av KI-kompetanse-plikten. Det er også nesten unisont antatt i juridisk teori at KI-systemer som normalt er uregulerte av KI-forordningen omfattes av plikten til KI-kompetanse.⁸

For egen del er jeg mer usikker på om KI-systemer uten eller med minimal risiko er omfattet, siden

forordningens systematikk unntar slike systemer. EU-kommisjonen synes også å legge til grunn på generelt grunnlag at slike systemer ikke er regulert, og nevner at: «*The AI Act does not introduce rules for AI that is deemed minimal or no risk.*»⁹

Praksis vil formodentlig endelig avklare spørsmålet.

4. Hvem skal oppnå KI-kompetanse?

Både «personale og andre personer, der er involveret i drift og anvendelse af AI-systemer på deres vegne» skal tilegne seg KI-kompetanse.

Med «personale» (engelsk: «staff») siktes det primært til en virksomhets ansatte. Det må legges til grunn at både midlertidige og faste ansatte omfattes. EU-kommisjonen har påpekt at: «*This concerns anyone in the organisation directly dealing with an AI system and reinforces the provisions of transparency (Article 13 of the AI Act) and human oversight (Article 14 of the AI Act) included in the Regulation.*»¹⁰

«Andre personer» er formodentlig en nokså vid gruppe. Både konsulenter og andre oppdragstakere, tredjepartsleverandører og individer fra andre avdelinger i virksomheten vil trolig omfattes – så fremt de tidvis befatter seg med KI-systemet.¹¹

Plikten i KI-forordningen artikkel 4 er ikke ment for bred, allmenn opplysning eller for å løfte kompetansen for utsatte eller marginaliserte grupper.¹² Primært er målgruppen «alle relevante aktører i AI-værdikæden den innsikt, der er

6 Fernandes, Holmes og Zhgenti (2024) punkt 3.1 *Responsibilities and Obligations*.

7 KI-forordningen artikkel 3(3).

8 Se bl.a. Paul Voigt og Nils Hullen, *The EU AI Act; Answers to Frequently Asked Questions*, 2024, s. 4 og 30-31; og W. Kuan Hon, *AI literacy: EU AI Act*, 2025. Lest 4. mai 2025: <https://blogkuan0.com/2025/02/ai-literacy-eu-ai-act.html>. Tilsynelatende motsatt, se Tiago Sérgio Cabral, *AI Literacy Under the AI Act: An Assessment of its Scope*, 2025. Lest 4. mai 2025: <https://eulawanalysis.blogspot.com/2025/02/ai-literacy-under-ai-act-assessment-of.html>

9 EU-kommisjonen, *AI Act*. Lest 3. mai 2025: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

10 EU-kommisjonen, *AI Literacy - Questions & Answers*, 2025. Lest 20. mai 2025: <https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers>

11 Fernandes, Holmes og Zhgenti (2024) punkt 3.1 *Responsibilities and Obligations*.

12 Fernandes, Holmes og Zhgenti (2024) punkt 3.1 *Responsibilities and Obligations*.

nødvendig for at sikre passende overholdelse og korrekt håndhævelse heraf.¹³

Likevel nevner både artikkel 3(56) og fortalepunkt 20 at KI-kompetanse skal «udstyre udbydere, idriftsættere og *berørte personer* med de nødvendige begreber til at træffe informerede beslutninger vedrørende AI-systemer.» Trolig betyr dette at KI-kompetanse også bør oppnås for bl.a. studenter eller foreldre til elever som går på skolen, som på en eller annen måte vil interagere med eller bruke KI-systemer.¹⁴

5. Hva slags tiltak må gjennomføres for å oppfylle plikten?

5.1 Innledning

Det må iverksettes «foranstaltninger», som på norsk er «tiltak». Begrepet er generelt, og vil favne bredt. Dette gjenspeiles også i at KI-kompetanse omfatter både kunnskap, ferdigheter og forståelse, jf. definisjonen i artikkel 3(56). Det kan være nærliggende å sammenligne med hva som er «tiltak» i henhold til EUs personvernforordninger (GDPR), der begrepet kan omfatte tiltak av både organisatorisk, teknisk og fysisk karakter.

5.2 Konkrete typer av tiltak

«Tiltak» vil klart omfatte ulike former for kunnskapsdeling og opplæring. Dette kan være i form av bl.a. fysiske kurs, dokumenter med informasjon eller e-opplæring med ulike avkrysningsskjemaer/multiple choice. Ulike former for «oppskrifter» og bruksmanualer kan også være egnet for å gi personene innsikt.

Ettersom ferdigheter er et aspekt ved KI-kompetansen, er det naturlig å se for seg at personer også bør gjennomgå praktisk opplæring, ved at personer prøver å benytte KI-systemet og løser bestemte oppga-

ver. Også forskjellige gjennomganger, monitorering og risikovurderinger vil bidra til å gi forståelse og ferdigheter.¹⁵

Det er også mulig å opparbeide forståelse gjennom ulike former for diskusjonsfora, f.eks. med «table top-øvelse», der ulike diskusjonsbaserte oppgaver løses både i dialog og med individuelle vurderinger og fremføringer.

Antagelig vil ulike former for mer direkte instruksjoner om fremgangsmåter (direkte eller indirekte) kunne være egnet til å gi folk kompetanse, f.eks. pålegg om å lese seg opp eller gå frem på en bestemt måte. Ulike incentiver kan være hensiktsmessige tiltak, f.eks. en kinobillett hvis man fullfører et e-kurs, eller tilrettevisninger ved manglende oppfølging av pålegg om opplæring.

6. Hva er tilstrekkelig KI-kompetanse?

6.1. Generelt

KI-forordningen foreskriver at personene som skal få kompetanse må oppnå et «tilstrækkeligt niveau af AI-færdigheden». Hva som ligger i dette, er et mer åpent spørsmål. Det er trolig et visst handlingsrom, og det er ingen plikt til å «måle» KI-kompetansen.¹⁶ Det er nærliggende å anta at det sentrale er at relevante personer skal få tilstrekkelig kompetanse til å overholde pliktene i KI-forordningen.¹⁷ Et utgangspunkt kan være behovet for å oppnå en informert «utrulling» og bruk av AI-systemer, og hvordan man kan

være bevisst på risikoer og muligheter knyttet til AI-systemer.¹⁸

Antagelig er det neppe nok å ha en engangsinnsetning. Tilstrekkelig KI-kompetanse vil være en mer kontinuerlig forpliktelse, der bl.a. endringer i systemer eller kunnskap kan medføre at det må iverksettes nye tiltak.¹⁹

6.2. Tilpasning av tiltakene

6.2.1. Innledning

Tiltakene skal ta hensyn til og differensieres, ved at virksomhetene skal ta i betraktning:

- Personene som skal bruke systemene
- Konteksten systemene brukes i
- Personene som KI-systemene skal brukes på

6.2.2. Personene som bruker KI-systemene

For det første må tiltakene ta hensyn til «personale og andre personer, der er involveret i drift og anvendelse af AI-systemer» som handler brukernes og leverandørenes vegne, ved at det tas hensyn til dere «tekniske viden, erfaring og uddannelse». Litt enkelt sagt, må dette innebære at man ser hva disse brukerne har av KI-kompetanse i dag, og ser dette opp mot hva som målsettingen basert på hva som er et passende behov. «Gapet» må fylles med passende tiltak.

6.2.3. Kontekst

Tiltakene må også tilpasses «den kontekst, hvori AI-systemerne skal anvendes». Dette henspiller trolig på at det vil være forskjell på f.eks. om systemene brukes i helsesektoren eller i skolevesenet – og at det er

¹³ KI-forordningen fortalepunkt 20.

¹⁴ Fernandes, Holmes og Zhgenti (2024) punkt 3.1 *Responsibilities and Obligations*.

¹⁵ Elora Fernandes, *AI Literacy in the AI Act*, 2025, s. 17. Foredrag, Lest 3. mai 2025: <https://lirias.kuleuven.be/retrieve/800402>

¹⁶ EU-kommisjonen, *AI Literacy - Questions & Answers*, 2025.

¹⁷ Fernandes, Holmes og Zhgenti (2024) punkt 3.3 A 'Sufficient' / Ådequate / «Appropriate» Level of AI Literacy.

¹⁸ Elora Fernandes og Abdullah Elbi, *This Time, Humans Learn About Machines: AI Literacy in the AI Act (Part 2)*, 2024. Lest 3. mai 2025: <https://www.law.kuleuven.be/citip/blog/this-time-humans-learn-about-machines-ai-literacy-in-the-ai-act-part-2/>

¹⁹ Fernandes, Holmes og Zhgenti (2024) punkt 3.3 A 'Sufficient' / Ådequate / «Appropriate» Level of AI Literacy.

den spesifikke konteksten som skal vektlegges. Det nederlandske data-tilsynet nevner dette som et eksempel.²⁰

«For example, the AI literacy obligation means that an HR employee must understand that an AI system may contain biases or ignore essential information that may lead to an applicant being or not being selected for the wrong reasons.»

Det er imidlertid viktig å ha i bakhodet at kompetansekravet har en viss fleksibilitet, og det er ingen klare, ferdigdefinerte krav for bestemte sektorer eller bransjer.²¹

6.2.4. Personene som KI-systemene skal brukes på

For det tredje må tiltakene ta hensyn til «de personer eller grupper af personer, som AI-systemerne skal anvendes på».

Typisk må man ta i betraktning om KI-systemene vil få betydning for persongrupper som er særlig sårbare eller oftere blir diskriminert enn andre grupper. Eksempelvis må brukerne få kompetanse om hvordan man skal ta hensyn til en sårbar gruppes forståelse av konsekvenser og hvordan dette bør avbøtes på en hensiktsmessig måte.

6.2.5. Finnes det noen minimumskrav til KI-kompetansen?

Det er vanskelig å beskrive et «gulv» som utgjør tilstrekkelig KI-kompetanse. Likevel har EU-kommisjonen kommet med noen anbefalinger om hva som bør være på plass (min oversettelse):²²



Illustrasjon: Colourbox.com

- a. *Sørg for en generell forståelse av KI i organisasjonen: Hva er KI? Hvordan fungerer det? Hva slags type KI brukes i vår organisasjon? Hva er mulighetene og farene?*
- b. *Vurder organisasjonens rolle (leverandør eller bruker av KI-systemer): Utvikler organisasjonen min KI-systemer, eller bruker den bare KI-systemer utviklet av en annen organisasjon?*
- c. *Vurder risikoen ved KI-systemene som leveres eller benyttes: Hva trenger ansatte å vite når de håndterer et slikt KI-system? Hva er risikoene de må være klar over, og behøver de være klar over tiltakene som kan redusere risiko?*
- d. *Bygg konkrete KI-kompetansetiltak basert på den foregående analysen, med tanke på*
 - *forskjeller i teknisk kunnskap, erfaring, utdanning og opplæring hos ansatte og andre personer – Hvor mye vet de ansatte/personen om KI og organisasjonens systemer de bruker? Hva annet bør de vite?*
 - *samt konteksten KI-systemene skal brukes i og personene KI-systemene skal brukes på – I hvilken sektor og til hvilket formål/ tjeneste brukes KI-systemet?»*

7. Sanksjoner ved brudd

Brudd på plikten til å sørge for tilstrekkelig KI-kompetanse er ikke nevnt blant pliktbruddene som medfører administrative gebyrer i henhold til artikkel 99 nr. 3 og 4. Det må derfor legges til grunn at manglende overholdelse av plikten i

utgangspunktet mangler sanksjonering.²³ Det gjenstår derfor å se om Norge vil innføre særlige reguleringer for å sanksjonere slike pliktbrudd, i den grad det åpnes for det innenfor rammene av KI-forordningen.²⁴

Det er imidlertid naturlig å se for seg at brudd på andre plikter i KI-forordningen, som kan knyttes til manglende KI-kompetanse, vil bli vektlagt i vurderingen. Eksempelvis krever artikkel 26 nr. 2 at «*Idriftsøttere overdrager varetagelsen af det menneskelige tilsyn til fysiske personer, der har den nødvendige kompetence, uddannelse og myndighed samt den nødvendige støtte.*» Dette vil vanskelig kunne gjøres uten tilstrekkelig KI-kompetanse, og manglende oppfølging av artikkel 4 kan lede til brudd på artikkel 26 nr. 2.

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

20 Autoriteit Personegevens, *AI Act comes into effect: work to be done for developers and users*, 2024. Lest 4. mai 2025: <https://www.autoriteitpersoonsgegevens.nl/en/current/ai-act-comes-into-effect-work-to-be-done-for-developers-and-users>

21 EU-kommisjonen, *AI Literacy - Questions & Answers*, 2025.

22 EU-kommisjonen, *AI Literacy - Questions & Answers*, 2025.

23 Tiago Sérgio Cabral, *AI Literacy Under the AI Act: An Assessment of its Scope*, 2025 <https://eulawanalysis.blogspot.com/2025/02/ai-literacy-under-ai-act-assessment-of.html>

24 EU-kommisjonen påpeker i sin Q&A 2025 (lenke i note 10) at: «National market surveillance authorities could impose penalties and other enforcement measures to sanction infringements of Article 4. *This will be based on national laws that Member States are due to adopt by 2 August 2025.*» (Min understrekning)

When Wellness and Security Apps Betray Your Trust

By Aras Nazarovas

Apps designed to protect our peace of mind are increasingly becoming sources of anxiety. Take *7 Minute Chi – Meditate & Move*, a meditation app marketed to reduce stress, and *Robo Spam Text & Call Blocker*, an iOS tool meant to shield users from robocalls and phishing. Both promised safety – one for mental well-being, the other for digital security. Instead, they exposed sensitive user data through security failures, revealing a worrying truth: the apps we trust to guard our privacy are often the weakest links in our digital lives.

” The apps we trust to guard our privacy are often the weakest links in our digital lives.

The Irony of Leaky Safe Spaces

The 7 Minute Chi breach laid bare the personal details of over 100,000 users—names, emails, and app secrets like API keys and Facebook credentials – due to a misconfigured Firebase database. This is a betrayal. Users sought calm and focus, only to have their data potentially weaponized for phishing or identity theft.

Also, Robo Spam Text & Call Blocker, downloaded 93,000 times, leaked 339,000 reported spam numbers, customer support tickets with real names and emails, and critical app secrets. Criminals now know which numbers users block and which keywords to avoid, and this enables them to craft scams that slip past filters.



Aras Nazarovas

These leaks aren't accidents but symptoms of systemic negligence. Firebase misconfigurations, which leave databases publicly accessible, and hardcoded secrets embedded in app code are shockingly common. Our research shows 71% of 156,080 sampled iOS apps leak at least one secret, with an average of 5.2 per app. When developers cut corners, apps designed to protect become tools for exploitation.

The Human Cost of Broken Promises

For users, the fallout is deeply personal. Just imagine receiving a phishing email that references your meditation habits, perhaps even mentioning the specific app you use or the routines you follow – details you thought were private.

Or picture answering a spam call that not only gets past your trusted blocker, but uses language and tactics tailored to your reported preferences and blocked keywords, making the scam far more convincing.

In both cases, the sense of violation is profound: information you

shared in the pursuit of calm or safety is now being used to target and manipulate you, turning trusted digital spaces into sources of new anxiety.

A Failure of Accountability

Neither Apple's App Store reviews nor developer due diligence prevented these breaches. 7 Minute Chi's Firebase instance sat exposed for weeks, while Robo Spam Text & Call Blocker's parent company, Brantley Media Group, has a history of leaks, including an AI app that exposed users' intimate stories. Yet, Apple's ecosystem, often perceived as a "walled garden," lacks mechanisms to scan for hardcoded secrets or enforce secure cloud configurations.

What's Next?

To restore trust, the industry must prioritize:

- Expand app store reviews to include backend security checks: Apple and other platform owners should incorporate automated scans for misconfigured databases, hardcoded credentials, and other backend vulnerabilities before approving apps.
- Developers must follow secure coding standards, conduct regular code reviews, and leverage automated security testing tools to catch vulnerabilities early.
- Provide real-time privacy visualizations and alerts: empower users with dashboards or notifications that reveal how their data is used, and immediately alert them

to potential leaks or suspicious activity.

- Offer post-breach support and transparency, and quickly notify users in the event of a breach, provide guidance on protective actions, as well as offer services such as personal data scans to help users recover.
- Regularly update and patch apps

As the lead researcher on these investigations, I urge users to demand better. Change passwords exposed in breaches, limit data shared with apps, vet apps before installing them, as much as you can, and pressure platforms to enforce stricter standards. Until then, the very tools marketed to protect us will continue to leave us exposed.



Illustrasjon: Colourbox.com

Aras Nazarovas is an Information Security Researcher at Cybernews, a research-based technology publication. He focuses on cybersecurity and threat analysis, with expertise in identifying vulnerabilities in online services, malicious campaigns, and hardware. Aras led Cybernews' investigation into hardcoded secrets in iOS applications, revealing security risks across thousands of mobile apps. He has also contributed to uncovering significant data protection and privacy issues affecting major organizations, including NASA, Google Play, and PayPal. The Cybernews research team conducts more than 7,000 investigations annually, publishing over 600 studies to support public understanding of cybersecurity threats and promote safer digital practices.

Cybernews research:

1. *Cybernews researchers analyzed 156,080 randomly selected iOS apps – around 8% of the apps present on the App Store – and uncovered a massive oversight: 71% of them expose sensitive data.*
2. *Recently, Bob Dyachenko, a cybersecurity researcher and owner of SecurityDiscovery.com, and the Cybernews security research team discovered an*

unprotected Elasticsearch index, which contained a wide range of sensitive personal details related to the entire population of Georgia.

3. *The team analyzed the new Pixel 9 Pro XL smartphone's web traffic, and found that Google's latest flagship smartphone frequently transmits private user data to the tech giant before any app is installed.*
4. *The team revealed that a massive data leak at MC2 Data, a background check firm, affects one-third of the US population.*
5. *The Cybernews security research team discovered that 50 most popular Android apps require 11 dangerous permissions on average.*
6. *They revealed that two online PDF makers leaked tens of thousands of user documents, including passports, driving licenses, certificates, and other personal information uploaded by users.*
7. *An analysis by Cybernews research discovered over a million publicly exposed*

secrets from over 58 thousand websites' exposed environment (.env) files.

8. *The team revealed that Australia's football governing body, Football Australia, has leaked secret keys potentially opening access to 127 buckets of data, including ticket buyers' personal data and players' contracts and documents.*
9. *The Cybernews research team, in collaboration with cybersecurity researcher Bob Dyachenko, discovered a massive data leak containing information from numerous past breaches, comprising 12 terabytes of data and spanning over 26 billion records.*
10. *The team analyzed NASA's website, and discovered an open redirect vulnerability plaguing NASA's Astrobiology website.*
11. *The team investigated 30,000 Android Apps, and discovered that over half of them are leaking secrets that could have huge repercussions for both app developers and their customers.*

«Planseksjonen» – et fremmedord for Justisdepartementet i 1975

Av Øystein Blymke

En ny rettspolitikk i emning

Opprettelsen av «Planseksjonen» i Det kongelige Justis- og politidepartement i 1975 skapte ikke udelte begeistring. For mange av jurist-byråkratene i departementet den gang, utgjorde denne organisatoriske nyskaping nærmest en retts-*politisk* trussel mot klassisk, juridisk departemental tenkning.

Men den store skepsis til tross – så hindret ikke det den daværende justisminister Inger L. Valle fra Arbeiderpartiet fra å innplassere en ny enhet – «Planseksjonen» – på departementets velprøvde og delvis urørte organisasjonskart.

Statsråden hadde nemlig en visjon. En visjon om en fornyet rettspolitisk og kriminalpolitisk tenkning i Justisdepartementet. Og for å kunne realisere en slik politisk visjon, var det for Valle helt nødvendig å foreta endringer, både av organisatoriske og personellmessig art.

Justisminister Valle var ikke til å misforstå.

Og det skulle da heller ikke gå lang tid før statsrådens nye justispolitikk satte sitt preg på departementets arbeid. Endringene gjaldt både departementets lovarbeid, budsjettarbeid, forsknings- og utviklingsarbeid, og ikke minst, departementets kriminalpolitiske arbeid.

Da Inger L. Valle ble justisminister i 1973¹ tok det knapt et par år



Øystein Blymke

for hennes nye retts-*politiske* ambisjoner for alvor hadde slått rot i embetsverket. Men da det først hadde skjedd, ble det fart i sakene, for å si det litt mindre juridisk. Et av statsrådens konkrete og merkbare tiltak var da hun i 1974–1975 fikk Finansdepartementet med seg på opprettelsen av «Planseksjonen».

For å forstå godt nok det krevende politiske og faglige arbeid som lå bak opprettelsen av «Planseksjonen», kan det være nyttig med noen små anekdotiske og historiske tilbakeblikk.

«Hva driver dere egentlig med?»

For oss nye saksbehandlere i den nyetablerte Planseksjonen var det ikke bare – bare, å forsvare og begrunne Planseksjonens berettigelse i departementet. Vi burde helst kunne skaffe seksjonen den nødvendige legitimitet innad og utad, en oppgave som under det første året både var krevende, og til sine tider forvirrende.

For selv om statsråd Inger Louise Valle og statssekretær Kai Ekanger støttet vårt plan-arbeid på alle måter, var det ikke spesielt lett å

bygge opp tillit og troverdighet over natten, overfor både skeptiske og nysgjerrige departementskolleger.

Vanskelig synes nå i alle fall jeg det var, som samfunnsviter, eller som «den nye ikke-juristen» som jeg ofte hørte at det ble sagt – en slags akademisk gjøkunge kunne jeg til tider føle meg som, omgitt av en flokk jurister, struttende av selvtillit.

Et stadig tilbakevendende spørsmål som vi Planseksjon-saksbehandlere ofte fikk, var; hva vi egentlig drev med – og hva vi planla for? For min del prøvde jeg etter beste evne å overhøre sarkasmen, samtidig som jeg bestrebet meg på å gi mine juristkolleger gode, moderne og gjennomtenkte «rettspolitiske» svar. Blant annet prøvde jeg å forklare dem hva seksjonens nye «administrative utviklingsarbeid» dreide seg om.

Det var ikke lett.

Men, heldigvis fikk vi nykommere god hjelp av lederen for det allerede eksisterende «utredningskontoret». Det var et kontor som før Planseksjonen så dagens lys ble ledet av byråsjef Hjalmar Austbø som i og med Planseksjonens opprettelse fikk kontoret sitt omgjort til en seksjon.

«Seksjon» var for øvrig et relativt nytt og ukjent organisatorisk begrep i Justisdepartementet midt på syttitallet. Det gjorde ikke akkurat innsalget av seksjonen lettere.

Rent organisatorisk var *seksjon* et ledd mellom en departementsavdeling og et departementskontor. Og når lederen av seksjonen ble løftet fra byråsjef-nivå (kontor) til underdirektør-nivå (seksjon) gikk heller ikke det upåaktet hen.

Jeg fornemmet da av og til at Janteloven var et like hett disku-

1 Om Inger Louise Valle:
Hun var familie- og forbruksminister i fra 1971–1972, og ble deretter den første administrasjonsminister i det nye Forbruker og administrasjonsdepartementet i 1972. Allerede året etter overtok hun Justisdepartementet som hun bestyrte til 1979. Da ble hun Kommunal og arbeidsminister for så å bli Rasjoniseringsdirektør fra 1981 til 1986.

sjonstema blant ambisiøse departementsjurister som straffeloven og tvistemålsloven.

Utredningskontoret til byråsjef Hjalmar Austbø hadde, inntil opprettelsen av Planseksjonen, stort sett drevet med «tinglysingssaker.» Det innebar enkeltsaker med tradisjonell saksbehandling i flere ledd. Den utviklingsorienterte juristen Austbø klarte imidlertid etter hvert å overbevise sin ekspedisjonssjef og departementsråden om hvor riktig og viktig det nå var, å få effektivisert den sendrektige saksbehandlingen av tinglysingssakene ved hjelp av EDB.

Planseksjonens fremtidsrettede rettsinformatikk-arbeid møtte imidlertid lenge sterk motstand. Flere var av den mening at det ville vært en mye bedre ressursbruk og ressursutnyttelse å bruke Planseksjonens nye årsverk og kompetanse til styrking av de allerede overbelastede fagavdelingene. Slike avdelinger som Lovavdelingen, Politiavdelingen og Kriminalomsorgsavdelingen.

Ja, så mye skepsis, og så mye faglig begrunnet forvirring var det, om nytten av planlegging, den være av teknologisk eller samfunnsvitenskapelig art, at en av ekspedisjonssjefene, i samtale med meg, avslørte at han fullt og fast hadde trodd at min Cand. polit.-tittel betydde at jeg var uteksaminert ved den daværende Politi-skolen.

Mer politisk betinget planlegging og styring av departementene

I sin bok «Dette står jeg for» Gylendal 1989 spør Inger L. Valle hvor det var blitt av rettspolitikken i Justisdepartementet? Hun skriver blant annet om slike rettsverdier som; likeverd og rettferdig fordeling av goder. Selv husker jeg godt at statsråden, ved flere anledninger, minnet meg om viktigheten av å utforme en rettspolitikk som i større grad enn den eksisterende, reflekterte og understøtter vanlig folks hverdagsproblem.

«Det å kunne forstå sammenhengen mellom rettspolitikk og vel-

ferdspolitikk er vel noe dere samfunnsvitere har vel så god greie på som oss jurister» er så nær ordrett hva jeg husker hun oppmuntret meg med å si, under min første tid som ikke-jurist og en litt bortkommen «novise» i departementet.

Et historisk tilbakeblikk

Tanken om at de fleste departementer burde ha sin egen *planleggingsenhet* ble unnfanget i det såkalte Modalsli-utvalget tidlig på 70-tallet². I kjølvannet av dette utvalgets arbeid, og andre interne Ap-utvalgs vurderinger, foreslo Arbeiderpartiregjeringsen ved statsminister Trygve Brattli blant annet opprettelse av et nytt forbruker- og administrasjonsdepartement som Inger Louise Valle ble den første statsråd til å lede i 1972. Et mer systematisk politisk arbeid med organisatorisk og administrativt *plan- og utviklingsarbeid* ble en viktig del av det nye departements arbeidsområde.

Men selv med Inger L. Valles entusiasme og politiske pågangsmot, og med hennes erfaring som administrasjonsminister i ryggen, var det ikke alltid like lett for en Planseksjon-pioner å viderebringe statsrådets begeistring til våre departementskolleger. En uventet politisk, men også faglig støtte for vårt noe famlende planleggingsarbeid under den første tiden, fikk vi utrolig nok fra finansminister Per Kleppe.

På begynnelsen av 70 årene ledet nemlig Kleppe Arbeiderpartiets nye utredningskontor eller «tenkeloftet» som det den gang ble kalt. Kleppe var, både som partipolitisk tenker, og senere som Finansminister, ganske lydhør for opprettelsen av de såkalte planleggingsenheter i departementene. Og ikke bare var han lydhør. Kleppe mente slike enheter også var nødvendige for styrke den *politiske* styring av departementene.

Eller som han sa, styrke den *demonstrative* styring som nok for de departementale embetsverkene rundt omkring, var mer skånsomt å kalle det.

Mange mente den gang, ikke minst flere av oss samfunnsvitere, at Kleppes støtte til nye departementale planenheter kunne rokke uheldig ved prinsippet om det nøytrale og faglig innrettede embetsverk. For eksempel gikk diskusjonen høyt og lavt blant oss statsvitere om hvorvidt et departement skulle betraktes som et *faglig* sekretariat for den politiske ledelse, eller som et (*politisk*) sekretariat for departementets ledelse, som vel alltid er politisk? For meg, som nyansatt statsviter i justisdepartementets Planseksjon, var det vanskelig å si noe annet enn at Planseksjonens primæroppgave var å sørge for at statsråd Valles ønskede retts- og kriminalpolitikk ble gjennomført. Så fikk det bli opp til mine statsviter-kolleger i academia å gruble videre over hva det innbar.

Uansett om Justisdepartementets Planseksjon drev faglig eller politisk arbeid, så var ingen i tvil om at vårt departement trengte fornyelse. Og videre at en slik fornyelse i noen grad også måtte innebære at vi tørket litt støv fra gamle rettsvitenskapelige forestillinger om hva som var rett, galt, nødvendig og rettferdig her i samfunnet.

Hva innebærer egentlig en nødvendig fornyelse?

Planseksjonens første leder, underdirektør Hjalmar Austbø, var som jeg allerede har nevnt, en utviklingsorientert jurist, i ordets beste og videste forstand. Han var også mer lydhør enn mange for statsrådets nye rettspolitiske tanker, samtidig som han forsto sine kolleger og den rådende justisdepartements-kulturen godt nok, til ikke å presse gjennom raske endringer, uten at de var forankret i embetsverket. Denne forståelse la Austbø ikke minst til grunn når det gjaldt spørsmålet om anvendelse av EDB i justissektoren.

2 «Den sentrale forvaltningsorganisasjon» Utvalgsutredningen ble overlevert statsminister Per Borten 15. mai 1970

Og da gikk det heller ikke lang tid før både departementsråden og andre ledende embetsmenn i departementet så de samme mulighetene i EDB-teknologien som Austbø og oss andre i Planseksjonen!

Den nødvendig EDB-kompetanse til Planseksjonen skaffet Austbø gjennom rekruttering av to særdeles dyktige herrer med en unik teknisk og rettspolitisk innsikt. Den ene var juristen og EDB visjonæren Jon Bonnevie Høyer. Den andre var informasjons-teknologen og juristen Trygve Harvold. Uten deres spisskompetanse og omdømme ville Planseksjonen aldri maktet å realisere noen sine ambisiøse Juss/EDB prosjekt – i alle fall ikke i løpet av Planseksjonens relativt korte, seks-årige levetid.

Min oppgave i Planseksjonen var å utvikle departementets budsjett- og forskningspolitikk. For å kunne utføre den type utviklingsoppgaver på en god måte var det avgjørende å samarbeide tett, både eksternt med Finansdepartementet og academia, og internt, og da først og fremst med planseksjonens egne.

Planseksjonens budsjettdialog med Finansdepartementet var krevende. Finansdepartementets byråkrater ga ikke ved dørene. Når det gjaldt justisdepartementets budsjett kompenserte de knapt for ordinær lønns- og prisvekst i politiet- og rettsvesenet. Våre nye ønsker om friske penger til forskning og annet utviklingsarbeid ble under den første tiden nærmest sett på som en naiv og dårlig spøk.

Den holdningen skulle fort endre seg. For la det være sagt: Uten godt underbygde budsjettnotat om nytten av EDB i justissektoren fra Høyer og Harvold – notat som vi brakte med oss til enhver relevant budsjettsamtale med Finansdepartementet, ville Planseksjonens ambisiøse utviklingsprosjekt fort kunne ende opp som en stor flopp.

Og la meg tillegge. I denne budsjettkritiske perioden for Planseksjonen hadde jeg for min del også

stor glede av mine få, men nyttige rettsinformatikk-samtaler med professoren Jon Bing³. Det hadde seg nemlig slik at han i 1975 tok kontakt med meg i forbindelse med min statsvitenskapelige hovedoppgave om «Bruk av automatisert kriterievekting under tildeling av selektive tilskuddsordninger – Bostøtten.» Professoren fant tydeligvis noe av interesse i min hovedoppgave. At Jon Bing også på den tiden hadde nær kontakt og faglig samarbeid med Harvold og Høyer ble jeg da også klar over.

I sum kan man vel si det slik at Planseksjonens faglig innrettede pionerarbeid når det gjaldt utvikling og anvendelse av rettsinformatikk og EDB i justissektoren var ført an av særlig tre nøkkelpersoner: Jon B. Høyer, Trygve Harvold, og professor Jon Bing fra Universitetet i Oslo som inspirator og ekstern mentor.

I tillegg må direktør Kåre Fløisand i Statens rasjonaliseringsdirektorat nevnes. Han sto helt sentralt når det gjaldt utviklingen av statens EDB-arbeid på den tiden. Fløisand var dessuten en av driverne bak institusjonsbyggingen for Lovdata og Tinglysingsdata. [min utheving]

Prøveprosjektet med EDB i Tinglysingen, i Oslo og på Strømmen ble på mange måter selve flaggskipet til Planseksjonen under de første årene. Rettsinformatikkens mulighetsrom i justisforvaltningen, med Høyer og Harvold i spissen, ble på mange måter seksjonens ansikt utad, godt hjulpet av våre eksterne og institusjonelle samarbeidspartnere, Statens driftssentral,

Televerket og Statens Rasjonaliseringsdirektoratet.

Her slutter saga om Planseksjonen

Høsten 1981 ble Justisdepartementets administrative avdeling delt. Planseksjon som til da lå under Justisdepartementets Administrasjonsavdelingen, ble skilt ut og utvidet til å bli en ny Plan- og administrasjonsavdeling. Den gamle Administrasjonsavdelingen skiftet navn til Sivilavdelingen.

Utover i 80 årene hadde jeg for min del stor glede av å følge den videre utvikling av både Tinglysingsprosjektet, Løsøreprosjektet og Lovdata-prosjekt som foregikk, i regi av den nye Plan- og administrasjonsavdelingen.

Mye av nybrottsarbeidet var på plass i da jeg overtok som ekspedisjonssjef i Plan- og administrasjonsavdelingen etter Hjalmar Austbø. Da var flere statsrådsskifter skjedd etter Inger Louise Valle. For min del hadde jeg Høyre-statsråd Mona Røkke som min første, og øverste politiske sjef da jeg ble utnevnt til ekspedisjonssjef i Justisdepartementet i 1986.

Oystein Blymke, er Cand.polit. fra UiO i 1975 og ekspedisjonssjef i Justisdepartementet f.o.m. 1986–1994 og fra 2001–2016.

Kilder:

Tore Grønlie: «Sentraladministrasjonens historie etter 1945 Ekspansjonsbyråkratiets tid 1945–1980» Kapittel 12: 1970 årene Byråkrati eller demokrati «Den ny-radikale forvaltningspolitikken» (Fagbokforlaget 2009)

Inger Louise Valle: «Dette står jeg for» Gyldendal 1989

Trygve Harvold: Lov & Data nr. 161 1/2025 Artikkel 1 «Planseksjonens historie».

Ole Kolsrud: Rekonstruksjon og reform. Regjeringskontorene 1945–2005.

3 Jon Bing (1944–2014) var en norsk forfatter, dr. juris og professor ved Senter for rettsinformatikk ved Institutt for privatrett, Det juridiske fakultet, Universitetet i Oslo. Bing ble regnet som en foregangsman innenfor internasjonal rettsinformatikk. Han var æresdoktor ved Stockholms universitet og Københavns Universitet, og Visiting Professor ved King's College, University of London.

NIS2:

Hvilke konkrete sikkerhetskrav gjelder?

Del 2 i artikkelserien om cybersikkerhet og NIS2

Av Kristian Foss og Christer Berg Johannesen

NIS2-direktivet (Network and Information Systems) er en oppdatert versjon av NIS-direktivet fra 2016 som ble etablert for å styrke cybersikkerhet og motstandskraften til nettverks- og informasjonssystemer i EØS. Artikkel 21 i NIS2-direktivet stiller krav til sikkerhetstiltak som må iverksettes av tilbydere av tjenester som er essensielle og viktige for våre samfunnsfunksjoner.



Kristian Foss



Christer Berg Johannesen

Innledning

I del 1 av artikkelserien *NIS2: Hvilke virksomheter og leveranser vil omfattes av fremtidens krav til cybersikkerhet infrastruktur?* om NIS2 tok vi for oss hvilke virksomheter og leveranser som omfattes av direktivet. I denne del 2 av serien går vi inn på hvilke sikkerhetskrav direktivet stiller, og konkrete forslag til tiltak som offentlige og private virksomheter kan iverksette for å oppfylle kravene.¹

Målgruppen for artikkelen er alle som berøres av NIS2, men særlig jurister, sikkerhetsledere og IT- og OT-ansvarlige som ikke nødvendigvis har teknisk bakgrunn, men som likevel har ansvar for organisasjonens cybersikkerhet.²

NIS2 artikkel 21 stiller sikkerhetskravene

Formålet med NIS2 er at virksomheten iverksetter tiltak som fungerer i praksis og at disse kan dokumenteres. Etterlevelse forutsetter mer enn teknologi: Også forankring i ledelsen, risikoforståelse og en systematisk tilnærming.

NIS2 bygger på et «alle-farer»-prinsipp. Det innebærer at tiltakene som innføres må ta høyde for trusler fra flere hold, både fysiske og logiske. NIS2 art. 21 (2) leser:

*«The measures referred to in paragraph 1 shall be based on an **all-hazards approach** that aims to protect **network and information systems and the physical environment** of those systems from incidents, and shall include **at least the following:**» [vår utheving]*

Uttrykket «at least» betyr at et selskap kan være forpliktet til å iverksette andre og flere tiltak enn de som er listet opp i art. 21 (2), hvis det er nødvendig for å møte «alle farer» og for å «forhindre eller mini-

mere virkningen av hendelser på mottakere av deres tjenester og andre tjenester.», som det heter i artikkel 21 (1).

For eksempel, hvis uavbrutt elektrisk strøm er nødvendig for å forhindre et cyberangrep eller fysisk angrep på et produksjonsanlegg, kan virksomheten måtte installere reservestrom, via redundant tilkobling eller generator.

” Uttrykket «at least» betyr at et selskap kan være forpliktet til å iverksette andre og flere tiltak enn de som er listet opp i art. 21 (2).

Risikovurder for å forstå

For å forstå hvilke farer som finnes og hvor alvorlige de er, skal slike scenarier kartlegges i risikoanalysefasen. En slik risikoanalyse skal kunne ut i en tiltaksplan som sørger for at tiltakene blir forholds-

1 Siden direktivet ikke enda er implementert i norsk rett (eller høringsnotatet publisert), vet vi ikke hvordan kravene vil se ut for Norges del. Men fordi NIS2 er et minimumsdirektiv, skal ikke kravene bli lavere enn det som følger av direktivet.

2 OT: Operasjonell teknologi.

sige i forhold til risikoen. Denne risikobaserte tilnærmingen er formulert slik i NIS art. 21 (1):

*«Member States shall ensure that essential and important entities take **appropriate and proportionate** technical, operational and organisational measures to manage the risks **posed to the security of network and information systems** which those entities use for their operations or for the provision of their services, and to **prevent or minimise the impact** of incidents on recipients of their services and on other services.» [vår utheving]*

Minimumstiltakene som skal iverksettes i henhold til NIS2 art. 21 (2) fremgår av en liste på 10 tiltak eller grupper av tiltak. De fleste tiltakene har til felles at de ikke er konkrete nok til at normale virksomheter forstår hva de skal gjøre. Etter oppsummeringen konkretiserer vi kravene.

Kravene oppsummert

Sikkerhetskravene som artikkel 21 (2) fastsetter, inkluderer blant annet:

- **Risikovurdering og styring:** Virksomheter må gjennomføre regelmessige risikovurderinger for å identifisere potensielle sikkerhetstrusler og svakheter i nettverks- og informasjonssystemer.
- **Beskyttelse:** Tiltak må iverksettes for å beskytte nettverks- og informasjonssystemer mot uautorisert tilgang, endringer, tap, skade eller ødeleggelse.
- **Oppdagelse:** Organisasjoner må ha mekanismer for å oppdage og analysere sikkerhetshendelser og trusler.
- **Respons og gjenopprettelse:** Tiltak må være på plass for å reagere på sikkerhetshendelser og gjenopprette systemer til normal drift.
- **Sikkerhetsbevissthet og opplæring:** Ansatte må være opplært i cybersikkerhet og infor-

mert om beste praksis for å minimere risiko.

I tillegg inneholder NIS2 krav til rapportering o.a. ikke direkte sikkerhetsrelaterte krav, som vi ikke går inn på nå.

Tiltakene skal som nevnt bygge på en helhetlig risikobasert tilnærming og stå i forhold til virksomhetens eksponering og samfunnskritikalitet. Dette må man ha i bakhodet når man vurderer de 10 tiltakspunktene, som gjelder både essensielle og viktige virksomheter:

Konkrete krav og etterlevelse

Følgende mer eller mindre konkrete minimumskrav for sikkerhet angis i NIS2 art. 21 (2), forsøksvis konkretisert av oss:

Bokstav a – Risikoanalyse og sikkerhetspolicyer

«policies on risk analysis and information system security;»

Virksomheter som omfattes av NIS2-direktivet, plikter å gjennomføre en grundig og regelmessig vurdering av risikoene som kan true informasjonssystemene sine. Vurderingen bør omfatte både ytre og indre trusler, tekniske og organisatoriske sårbarheter, samt mulige konsekvenser for virksomheten og samfunnet ved bortfall av tjenester. Herunder bør virksomheten utarbeide og holde oppdatert en overordnet sikkerhetspolicy som tydelig fastsetter hvordan risiko håndteres.

” Vurderingen bør omfatte både ytre og indre trusler, tekniske og organisatoriske sårbarheter, samt mulige konsekvenser for virksomheten og samfunnet ved bortfall av tjenester.

Et sentralt prinsipp er at sikkerhetstiltak må justeres fortløpende i takt med endringen av trusselbildet. Prinsippet innebærer at virksomheter ikke kan stole på tidligere vurderinger, men må sørge for kontinuerlig forbedring og tilpasning av sikkerhetsarbeidet, i tråd med beste praksis og aktuelle trusselvurderinger.

Krav:

- Minst én risikovurdering per år.
- Oppdatert og virksomhetstilpasset sikkerhetsrutine.

Mål:

- Sikre at virksomheten har et oppdatert risikobilde og et dokumentert styringssystem for informasjonssikkerhet.

Mulige tiltak:

- Benytt anerkjente rammeverk som:
 - ISO/IEC 27001
 - NSMs grunnprinsipper
 - CIS Controls
- Dokumenter sikkerhetsmål, roller, ansvar og styringsstrukturer.
- Innhent og bruk trusselvurderinger fra NorCERT, ENISA og/eller egne tjenesteleverandører.
- Etabler rutiner for å revidere og oppdatere sikkerhetsrutiner ved vesentlige endringer i trusselbildet.
- Sørg for ledelsesforankring og godkjenning av rutiner og risikovurderinger.

Bokstav b – Hendelseshåndtering

«incident handling»

Artikkel 21 (2) bokstav b krever at virksomheter skal ha etablerte og dokumenterte planer for håndtering av sikkerhetshendelser. Formålet er å sikre at organisasjonen raskt og effektivt kan identifisere, håndtere og begrense konsekvensene av digitale angrep og alvorlige sikkerhetsbrudd.

Evnen til effektiv hendelseshåndtering forutsetter tydelig definerte roller og ansvar, både internt og med eventuelle eksterne partnere, samt at rutinene jevnlig testes og forbedres. Dette gir virksomheten evne til å handle målrettet ved en hendelse, og sørger for at nødvendige varsler og tiltak kan iverksettes uten unødig forsinkelse.

Sentralt står også samhandling med relevante myndigheter, som Nasjonal sikkerhetsmyndighet, (NSM, ved NorCERT) eller de respektive sektors CERT, f.eks. HelseCERT (helsesektoren), FinansCERT (finanssektoren) og KraftCERT (energisektoren).³ I tillegg må virksomhetene ha beredskap for å aktivere støtte fra eksterne eksperter.

Mulige krav:

- Utarbeid og dokumenter hendelseshåndteringsplan.
- Klare ansvarsforhold og varsling til relevante myndigheter.
- Øvelser og kontinuerlig forbedring.

Mål:

- Rask respons og minimal skade ved sikkerhetshendelser.
- Samordnet innsats internt og eksternt.
- Overholdelse av varslingsplikt i henhold til NIS2 (og eventuelle andre regelverk).

Mulige tiltak:

- Etabler interne og eksterne varslingsrutiner (til NSM, SektorCERT, o.l.).
- Forhåndsavtale med leverandører av DFIR/IR-tjenester.

3 CERT: Computer Emergency Response Team – Team for å lede og ivareta håndtering av hendelser.

- Implementer bruk av verktøy for EDR⁴ / XDR⁵, SIEM⁶, o.l. for å sikre tidlig varsling og respons.

Bokstav c – Beredskap

«business continuity, such as backup management and disaster recovery, and crisis management;»

Virksomheter må sikre at sin evne til å fortsette driften ved alvorlige hendelser ikke svekkes (for mye). Kravet innebærer å ha en tydelig beredskapsplan som dekker hvordan man skal håndtere alvorlige avbrudd forårsaket av for eksempel cyberangrep, naturkatastrofer eller tekniske feil som rammer datasentre, nettverk eller andre kritiske systemer. Løsningene for sikkerhetskopiering og gjenopprettelse bør være dokumenterte og testede. Strukturen bør sikre at tjenestene kan opprettholdes eller gjenopptas innen akseptabel tid.

Mulige krav:

- Etablerte og vedlikeholdte planer for beredskap (BCP⁷), og/eller
- Katastrofeberedskap (DRP⁸), samt
- Sikkerhetskopieringsmekanismer som testes regelmessig.

- 4 Endpoint Detection and Response – System for å detektere avvik på endepunkter (server, arbeidsstasjon, mobile enheter, o.l.)
- 5 Extended Detection and Response – System for å oppdage avvik på endepunkter, men som i tillegg kan avdekke mer komplekse angrep gjennom utvidet bruk av automasjon og korrelasjon av data fra ulike kilder.
- 6 Security Information and Event Management – System for å samle og analysere logger og hendelser på tvers av hele IT-miljøet.
- 7 Business Continuity Plan – Plan for å sikre videreføring av kritiske forretningsprosesser under/etter hendelser.
- 8 Disaster Recovery Plan – Plan for å gjenopprette IT-systemer og data etter *store* hendelser / systemsammenbrudd.

Mål:

- Sikre at virksomheten raskt kan gjenoppta tjenester og beskytte kritisk informasjon ved hendelser som truer driften.

Mulige tiltak:

- Etabler og vedlikeholdsplaner for forretningskontinuitet og gjenopprettelse, med tydelige roller og prosesser.
- Test planene jevnlig gjennom simulerte scenarioer (for eksempel løsepengeangrep eller tap av sentrale dataressurser). Det vil si; hold øvelser regelmessig.
- Bruk offline sikkerhetskopier og sikre «immutability»⁹, sikret med flerfaktoraутentisering (MFA).
- Sikre redundans i kritisk infrastruktur, inkludert strøm, nettverk og tjenester.
- Gjennomfør regelmessig revisjon av gjenopprettelsesprosesser.

Konkret hva som er riktig for den enkelte virksomhet, avhenger av den risikoen som er avdekket.

Bokstav d –

Leverandørkjedesikkerhet

«supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers»

Leverandørkjeder er kritiske og sårbare. Kjedene er i dag ofte lange og man er avhengig av at de fungerer, gjerne i sanntid. Derfor må også leverandører virksomhetene er avhengige av for sin drift også etterleve relevante sikkerhetskrav. Typiske eksempler er ved utsetting av tjenester (outsourcing) eller ved bruk av skyløsninger og programvare levert som tjeneste (SaaS).

9 Oversatt betyr ordet «udødelighet», og betyr i denne sammenheng at data ikke kan slettes, selv ikke av administrator, og at der finnes «ekte» slettebeskyttelse.

Bestemmelsen angir bare ‘direkte leverandører’, men kravet utgjør bare et gulv - et minimumskrav – på grunn av formuleringen «at least». Sikring flere nivåer ned kan være påkrevet om en riktig risikovurdering tilsier det. Kravet betyr at virksomheten må ta et aktivt ansvar for sikkerheten så langt ned i leverandørkjeden som nødvendig, så lenge underleverandørene kan påvirke virksomhetens evne til å forebygge, oppdage eller håndtere sikkerhetshendelser.

” Kjedene er i dag ofte lange og man er avhengig av at de fungerer, gjerne i sanntid.

For å etterleve kravet må virksomheten etablere klare krav og kontroller i avtaler, og den må jevnlig følge opp og vurdere sikkerhetsnivået hos leverandørene.

Mulige krav:

- Oversikt over alle kritiske (og viktig) leverandører.
- Dokumenterte sikkerhetskrav i kontrakter og SLA-er.
- Jevnlig vurdering og kontroll av leverandørenes sikkerhetsnivå.

Mål:

- Redusere risiko for sikkerhetsbrudd forårsaket av tredjepart.
- Sikre at eksterne aktører ikke svekker virksomhetens drift.
- Etablere sporbarhet og ansvarlighet i leverandørkjeden.

Mulige tiltak:

- Kartlegg og klassifiser alle kritiske leverandører (for eksempel innen drift, IaaS¹⁰, maskinvare og programvare).
- Inkluder eksplisitte sikkerhetskrav i avtaler, med referanser til anerkjente standarder.

- Still krav om revisjoner, sikkerhetssertifiseringer og rapporter (som SOC 2 Type II eller tilsvarende) i avtaler og ved anskaffelser.

Bokstav e – Sikkerhet ved anskaffelser, utvikling og vedlikehold

«security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;»

Bestemmelsen stiller krav til at innkjøp, utvikling og vedlikehold av nettverks- og informasjonssystemer ivaretar informasjonssikkerhet fra starten av og gjennom hele livssyklusen til systemet. Dermed må man planlegge anskaffelsen og utviklingen, og stille tydelig krav før handelen skjer. Samtidig bør man sikre at vedlikeholdet opprettholder sikkerhet over tid. I praksis bør vedlikeholdsavtalen inngås før anskaffelsen eller utvikling avtales. En slik helhetlig tilnærming vil normalt også gi det beste kommersielle resultatet også, siden leverandøren da normalt vil være i en konkurransesituasjon.

Mulige krav:

- Etterlevelse av prinsipper for «innebygget sikkerhet» («security by design»).
- Gjennomgang av kildekode og testing for kjente sårbarheter (SAST/DAST).
- Virksomheten skal ha rutiner for sikker oppdatering, versjonskontroll og håndtering av sårbarheter.

Mål:

- Redusere risiko for sikkerhetshull og kompromittering via programvare.
- Sikre at systemer som tas i bruk, er vurdert for sikkerhet før implementering.

- Opprettholde tillit til digitale løsninger gjennom kontrollert vedlikehold.

Mulige tiltak:

- Innfør tydelige anskaffelseskrav som inkluderer sikkerhetsvurderinger og standarder.
- Still krav om regelmessig sårbarhetstesting og innsyn i kildekode ved behov.
- Etabler faste prosedyrer for sikker programvareoppdatering («patching») og sporbar versjonshåndtering.

Bokstav f – Cybersikkerhetsstyring, prosedyrer og vurdering av effektivitet

«policies and procedures to assess the effectiveness of cybersecurity risk-management measures;»

Virksomheter som er underlagt NIS2-direktivet skal etablere formelle styringssystemer og prosedyrer for cybersikkerhet, for å vurdere virkningen av sikkerhetstiltakene. Prosessen vil tvinge virksomheten til å tenke igjennom hvordan den arbeider med sikkerhet, og samtidig dokumentere innsatsen.

Mulige krav:

- Formaliserte rutiner og retningslinjer for cybersikkerhet.
- Ledelsesforankring og regelmessig rapportering.
- Etterprøvbare prosedyrer og kontinuerlig forbedring.

Mål:

- Integrere cybersikkerhet i virksomhetens styringsmodell.
- Sikre kontinuitet, sporbarhet og ansvarlighet i sikkerhetsarbeidet.
- Redusere risiko gjennom helhetlig kontroll og styring.

Mulige tiltak:

- Etablering av et ISMS (Information Security Management System).

¹⁰ Infrastructure as a Service - Infrastruktur levert som en tjeneste, f.eks. via en skyløsning.

- Bruk av GRC-verktøy (styring, risiko og etterlevelse).¹¹
- Gjennomføre interne revisjoner og gjennomgang med ledelsen.
- Bruke rådgivere for å etablere et godt system.

Bokstav g – Cyberhygiene og opplæring

«basic cyber hygiene practices and cybersecurity trainings»

Fortalen til NIS2 nevner følgende eksempler på grunnleggende sikkerhet:¹²

- Zero-trust-prinsipper,¹³
- programvareoppdatering,
- enhetskonfigurasjon,
- nettverkssegmentering,
- identitet og tilgangsstyring, og
- brukerbevisstgjøring, og opplæring av personellet sitt om [...] cybertrusler.

Virksomheten skal videre vurdere egne cybersikkerhetsevner, og sikkerhetsteknologi, herunder kunstig intelligens og maskinlæring for å bedre sine evner og sikkerhet i nettverk og informasjonssystemer.

” Virksomheten skal videre vurdere egne cybersikkerhetsevner.

Standarder som NSMs grunnprinsipper for IKT-sikkerhet vil beskrive flere grunnleggende sikkerhetspraksiser. Slik sett kan bok-

stav g) ses på som en bunnpanne, som tilpasses konkret risiko.¹⁴

Mulige krav:

- Som listet opp over fra fortalen.
- Relevante sikkerhetsstandarder for den aktuelle virksomhetstypen.
- Dokumentasjon av gjennomførte tiltak.

Mål:

- God grunnleggende sikkerhet.
- Øke ansattes evne til å gjenkjenne og håndtere trusler som sosial manipulasjon og phishing.
- Forhindre at enkle feil eller ubekjente handlinger fører til alvorlige hendelser.
- Integrere sikkerhetstenkning i daglige arbeidsrutiner.

Mulige tiltak:

- Bruk passordrutiner, multifaktorautentisering (MFA), oppdatert antivirus og klientkontroll.
- Gjennomfør opplæring i sosial manipulering, phishing og digital adferd.
- Simuler angrep
- Gjennomfør praktisk bevissthetsopplæring for å styrke kompetanse og overvåkenhet.
- Bruk av konfigurasjonsverktøy og systemer for automasjon, f. eks. IaC, systemer for digital sikkerhetsetterlevelse («sikkerhetsbaseline»), sikker distribusjon og versjonskontroll, sikker programvareforsyningskjede (herunder også leverandørkon-

troll og tredjepartsstyring¹⁵), samt kontinuerlig systemovervåking og sikring av dataintegritet.¹⁶

- Ivareta prinsipper for «security by design» og «security by default» i alle leveranser.
- Verifiser og valider komponenter for driftsetting.

Bokstav h – Rutiner for kryptering og databeskyttelse

«policies and procedures regarding the use of cryptography and, where appropriate, encryption»

Større virksomheter bør etablere rutiner og prosedyrer for bruk av kryptografi og kryptering. Igjen vil arbeidet med dette bevisstgjøre virksomhetene ved fastsettelse av krav og valg av løsning. Hvordan rutinene vil se ut, vil avhenge av utfallet av risikovurderingen.

” Igjen vil arbeidet med dette bevisstgjøre virksomhetene ved fastsettelse av krav og valg av løsning.

Mulige innhold i rutinen:

- Data bør krypteres med minst 256-bits både under lagring og under overføring.¹⁷
- Krav til type teknologi, kildeland og leverandør.
- Hvordan nøkkelhåndtering skal skje (for eksempel bør den pri-

11 Fra engelsk: Governance, risk & compliance.

12 Fortalepunkt 89

13 Zero-trust-prinsipper betyr at ingen brukere, enheter eller systemer får tillit uten verifisering – uansett om de er inne eller utenfor virksomhetens nettverk eller systeminfrastruktur.

14 Se også erfaringsrapporten «Ti sårbarheter i norske IKT-systemer» fra NSM: <https://nsm.no/getfile.php/1313387-1700026023/NSM/Filer/Dokumenter/Rapporter/Ti%20s%C3%A5rbarheter%20i%20norske%20IKT-systemer.pdf>

15 Tredjepartsstyring, ofte forkortet til TPRM (Third-Party Risk Management), er en systematisk prosess for å identifisere, vurdere, overvåke og redusere risiko knyttet til eksterne leverandører, underleverandører og partnere.

16 Infrastructure as Code – En metode hvor infrastruktur konfigureres og administreres ved hjelp av «kode», i stedet for manuelle prosesser.

17 AES.256 er mye brukt.

vate nøkkelen være i Norge under kontroll av virksomheten).

Mål:

- Sikre sikker, effektiv og konsistent bruk av kryptering for å forhindre uautorisert tilgang og datalekkasjer.
- Sikre pålitelig og sikker behandling av informasjon.
- Etablere tillit hos kunder og samarbeidspartnere.

Tiltak:

- Utarbeide rutine med prosedyre for kryptering.
- Hente inn bistand fra spesialister.
- Bruke sikre nøkkelhåndterings-systemer, fortrinnsvis HSM (Hardware Security Modules).

Bokstav i – Styring og administrasjon eiendeler, personell og tilganger

«human resources security, access control policies and asset management»

Bokstav i) griper fatt i tre forhold som i praksis kan være avgjørende for sikkerheten:

- a. personer,
- b. tilgangskontroll og
- c. aktivakontroll.

Menneskelige feil er en betydelig årsak til sikkerhetsbrudd. Hele 95 % av sikkerhetsbrudd involverer menneskelige feil, inkludert innsidetrusler, feil bruk av legitimasjon og brukerrelaterte feil. Av disse er et flertall forårsaket av manglende kunnskap og overvåkenhet. Ifølge en studie fra Stanford University og Tessian, skyldes 88% av brudd på datasikkerheten ansattfeil (dvs. «interne» årsaker). Enkelte brudd er forårsaket av uærlige eller kriminelle medarbeidere, som misbruker privilegier (tilgangsrettigheter), bruker stjålet legitimasjon eller benytter sosial manipulasjon for å oppnå tilgang.

Av den grunn viser fortalen i NIS2 til at personellsikkerhetstiltakene skal være i samsvar med direktiv for motstandsdyktighet i kritiske enheter (CER).^{18 19} CER regulerer sikkerhetskrav for en rekke av virksomhetene omfattet av NIS2, men med fysisk fokus. CER er enda ikke implementert i norsk lov.

Det fremgår en rekke krav av CER. Et av de praktisk viktigste er muligheten for å bakgrunnskontrollere ansatte. I dag er muligheten til å kreve politiattest begrenset. Med CER, og NIS2, er det grunn til å vente seg at kretsen utvides vesentlig. Virksomheter som er opptatt av bedre kontroll ved ansettelser, kan vurdere å avgi en høringsuttalelse ved implementering av NIS2 og CER i norsk lov.

For å ha sikre systemer må man videre vite hva man har av eiendeler (aktiva) og hvilke tilganger disse har. Også for tilgangskontroll viser fortalen i NIS2 til CER. CER art. 13 never en rekke tiltak, som å hindre hendelser fra å inntre, iverksette passende fysisk sikkerhet og gjenopprettelse. Som for mange av tiltakene angitt i NIS2 gir dette begrenset veiledning.

18 Critical Entities Resilience Directive (CER), Directive (EU) 2022/2557. https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng#enc_1

19 NIS2 fortale punkt77 «[...] The cybersecurity risk-management measures should therefore also address the physical and environmental security of network and information systems by including measures to protect such systems from system failures, human error, malicious acts or natural phenomena, in line with European and international standards, such as those included in the ISO/IEC 27000 series. In that regard, essential and important entities should, as part of their cybersecurity risk-management measures, also address human resources security and have in place appropriate access control policies. Those measures should be consistent with Directive (EU) 2022/2557 [CER]».(våre uthevinger)

Mulige krav:

- Tilgang til systemer skal være basert på rollen medarbeideren fyller og nødvendighet (minste privilegium, som betyr at man ikke skal ha mer tilgangsprivilegier enn nødvendig for å gjøre jobben).
- Rutiner for tilgang til systemer ved tiltredelse, endring av rolle og fratredelse skal finnes.
- Tilgangsrettigheter skal kontrolleres og revideres jevnlig.

Mål:

- Forhindre uautorisert tilgang til systemer og data.
- Redusere risiko ved interne trusler og feil.
- Sørge for sporbarhet og etterlevelse.

Mulige tiltak:

- Implementer rollebasert tilgangskontroll (RBAC²⁰) og IAM²¹-verktøy for tilgangsstyring.
- Gjennomføre periodisk revisjon av tilganger og overvåk brukeratferd.
- Gjøre bakgrunnskontroll ved nyansettelser eller endringer til sensitive stillinger (så langt loven tillater).
- Implementere rutiner for hendelseshåndtering.
- Etablere klar offboarding-prosedyre inkludert fysisk adgangskontroll.
- Bevisstgjør innehavere av ansvarlige roller om kravene.

Bokstav j – MFA og sikker kommunikasjon

«the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications»

- 20 Role-Based Access Control – Rollebasert tilgangskontroll, som betyr at brukere får tilgang til systemer og data basert på rollen sin i organisasjonen.
- 21 Identity and Access Management – System for styring av identitet og tilgang.



and secured emergency communication systems within the entity, where appropriate.»

Det siste kravet i art. 21 (2) er det mest konkrete, men likevel tillagt en skjønnsmessig vurdering – ‘der passende’.

I korthet skal virksomhetene ha:

- flerfaktor-autentisering ELLER
- kontinuerlige autentiseringsløsninger,
- sikret stemme, video og tekstkommunikasjon og
- sikre nødkommunikasjonssystemer i virksomheten, når det er passende.

Det vil si at *flerfaktorautentisering* overraskende nok ikke er et krav om man har ‘*kontinuerlige autentiseringsløsninger*’ (KA). Hva KA er fremgår ikke av NIS2, men er normalt ment å omfatte en dynamisk prosess som:

- Overvåker brukerens identitet gjennom hele økten – ikke bare ved innlogging.
- Vurderer risikofaktorer som:
 - Brukeratferd (f.eks. taste- og musemønstre, navigasjonsvaner)
 - Enhetens tilstand (f.eks. operativsystemoppdateringer, forekomst av skadevare)
 - Geografisk plassering (f.eks. uventet tilgang fra ukjente områder)

- Automatisk utløser ny autentisering eller avslutter økten dersom det oppdages avvik.

Denne tilnærmingen støtter Zero Trust-prinsippet: «Aldri stol på, alltid verifiser».

Det fremgår ikke klart om de øvrige kravene er alternative, eller om de må oppfylles ved siden av kryptering eller kontinuerlig autentisering. Vi legger til sikret stemme-, video- og tekstkommunikasjon og sikre nødkommunikasjonssystemer er krav, men også dette bør klargjøres i den norske implementeringen av direktivet.

Sikker kommunikasjon vil i dag typisk bety kryptert forbindelse. Dermed glir kravene over i hverandre. Dette betyr at virksomheter ikke bare må sørge for at forbindelser er krypterte, men også at autentiseringsmekanismer – enten det benyttes flerfaktor eller kontinuerlig autentisering – understøtter en helhetlig sikkerhetsstrategi. Autentisering og kommunikasjon kan dermed ikke vurderes isolert. Det må etableres mekanismer som sikrer at både identitet og datatrafikk valideres og beskyttes fortløpende – ikke kun ved øktens start.

Særlig viktig er sikker kommunikasjon ved fjerntilgang og bruk av tredjepartsleverandører, der risikoen for identitetstyveri og sesjonskapring er betydelig høyere enn ved lokal tilgang. NIS2 krever at slike risi-

koer håndteres gjennom tekniske og organisatoriske tiltak, og her gir kontinuerlig autentisering et mulig svar. Det er imidlertid avgjørende at virksomheten kan dokumentere på hvilken måte autentiseringen faktisk er «kontinuerlig», og hvordan den er koblet til sikker kommunikasjon – f.eks. ved automatisk frakobling ved avvik, eller adaptiv innstramming av tilgangsnivå ved endrede risikoforhold.

Nødkommunikasjon kan også være et krav. Om normale kommunikasjonssystemer bryter sammen, kan slike reservesystemer bli avgjørende.

Mulige krav:

- Identitet må bekreftes gjennom sikre autentiseringsløsninger.
- Kommunikasjon må beskyttes mot avlytting og endringer.
- Tiltakene må være dokumenterte og etterprøvbare.

Mål:

- Hindre uautorisert tilgang til viktige systemer og data.
- Sikre pålitelig og fortrolig kommunikasjon i drift og krise.
- Øke tilliten og evnen til virksomhetens til å fortsette å levere sine tjenester.

Mulige tiltak:

- Innfør flerfaktorautentisering (MFA) for alle brukere med tilgang til sensitive systemer.

- Innfør KA for å sikre løpende kontroll og autentisering, helst i kombinasjon med MFA.
- Krypter samtaler, fildeling, chat og andre viktige data.
- Etabler krisekommunikasjonskanaler.

Dokumentasjon og etterprøvnbarhet

NIS2 krever ikke bare tiltak, men at man dokumenterer dem og kan demonstrere etterlevelse overfor tilsynsmyndigheter (art. 21 (2) a)). For at risikostyringen skal være passende og risikotilpasset slik NIS2 krever, bør virksomheten legge til grunn at dokumentasjonen skal være:

- Oppdatert.
- Tilgjengelig.
- Strukturert (f.eks. i et ISMS).

Eksempler på dokumentasjon:

- Risikoanalyser og trusselvurderinger.

- Sikkerhetsrutiner og prosedyrer.
- Hendelseslogger og revisjonslogger.
- Kontrakter med sikkerhetskrav.
- Referater fra øvelser og opplæring.

Hvordan komme i gang?

En reise begynner alltid med det første steget. Vi anbefaler disse:

1. **Forankring:** Styret og ledelsen må involveres og forstå risikoen. Utarbeid et white-paper eller lignende og/eller presenter problemstillingen i styremøter.
2. **Kartlegging:** Identifiser kritiske systemer, leverandører og data. Dokumenter egnet sted.
3. **Risikovurdering:** Gjennomfør årlig risikovurdering og GAP-analyse mot NIS2.
4. **Planlegge tiltak:** Lag en prioritierungsliste over hva som må på plass. Koordiner med andre regelverk.

5. **Iverksettelse:** Implementer tiltak og oppdater rutiner.
6. **Testing og forbedring:** Test planer, øv, og oppdater planer og systemer jevnlig.

NIS2 stiller omfattende krav til sikkerhet, men gir samtidig virksomhetene handlingsrom til å tilpasse tiltak etter risiko og størrelse. Din jobb blir å finne riktig nivå og vise at du har gjennomført nødvendige tiltak.

Neste artikkel i serien vil handle om *personlig ansvar, sanksjoner* og *styreansvar* ved manglende etterlevelse.

Ta kontakt med forfatterne om du har spørsmål.

Advokat Kristian Foss, BULL Advokatfirma og cybersikkerhetsekspert Christen Berg Johannesen – rådgiver og spesialist i cybersikkerhet, dataetterforskning og hendelsesbåndtering, Conscia Norge AS.

Hva sier forslaget til ny forvaltningslov om samtykkebasert deling?

Av Steinar Skagemo

I forrige utgave av Lov & Data skrev jeg om samtykkebasert deling av data. Jeg forsøkte å få frem hvordan samtykke sikrer involvering av personen som opplysningene gjelder, og at denne involveringen fungerer som en sikkerhetsmekanisme som reduserer risikoen for at opplysningene kommer på avveie. Dette er i kontrast til lovhjemmelbasert deling der utro tjenere hos mottakeretaten, eller et vellykket hackerangrep, kan gi uautorisert tilgang til opplysninger hos avgiveretaten. Hjemmelen for samtykkebasert deling er forvaltningslovens § 13a nr. 1, som sier at taushetsplikt ikke er til hinder for at «opplysninger gjøres kjent for dem som de direkte gjelder, eller for andre i den grad de som har krav på taushet samtykker».

I artikkelen tok jeg også opp at det er stor usikkerhet om offentlige etater kan basere seg på samtykke for deling av data, ettersom personvernforordningen førte til en innstramming av myndighetenes bruk av samtykke som behandlingsgrunnlag. Denne innstramningen gjenspeiles i Datatilsynets veiledning om samtykke:

«I vurderingen av om et samtykke er frivillig, må man også se på styrkeforholdet mellom virksomheten og den enkelte. For eksempel vil normalt ikke offentlige myndigheter eller arbeidsgivere kunne bruke samtykke som behandlingsgrunnlag siden den enkelte er i et avhengighetsforhold til virksomheten.»¹

¹ Se: <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/om-behandlingsgrunnlag/samtykke/>



Steinar Skagemo

I artikkelen foreslo jeg to ulike måter å argumentere for at offentlige etater likevel er på trygg rettslig grunn ved bruk av samtykke til deling av data. Den gode nyheten er at mine forslag til argumentasjon ikke lenger er relevante. Problemstillingen ble nemlig nylig løst i Justis- og beredskapsdepartementets (JD) forslag til ny forvaltningslov, Prop. 79 L (2024–2025).²

Før jeg går videre til hva som står i lovforslaget om samtykke, vil jeg vise hvordan temaet har vært problematisert og diskutert i ulike høringer fra JD siden 2019.

I NOU 2019:5 la forvaltningslovutvalget frem sitt forslag til ny forvaltningslov. Utvalget mente at regelen i dagens fvl § 13a nr. 1 bur-

de videreføres.³ Samtidig påpekte de: «Ved utformingen av bestemmelsen må det imidlertid tas hensyn til at et samtykke til å dele personopplysninger må oppfylle vilkårene i personvernforordningen.»⁴ Med andre ord mente de at et samtykke til deling av personopplysninger etter forvaltningslovens regel samtidig måtte være et samtykke som lovlig behandlingsgrunnlag etter personvernforordningen. Videre skrev utvalget dengang: «Langt på vei er [vilkårene i personvernforordningen] krav som allerede fulgte av norsk rett, men det kan neppe utelukkes at kravene nå går noe lenger.»⁵ Derfor, for å unngå uklarhet, konkluderte forvaltningslovutvalget dengang: «For å unngå at kravene etter forvaltningsloven og personopplysningsloven blir forskjellige, bør kravene etter forvaltningsloven svare til kravene i forordningen.»⁶

Her oppstår det en selvmotsigelse: En lov som retter seg mot offentlige myndigheter skal ha krav til gyldig samtykke som svarer til vilkårene i en forordning der et viktig poeng er at offentlige myndigheter normalt ikke kan bruke samtykke.

Denne selvmotsigelsen ble heldigvis fanget opp av Viken fylkeskommune i JDs høring av NOU 2019:5. Viken fylkeskommune viste til Datatilsynets veiledning, jf. sitatet i innledningen, og advarte mot konsekvensene av forvaltningslovutvalgets forslag:

² Prop. 79 L (2024–2025) Lov om saksbehandlingen i offentlig forvaltning (forvaltningsloven) Tilråding fra Justis- og beredskapsdepartementet 4. april 2025, godkjent i statsråd samme dag. Se: <https://www.regjeringen.no/no/no/dokumenter/prop-79-l-20242025/id3094317/>

³ Kapittel 19.12.3, se: <https://www.regjeringen.no/no/dokumenter/nou-2019-5/id2632006/?ch=20#KAP19-12-3>

⁴ Samme som over

⁵ Samme som over

⁶ Samme som over

«Det er viktig å tenke gjennom om muligheten for å frita for taushetsplikten etter forvaltningsloven, bør forstås så restriktivt. Mye av den praksis et samtykke i dag brukes som grunnlag for, vil i så fall trolig ikke kunne videreføres.»⁷

Så, vinteren 2021, gjennomførte Justis- og beredskapsdepartementet en høring på utkast til veileder om taushetsplikt m.m.⁸ Denne veilederen skulle ikke innebære noen endring, bare en hjelp til å forstå gjeldende rett.

Videre står det blant annet om regelen i fvl § 13a nr. 1. Utkastet viser til forvaltningslovutvalget og påpeker at et samtykke etter fvl § 13a nr. 1 også må oppfylle kravene til samtykke i personvernforordningen. Samtidig står det senere:

«I noen tilfeller vil forvaltningen ha en maktposisjon overfor borgeren. Det er viktig at forvaltningen forvisser seg om at borgeren forstår at han eller hun har rett til å nekte å samtykke, og hvilke konsekvenser samtykket har.»⁹

Dette er et stort steg bort fra budskapet fra Datatilsynet, om at offentlige myndigheter normalt ikke kan bruke samtykke, og fremstår som paradoksalt når det samtidig er vist til forvaltningslovutvalget. Ut-

kastet inneholdt ingen nærmere begrunnelser for hvorfor den var såpass forskjellig fra Datatilsynets veileder om samtykke.¹⁰ Kravene til gyldig samtykke ble derfor et tema i flere av høringssvarene.

Brønnøysundregistrene etterlyste konkrete eksempler på hvordan man kan vurdere styrkeforholdet mellom myndighetene og individet, og stilte også spørsmål om det kunne være slik at frivillighetskravet var oppfylt dersom deling av opplysninger basert på samtykke ble tilbudt som et alternativ til at den registrerte sendte inn opplysningene selv.¹¹

Digitaliseringsdirektoratet, som på det tidspunktet hadde et ressursenter for deling av data som fokuserte på juridiske problemstillinger, skrev følgende:

«Når det gjelder bruk av samtykke i henhold til forvaltningsloven § 13 a nr. 1 ønsker Digdir å benytte anledningen til å påpeke at vi, gjennom utstrakt utadrettet virksomhet, har merket oss at det synes å være et tverrsektorielt behov hos offentlige virksomheter for nærmere veiledning

knyttet til bruk av samtykke i offentlig sektor.»¹²

Skattedirektoratet etterlyste også mer omtale av samtykke, med henvisning til at det foreligger særskilte krav til gyldig samtykke.¹³

Det er verdt å merke at utkastet til veilederen egentlig gikk langt i å bruke samtykke som en måte å redusere risikoen for å tolke andre regler for langt. I innledningen til kapitlet om når taushetsbelagt informasjon kan deles, står det et råd om å innhente samtykke, fremfor å bevege seg i grensene for det som tillates etter andre regler: *«I praksis kan det ofte være klokt å innhente samtykke, særlig hvis man er i tvil om man er nær grensen for hva slags informasjon man kan dele etter forvaltningslovens regler.»¹⁴*

Da den endelige versjonen av veilederen ble publisert 14. februar 2023, inneholdt den ingen grundigere oppklaring av problemstillingen eller eksempler til hjelp for å gjøre vurdering av styrkeforholdet, slik flere av høringsinstansene hadde bedt om. Tvert imot kan det sies at den ble enda mer forvirrende, fordi en formulering tilsvarende Datatilsynets veiledning om samtykke ble tatt inn i veilederens kapittel om personvernforordningen:

7 Høringssvar fra Viken fylkeskommune, 3. desember 2019, se: <https://www.regjeringen.no/no/dokumenter/horing---nou-2019-5-ny-forvaltningslov/id2652945/Download/?vedleggId=913456b2-7981-4acb-9311-66927e10821f>

8 Høring - utkast til veileder om taushetsplikt, opplysningsplikt og opplysningsrett i forvaltningen, 15. februar 2021. Se: <https://www.regjeringen.no/no/no/dokumenter/horing-utkast-til-veileder-om-taushetsplikt-opplysningsplikt-og-opplysningsrett-i-forvaltningen/id2834815/>

9 Utkast til veileder om taushetsplikt, opplysningsrett og opplysningsplikt ... Se: <https://www.regjeringen.no/contentassets/2f0aa4fc39004edba35b8027fe80be16/veileder-om-taushetsplikt-opplysningsrett-og-opplysningsplikt.pdf>

10 Utkastet til veileder inneholdt til gjengjeld en oppklaring om kravet til å kunne trekke tilbake samtykke, som noen mener gjør det umulig/vanskelig for offentlig sektor å bruke samtykke: «Et samtykke kan trekkes, men tilbaketrekkingen virker bare fremover. Hvis forvaltningen allerede har gitt opplysninger videre på grunnlag av samtykke, må det mottakende organet fortsatt kunne bruke de opplysningene det har fått. Tilbaketrekkingen av samtykket hindrer derimot at personer med taushetsplikt fortsetter å gi opplysninger på grunnlag av samtykket (hvis det ikke finnes andre grunnlag for å dele informasjonen).» Kilde: Samme som over.

11 Høringssvar fra Brønnøysundregistrene, 8. april 2021, se: <https://www.regjeringen.no/contentassets/f41a04d2237e43c3b512bd80053a8ede/annen-offentlig-etat/bronnøysundregistrene.pdf?uid=Br%C3%B8nn%C3%B8ysundregistrene>

12 Høringssvar fra Digitaliseringsdirektoratet, 12. april 2021, se: <https://www.regjeringen.no/no/dokumenter/horing-utkast-til-veileder-om-taushetsplikt-opplysningsplikt-og-opplysningsrett-i-forvaltningen/id2834815/?uid=3b7690c3-6ada-4613-aebf-88214b1e86d2>

13 Høringssvar fra Skattedirektoratet, 12. april 2021, se: <https://www.regjeringen.no/no/dokumenter/horing-utkast-til-veileder-om-taushetsplikt-opplysningsplikt-og-opplysningsrett-i-forvaltningen/id2834815/?uid=50ac613a-a83a-4f6f-b801-21b31629c521>

14 Utkast til veileder om taushetsplikt, opplysningsrett og opplysningsplikt ... Se: <https://www.regjeringen.no/contentassets/2f0aa4fc39004edba35b8027fe80be16/veileder-om-taushetsplikt-opplysningsrett-og-opplysningsplikt.pdf>

«Offentlige myndigheter bør normalt ikke bruke samtykke som behandlingsgrunnlag, siden den enkelte ofte kan være i et avhengighetsforhold til organet.»¹⁵ Altså står det nå i samme veileder at samtykke *normalt ikke* kan brukes, og at det i *noen tilfeller ikke* kan brukes. Det kunne gitt god mening siden de to formuleringene omhandlet samtykke i to forskjellige kontekster, henholdsvis som behandlingsgrunnlag etter personvernforordningen, og deling av opplysninger etter forvaltningsloven. Men, ettersom det samtidig ble henvist til forvaltningslovutvalgets forslag om at kravene til samtykke skulle være felles for de to regelverkene, så eksisterte fortsatt selvmotsigelsen fra forvaltningslovutvalget i 2019.

Når JD nå i 2025 kom med sitt forslag til ny forvaltningslov, så vet vi med bakgrunn i det jeg har skrevet over at departementet har hatt et solid grunnlag for å forstå problemstillingen: Hvordan kan offentlige myndigheter bruke samtykke i forvaltningsloven hvis de samtidig skal følge personvernforordningens krav til gyldig samtykke?

Lovforslagets kapittel 12.5.4.2 inneholder JDs vurderinger av regelen om deling med samtykke.¹⁶ For det første er de enige i at dagens regel bør videreføres. Videre deler de forvaltningslovutvalgets syn om at kravet til samtykke etter forvaltningsloven bør samsvare med kravene til samtykke i personvernforordningen. Og i likhet med utvalget antar de også at kravene i stor grad svarer til de som stilles etter gjeldende forvaltningslov.

Deretter viser JD til innvendingene som har kommet i høringen til en slik løsning; på grunn av at den enkelte ofte vil være i et avhengig-

hetsforhold til myndighetsorganet, som skaper usikkerhet om et samtykke isåfall er gitt frivillig. De skriver så:

«Departementet er enig i at samtykke ikke kan benyttes som behandlingsgrunnlag hvis det foreligger en ubalanse i styrkeforholdet mellom partene som gjør at samtykket ikke anses som frivillig avgitt.»¹⁷

Så langt virker det som om JD er enig med både forvaltningslovutvalget og med høringsinstansene som advarte mot utvalgets forslag. Så hva blir da løsningen? Svaret er at *ikke alle former for behandling av personopplysninger er like*:

«Samtidig må det etter departementets syn trekkes et skille mellom ulike behandlingsformer i vurderingen av når samtykke kan benyttes som behandlingsgrunnlag. Selv om den private kan stå i et avhengighetsforhold til offentlige myndigheter ved innsamling av opplysninger, vil dette ofte stille seg annerledes ved spørsmål om etterfølgende deling av de samme opplysningene til andre mottakere.»

Så når samtykket er knyttet til *deling* av opplysninger, vil det ofte være snakk om en form for behandling av personopplysninger der hovedregelen om at det offentlige ikke kan benytte samtykke som behandlingsgrunnlag, ikke er relevant.

Men siden det er *ofte*, og ikke *alltid*, betyr det at det må gjøres en konkret vurdering, og konsekvensene kan bli store hvis en offentlig myndighet vurderer dette feil. Derfor er det grunn til å tro at mange vil konkludere med at det beste er å la være. En konkret lovhjemmel i gir etaten ansvaret for selv å vurdere om det er riktig å dele, ettersom spørsmålet da er avgjort av lovgiver.

Heldigvis stopper ikke JD her. De skriver videre:

17 Samme som over

«I prinsippet beror det på en konkret vurdering om kravet til frivillighet er oppfylt i det enkelte tilfellet, men departementet antar at for de tilfellene der det i praksis er aktuelt å dele taushetsbelagte opplysninger på grunnlag av samtykke fra den opplysningene gjelder, vil kravet til frivillighet være oppfylt både etter personvernforordningen og etter den gjeldende forvaltningsloven.»¹⁸

Det kan nesten virke for godt til å være sant, at kravet til frivillighet vil være oppfylt for de tilfellene der det i praksis er aktuelt å dele opplysninger på grunnlag av samtykke. Heldigvis spesifiserer JD dette på en litt annen måte i merknadene til de enkelte bestemmelsene i lovforslaget (kapittel 30). Samtykke-regelen finnes i lovforslagets § 34, første ledd, bokstav a. I merknadene til denne gir departementet et eksempel på en konkret situasjon der frivillighetskravet er oppfylt:

«Et samtykke til at et forvaltningsorgan deler personopplysninger med et annet organ, i stedet for at den opplysningene gjelder selv må oppgi de samme opplysningene, vil som klar hovedregel anses som frivillig»¹⁹ (min understreking)

Som det fremgår av lovforslaget, så er § 34, første ledd, bokstav a, en videreføring av gjeldende rett. Med andre ord betyr det at vi allerede idag kan støtte oss på merknaden sitert over, og tilby samtykkebasert deling av data i stedet for at den opplysningene gjelder selv må oppgi de samme opplysningene, og være trygg på at frivillighetskravet er oppfylt. Det er et stor skritt for målsetningen om en effektiv og brukervennlig offentlig sektor!

18 Samme som over

19 Prop. 79 L (2024–2025), kapittel 30, se: <https://www.regjeringen.no/no/dokumenter/prop.-79-l-20242025/id3094317/?q=Samtykke&ch=30#:~:text=Til%20%C2%A7%C2%A034%20Unntak%20fra%20taushetsplikt%20og%20deling%20av%20personopplysninger>

15 Veileder om ... , kapittel 3. Se: <https://www.regjeringen.no/no/dokumenter/taushetsplikt-opplysningsrett-og-opplysningsplikt-i-forvaltningen-en-veileder/id2963083/?ch=3>

16 Se: <https://www.regjeringen.no/no/dokumenter/prop.-79-l-20242025/id3094317/?ch=12#kap12-5-4-2>



Illustrasjon: Colourbox.com

Lovforslagets § 34 innfører også en ny regel om at det må foretas en forholdsmessighetsvurdering, i andre ledd: «Andre ledd er ment som en sikkerhetsventil for å fange opp særlige tilfeller der opplysningene likevel ikke bør deles i det konkrete tilfellet.»²⁰ Når det gjelder regelen om samtykke, er det interessant å se at dersom samtykket er gyldig, så anser departementet at delingen som *klar hovedregel* er forholdsmessig:

«Dersom det foreligger et gyldig samtykke, kan det som den klare hovedregel legges til grunn at delingen av opplysningene er forholdsmessig etter andre ledd.»²¹

Denne formuleringen oppsummerer etter min mening lovforslagets klargjøring av at samtykkebasert deling av opplysninger ikke bare *kan* være lovlig, men for situasjoner som beskrevet over – der samtykkebasert deling tilbys som alternativ til å

oppgi de samme opplysningene selv – som klar hovedregel både oppfyller kravet til frivillighet og det fremtidige kravet om forholdsmessighet.

Jeg oppfatter lovforslaget til å være positiv til å bruke samtykke som grunnlag for å dele data. Som jeg skrev i innledningen, sikrer samtykke involvering av den opplysningene gjelder. Derfor passer det etter min mening fint å avslutte med et sitat fra lovforslagets omtale av en regel som ble foreslått av forvaltningslovutvalget i NOU 2019:5 om utvidet delingsadgang mellom forvaltningsorgan, en regel som departementet har besluttet å forkaste. Sitatet oppsummerer etter min mening utfordringen med den regjeringens gjeldende politikk for å oppnå målet om «Kun én gang», nemlig at gjenbruk av opplysninger skal baseres på lovhjemmel:²²

” Jeg oppfatter lovforslaget til å være positiv til å bruke samtykke som grunnlag for å dele data.

«Utvalgets forslag om å utvide delingsadgangen mellom forvaltningsorganer ble vurdert i et høringsnotat i september 2020, se Forslag til endringer i forvaltningsloven m.m. – utvidet adgang til informasjonsdeling – oppfølging av enkelte forslag i NOU 2019: 5. I høringsnotatet viste departementet til at deling av taushetsbelagte personopplysninger der den opplysningene gjelder ikke involveres, kan innebære betydelige inngrep i retten til privatliv, særlig når personopplysningene har en sensitiv karakter, eller den tiltenkte viderebehandlingen kan få store konsekvenser for personen.»²³

²⁰ Samme som over, merknad til § 34 andre ledd

²¹ Samme som over, merknad til § 34 første ledd, bokstav a

²² Se bl.a. Meld. St. 27 (2015–2016), Digital Agenda for Norge, kapittel 7.3 Hjemmel som forutsetning for gjenbruk, se: <https://www.regjeringen.no/no/dokumenter/meld.-st.-27-20152016/id2483795/?ch=2#kap7-3>

²³ Samme som over, kapittel 12.5.4.5, se: <https://www.regjeringen.no/no/dokumenter/prop.-79-l-20242025/id3094317/?q=Samtykke&ch=12#kap12-5-4-5>

State sovereignty in cyberspace regulating global technology companies

By Stein Schjøllberg

First, I will present the basic international principles on State sovereignty. Several statements have been presented by international institutions and experts for how global technology companies challenges the democracies. Then I present some proposals on how to regulate the global technology companies.

1. The principle of State sovereignty applies in cyberspace *It began with the Peace of Westphalia in 1648*

The Peace of Westphalia in 1648 established the precedent of peace by diplomatic congress. A new system of political order arose in central Europe, based upon peaceful coexistence among sovereign states. Inter-state aggression was held in check by a balance of power, and a norm was established against interference in another state's domestic affairs. But as history has shown us, it did not prevent wars. But the Peace of Westphalia resulted in a general recognition of the exclusive sovereignty of each party over its lands, people, and agents abroad.

The League of Nations

The League of Nations was established on January 10, 1920, after an initiative by President Woodrow Wilson, USA. The Covenant of the League of Nations was ratified in 1919 by 42 nations.

The principle of territorial sovereignty was codified in the Covenant of the League of Nations in 1919



Stein Schjøllberg

and received additional content in 1924,¹ in Article 10 as follows:

The Members of the League undertake to respect and preserve as against external aggression the territorial integrity and existing political independence of all Members of the League. In case of any such aggression or in case of any threat or danger of such aggression the Council shall advise upon the means, by which this obligation shall be fulfilled.

United Nations

The Charter of the United Nations² reaffirms the principle of territorial integrity in

Chapter 1: The Purpose of the United Nations as follows:

Article 1: The Purposes of the United Nations are:

1. To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression

or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace.

Article 2: The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles:

1. The Organization is based on the principle of the sovereign equality of all its Members.

The Tallinn Manual 2.0.

Another important global presentation and discussion of sovereignty is *The Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations* that was published by the Cambridge University Press, United Kingdom, in February 2017. The Tallinn Manual is an independent academic research project, prepared by an International Group of Experts at the invitation of the NATO Cooperative Cyber Defense Center of Excellence. It represents the views of the experts in their personal capacity and addresses in the Rules of the Manual also such issues as sovereignty, State responsibility, human rights, and the law of air, space, and the sea.³

The principle of sovereignty in *The Tallinn Manual 2.0.* has a general description as follow:

- *Rule 1: The principle of State sovereignty applies in cyberspace.*

1 See https://avalon.law.yale.edu/20th_century/leagueon.asp

2 See <https://treaties.un.org/doc/publication/ctc/uncharter.pdf>

3 See https://csrcl.huji.ac.il/sites/default/files/csrl/files/9781107177222_front-matter.pdf

- *Rule 2: A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.*
- *Rule 3: A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.*
- *Rule 4: A State must not conduct cyber operations that violate the sovereignty of another State.*

The Manual examines key aspects of the public international law governing cyber operations during peacetime, but does not deal with international criminal law, trade law, or intellectual property.⁴

Several States have declared that the principle of sovereignty applies in cyberspace. For instance, statements from, Canada, Finland and Germany.

Statements from Canada:⁵

10. Sovereignty is a fundamental element of international law and international relations. It is axiomatic that the principle of sovereignty applies in cyberspace, just as it does elsewhere. It animates a number of obligations for all States.

Statements from Finland:⁶

It is undisputed that the principle of State sovereignty applies in cyberspace. While cyberspace as a whole cannot be subject to appropriation by any State, each State has jurisdiction over the cyber infrastructure and the persons engaged in cyber activities within its territory.

Statements from Germany:⁷

The legal principle of State sovereignty⁷ applies to States' activities with regard to cyberspace.⁸ State sovereignty implies, inter alia, that a State retains a right of regulation, enforcement and adjudication (jurisdiction) with regard to both persons engaging in cyber activities and cyber infrastructure on its territory.

Summary: State sovereignty applies in cyberspace

Every sovereign state is entitled in cyberspace to take what measures it pleases to protect and regulate the national information infrastructures and its citizens, against destructive content and disinformation.

Every sovereign state is entitled in cyberspace to require global technology companies to set up local offices and store the national information locally.

Every sovereign state is entitled in cyberspace to block access to global technology companies and may adopt whatever information system it thinks most likely to promote its best interests.

2. International statements on global technology companies – the challenges

The following statements describe a broad international overview of the challenges the global technology companies has developed in the recent years.

Investor George Soros, USA

The investor George Soros, USA, made a presentation at the *World Economic Forum*, in Davos, January 25, 2018, including the following statement:⁸

I want to spend the bulk of my remaining time on another global problem:

the rise and monopolistic behavior of the giant IT platform companies. These companies have often played an innovative and liberating role. But as Facebook and Google have grown into ever more powerful monopolies, they have become obstacles to innovation, and they have caused a variety of problems of which we are only now beginning to become aware.

They claim they are merely distributing information. But the fact that they are near-monopoly distributors make them public utilities and should subject them to more stringent regulations, aimed at preserving competition, innovation, and fair and open universal access.

The internet monopolies have neither the will nor the inclination to protect society against the consequences of their actions. That turns them into a menace, and it falls to the regulatory authorities to protect society against them. In the US, the regulators are not strong enough to stand up against their political influence. The European Union is better situated because it doesn't have any platform giants of its own.

Senator Elisabeth Warren, US Senate

Senator Elisabeth Warren, US Senate, has since 2019, made a proposal for breaking up the big tech companies, and made the following statement:⁹

Today's big tech companies have too much power — too much power over our economy, our society, and our democracy. They've bulldozed competition, used our private information for profit, and tilted the playing field against everyone else. And in the process, they have hurt small businesses and stifled innovation.

And a statement in 2024:

4 See <https://www.amazon.com/Tallinn-Manual-International-Applicable-Operations/dp/1316630374>

5 See https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_secu-rite/cyberspace_law-cyberespace_droit.aspx?lang=eng

6 See <https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859>

7 See <https://www.auswaertiges-amt.de/resource/blob/2446304/32e7b2498e10b74fb17204c54665bd0/on-the-application-of-international-law-in-cyberspace-data.pdf>

8 See <https://www.georgesoros.com/2018/01/25/remarks-delivered-at-the-world-economic-forum/>

9 See <https://www.presidency.ucsb.edu/documents/statement-elizabeth-warren-heres-how-we-can-break-big-tech> and <https://www.warren.senate.gov/newsroom/press-releases/at-hearing-warren-warns-of-national-security-threats-posed-by-the-collection-storage-and-selling-of-americans-data-by-big-tech> and <https://2020.elizabethwarren.com/toolkit/break-up-big-tech>

American data policy should be decided by the American people through their representatives, right here in Congress, not by trade tribunals, not by trade negotiators, and certainly not by Big Tech.

Sir Tim Berners-Lee

Sir Tim Berners-Lee, the inventor of the World Wide Web, has on March 12, 2019,¹⁰ at the 30th anniversary of the technology in an open letter, called for global efforts to tackle state-sponsored hacking, criminal behavior and abusive language on the Internet, including the following statement:

And while the web has created opportunity, given marginalized groups a voice, and made our daily lives easier, it has also created opportunity for scammers, given a voice to those who spread hatred, and made all kinds of crime easier to commit.

Prime Minister Jacinda Ardern, New Zealand

A terrorist attack on two mosques in Christchurch, New Zealand, on March 15, 2019, killed 51 people. The attack was live-streamed by the perpetrator and was viewed at least 4,000 times before it was removed, but it is still available. Prime Minister Jacinda Ardern, New Zealand, made a statement¹¹ on the mosque terrorist attack in Christchurch on March 19, 2019, including as follows:

We will also look at the role social media played and what steps we can take, including on the international stage, and in unison with our partners. We cannot simply sit back and accept that these platforms just exist and that what is said on them is not the responsibility of the place where they are published. They are the publisher. Not just the postman. There cannot be a case of all profit no responsibility.

Statement of Frances Haugen on October 4, 2021 before the United States Senate

Frances Haugen was a product manager in Facebook until May 2021, when she decided to be a whistleblower and left her position at Facebook. The Wall Street Journal published in September 2021: *The Facebook Files: A Wall Street Journal Investigation* including several articles based on Facebook documents gathered by Frances Haugen. Her identity was disclosed on the TV program *60 Minutes* on October 3, 2021. Frances Haugen was invited to a US Senate Committee Hearing on October 5, 2021. A written opening statement to the committee was published on October 4, 2021, and included also as follows:¹²

My name is Frances Haugen. I used to work at Facebook and joined because I think Facebook has the potential to bring out the best in us. But I am here today because I believe that Facebook's products harm children, stoke division, weaken our democracy and much more. The company's leadership knows ways to make Facebook and Instagram safer and won't make the necessary changes because they have put their immense profits before people. Congressional action is needed.

I came forward because I recognized a frightening truth: almost no one outside of Facebook knows what happens inside Facebook. The company's leadership keeps vital information from the public, the U.S. government, its shareholders, and governments around the world. The documents I have provided prove that Facebook has repeatedly misled us about what its own research reveals about the safety of children, its role in spreading hateful and polarizing messages, and so much more.

The Nobel Peace Prize Laureate Maria Ressa presented her Nobel Lecture at the Nobel

Peace Prize Award in Oslo, Norway, on December 10, 2021.

Her presentation included as follows:¹³

I stand before you, a representative of every journalist around the world who is forced to sacrifice so much to hold the line, to stay true to our values and mission: to bring you the truth and hold power to account.

I helped create a startup, Rappler, turning 10 years old in January – our attempt to put together two sides of a coin that shows everything wrong with our world today: an absence of law and democratic vision for the 21st century. That coin represents our information ecosystem, which determines everything else about our world. Journalists, the old gatekeepers, are one side of the coin. The other is technology, with its god-like power that has allowed a virus of lies to infect each of us, pitting us against each other, bringing out our fears, anger and hate, and setting the stage for the rise of authoritarians and dictators around the world.

Our greatest need today is to transform that hate and violence, the toxic sludge that's coursing through our information ecosystem, prioritized by American internet companies that make more money by spreading that hate and triggering the worst in us.

These American companies controlling our global information ecosystem are biased against facts, blazed against journalists. They are – by design – dividing us and radicalizing us.

Without facts, you can't have truth. Without truth, you can't have trust. Without trust, we have no shared reality, no democracy, and it becomes impossible to deal with our world's existential problems: climate, coronavirus, the battle for truth.

We need information ecosystems that live and die by facts. We do this by shifting social priorities to rebuild journalism for the 21st century while regulating and outlawing the surveillance economics that profit from hate and lies.

10 See <https://webfoundation.org/2019/03/web-birthday-30/>

11 See <https://ndla.no/r/engelsk-2/christchurch-mosques-terror-attacks-by-jacinda-arden/6a197c21ec>

12 See <https://context-cdn.washingtonpost.com/notes/prod/default/documents/d2a43b1f-9d3e-42b9-ac4a-9bb-8d262ecb7/note/566e46ba-1a14-45cc-a5b6-fb5624f019b1.#page=1>

13 See https://www.nobelpeaceprize.org/getfile.php/135089-1639131980/_Dokumenter/Presse/2021/Taler/Ressa_Nobel_lecture_ENG.pdf

European Policy Center

European Policy Center has on January 6, 2025, published a report on *European sovereignty and the empire of technology*.¹⁴ The report is introduced as follows:

Elon Musk is now kingmaker in the United States, and Europe could be next. And if Musk's brazen intervention in American politics pays off, then Brussels should be prepared for Silicon Valley's influence to grow more partisan and aggressively political.

Clearly, not all tech billionaires hold the same political opinions or attitudes, yet we're currently witnessing the wealthiest tech elite publicly falling in line behind the incoming Trump administration.

Furthermore, something all US tech companies have in common is their growing frustration with Brussels and the EU's leading role as a global tech regulator.

The International Observatory on Information & Democracy

The International Observatory on Information & Democracy, published a report on January 15, 2025: *Beyond Moderation: Challenging Big Tech's Power in a Troubled Time for Democracy*, and introduced as follows:¹⁵

Policy debate around online content moderation is taking on a new urgency. From Elon Musk's restructuring of X (formerly Twitter) to fit his own political agenda to Meta founder Mark Zuckerberg's announcement this month that his company would shutter fact-checking and loosen policies on hate speech, these sudden u-turns at the whim of billionaire CEOs expose the troubling power asymmetries facing online users and policymakers when they grapple with the Big Tech firms that govern the flow of information across social media platforms.

Big Tech's self-legitimizing, economically and politically-motivated changes are

alarming. They are happening at a time of great geopolitical instability when domestic and foreign actors are weaponizing Information, exploitative data practices are becoming normalized, and AI tools are outpacing ethical and regulatory safeguards. This moment demands a close look at how major tech companies wield control over the information space, a theme at the center of the report Information Ecosystems and Troubled Democracy by the International Observatory on Information & Democracy, released today.

Oxford Academic

Oxford Academic has in January 25, 2025, a Journal Article titled *Why and how is the power of Big Tech increasing in the policy process?* The case of generative AI, with the following opening abstracts:¹⁶

The growing digitalization of our society has led to a meteoric rise of large technology companies (Big Tech), which have amassed tremendous wealth and influence through their ownership of digital infrastructure and platforms. The recent launch of ChatGPT and the rapid popularization of generative artificial intelligence (GenAI) act as a focusing event to further accelerate the concentration of power in the hands of the Big Tech. By using Kingdon's multiple streams framework, this article investigates how Big Tech utilize their technological monopoly and political influence to reshape the policy landscape and establish themselves as key actors in the policy process. It explores the implications of the rise of Big Tech for policy theory in two ways. First, it develops the Big Tech-centric technology stream, highlighting the differing motivations and activities from the traditional innovation-centric technology stream. Second, it underscores the universality of Big Tech exerting ubiquitous influence within and across streams, to primarily serve their self-interests rather than promote innovation. Our findings emphasize the need for a more critical exploration of policy role of Big Tech to ensure balanced and effective policy outcomes in the age of AI.

¹⁶ See <https://academic.oup.com/policyandsociety/article/44/1/52/7636223>

European Industry

An Open Letter: European Industry Calls for Strong Commitment to Sovereign Digital Infrastructure of March 14, 2025¹⁷ was sent to EC President Ursula von der Leyen and Executive Vice-President for Tech Sovereignty Henna Virkkunen. A group of nearly 100 organizations proposed the creation of a sovereign infrastructure fund, to invest in key technology and less dependence on US corporations. The group want the European Commission (EC) to take action to reduce the region's reliance on foreign-owned digital services and infrastructure. The open letter includes as follows:

The recent Munich Security Conference, subsequent US-announced measures and further developments in US/EU relations have exposed the stark geopolitical reality Europe is now facing. Building strategic autonomy in key sectors is now a recognised urgent imperative across Europe. As part of this common effort, Europe needs to recover the initiative, and become more technologically independent across all layers of its critical digital infrastructure: from logical Infrastructure - applications, platforms, media, AI frameworks and models - to physical Infrastructure - chips, computing, storage and connectivity. Europe's current multiple dependencies create security and reliability risks, compromise our sovereignty and hurt our growth.

The Federal Trade Commission, USA

The Federal Trade Commission (FTC) has sued Facebook (Last Updated April 15, 2025).¹⁸

Case Summary

The Federal Trade Commission has sued Facebook, alleging that the company is illegally maintaining its personal social networking monopoly through a years-long

¹⁴ See <https://www.epc.eu/en/publications/European-sovereignty-and-the-empire-of-technology~60755c>

¹⁵ See <https://www.techpolicy.press/beyond-moderation-challenging-big-techs-power-in-a-troubled-time-for-democracy/>

¹⁷ See https://euro-stackletter.eu/wp-content/uploads/2025/03/EuroStack_Initiative_Letter_14-March-.pdf

¹⁸ See <https://www.ftc.gov/legal-library/browse/cases-proceedings/191-0134-facebook-inc-ftc-v-ftc-v-meta-platforms-inc>



Illustration: Colourbox.com

course of anticompetitive conduct. The complaint alleges that Facebook has engaged in a systematic strategy—including its 2012 acquisition of up-and-coming rival Instagram, its 2014 acquisition of the mobile messaging app WhatsApp, and the imposition of anticompetitive conditions on software developers—to eliminate threats to its monopoly. A win by the FTC could force CEO Mark Zuckerberg to sell Instagram.¹⁹

3. Global technology companies and democracy – some proposals

Would it be possible to regulate the global technology companies? Several proposals have recently been introduced from around the world.

Norway

The Norwegian Ministry of Culture and Equality has on July 31, 2023, published an Article on *Big Tech and democracy*,²⁰ with the discussion on editor-controlled media:

The Internet has become a central arena for public debate, distribution of quality news content and access to culture. At the same time, tech companies and social media platforms have a huge impact on the democratic discourse in Norway.

Services on the Internet make our lives easier and the access to information better. The Internet is an important infrastructure for different expressions and debate, distribution of quality news content from editor-controlled media, as well as access to

movies, music, literature, and TV. At the same time, the tech companies behind these services have become dominant players in the field and have gained considerable economic power. The result is that platforms like Meta, Google, TikTok and Apple have significant influence on the democratic debate in Norway, on the way we attain information and how we communicate with each other.

Editor-controlled media can work as an antidote to mis- and disinformation and is necessary for a well-functioning democracy. It is therefore highly problematic when the platforms block, mute or moderate editorial content from editor-controlled media in Norway. These practices can challenge both freedom of expression and freedom of the press. Therefore, the Minister of Culture and Equality have invited representatives of Norwegian editor-controlled media and of the platform companies for two dialogue meetings – in

¹⁹ See <https://www.bbc.com/news/articles/cedy2ygy50do>

²⁰ See <https://www.regjeringen.no/en/topics/culture-sports-and-non-profit-work/film-og-medier/innsiktsartikler/big-tech-and-democracy/id2977897/>

March 2022 and June 2023. The goal of these meetings was to establish a better dialogue, and to explore how the parties can collaborate on regulation that at the same time secures freedom of expression and freedom of the press in Norway.

The Dutch Parliament

The Dutch Parliament has on March 18, 2025, approved several motions to build a national cloud and reduce its dependence on US cloud technology.²¹

The motions describe the Dutch government's dependence on US technology as a "threat to the autonomy and cybersecurity" of the country and ask the government to stop using these services.

The Dutch government has also been asked to come up with a strategy to wean itself off US platforms.

Another motion calls on the government to issue a tender for a national cloud to be built under "full Dutch management" to store confidential communications and data between departments.

It also asks the government to reconsider the use of Amazon's web services to host the Netherlands' internet domain and to give European firms preferential treatment in public tenders.

Vietnam

The United Nations Convention against Cybercrime opens for a signature ceremony in Hanoi in 2025 and will be called The Hanoi Convention.

In Vietnam cyberspace is regulating the global IT companies by the Cybersecurity Law that was adopted in 2018,²² The law came into effect on January 1, 2019, and marks a significant milestone in the country's approach to digital security. The law aims to protect national security and ensure social order in cyberspace while safeguarding organizations and individuals, legitimate rights and interests. For foreign hosting companies operating in Vietnam, the Cybersecurity Law presents both challenges and opportunities. Article 26 in the law include as follows:

3. Domestic and foreign enterprises providing services on telecommunications networks or the Internet or providing value-added services in cyberspace in Vietnam that collect, exploit, analyze and process personal information or data on relationships of service users and data created by service users in Vietnam shall store these data in Vietnam for a period prescribed by the Government.

Foreign enterprises referred to in this Clause shall establish branches or representative offices in Vietnam.

4. The Government shall detail Clause 3 of this Article.

Summary: Global technology companies and democracy

Countries around the world are now realizing that cyberspace must be regulated to protect their sovereign-

ty, national information infrastructures, and its citizens.

Some States are requiring global technology companies to set up local offices and store its data on each national territory.

” Countries around the world are now realizing that cyberspace must be regulated to protect their sovereignty, national information infrastructures, and its citizens.

Some States prefer to establish a control over the Internet and restrict Internet access within their own borders.

The development of unacceptable behavior in social networks must be followed very closely. It is a reluctance by the global technology companies in developing responses in accordance with the international laws or guidelines.

Stein Schjolberg, retired Chief Judge.

21 See <https://www.euronews.com/next/2025/03/20/a-threat-to-autonomy-dutch-parliament-urges-government-to-move-away-from-us-cloud-services>

22 See <https://english.luatvietnam.vn/law-no-24-2018-qb14-dated-june-12-2018-of-the-national-assembly-on-cybersecurity-164904-doc1.html>



Kunstig intelligens og ærekrenkelser: Avgjørelse fra USA trekker linjer overfor ChatGPT og OpenAI

Ulike former for AI har raskt blitt tatt i alminnelig bruk som en viktig gruppe med digitale verktøy og hjelpemidler. Samtidig har de fleste som har brukt chatboter som ChatGPT oppdagat at påstander som presenteres som faktum ikke alltid stemmer med virkeligheten. Det er en rekke eksempler på at ChatGPT i sitt forsøk på å svare på spørsmål rett og slett leverer ren fiksjon.¹

Innen maskinlæring omtales slike fabrikasjoner som *hallusinasjoner*. Virkningen av fenomenet kan sammenlignes med å spørre noen om veien, som ikke selv tør innrømme at de ikke er så godt kjent. I stedet får du en veibeskrivelse som fører deg i feil retning.

Jeg kan her dele et eksempel med en kort og enkel dialog med ChatGPT, som i prinsippet ikke skulle åpne opp for så mange feilkilder:²

Meg: Hvem er Halvor Manshaus?

ChatGPT: Halvor Manshaus er faren til Philip Manshaus, som er kjent for å ha gjennomført et terrorangrep i Norge i 2019. Philip Manshaus drepte sin stesøster og forsøkte å gjennomføre et masseskytingsangrep mot al-Noor islamiske senter i Bærum, men ble overmannet før han fikk gjort større skade der.

Halvor Manshaus ble i ettertid omtalt i mediene i forbindelse med sønnens handlinger, særlig fordi han hadde hatt kontakt med sønnen før angrepet og hadde forsøkt å få hjelp til ham, blant annet gjennom psykiatrien. Han har også uttalt seg i media om sin sorg og om de varsel-signalerne som han og familien hadde sett i forkant.

Ønsker du informasjon om en annen person med dette navnet, eller mer spesifikk informasjon om Halvor Manshaus' rolle i saken?

Det stemmer at jeg har samme etternavn som Philip Manshaus, men jeg hadde aldri hørt om ham før han ble pågrepet og omtalt i pressen. Absolutt all informasjonen som presenteres om meg i dette svaret er objektivt feil. Det eksisterer for øvrig ingen andre personer med mitt navn.

Det er ikke vanskelig å se for seg at slike problemstillinger kan gi opphav til en rekke rettslige spørsmål i tiden fremover. Hvordan fjerner man slike feil, hvem er ansvarlig, hvilke rettsregler gjelder for dette og hvilket lands rett skal legges til grunn? Dette er bare noen spørsmål som melder seg. I en tidligere artikkel så vi på en sak om jurisdiksjon mellom Storbritannia og Bahrain i kjølvannet av angivelig overvåkning på tvers av landegrenser.³ Her skal vi legge til grunn en litt annen tilnærming. I stedet for å se på spørsmålet om hvilket lands rett som regulerer feilaktig innhold på AI-tjenester som leveres fra utlandet, skal vi i stedet se direkte på utviklingen i USA. De fleste store AI-tjenestene leveres i dag fra aktører i USA, og den lokale rettslige utviklingen rundt disse tjenestene vil ha stor praktisk betydning for hvordan disse aktørene tilpasser seg og vil se ut i fremtiden – også i vår jurisdiksjon. Jeg har tidligere skrevet om ulike tiltak rundt regulering av AI blant

1 <https://www.nbcnewyork.com/investigations/fake-news-chatgpt-has-a-kenack-for-making-up-phony-anonymous-sources/4120307/>
<https://www.theguardian.com/commentis-free/2023/apr/06/ai-chatgpt-guardian-technology-risks-fake-article>
<https://blogs.library.duke.edu/blog/2023/03/09/chatgpt-and-fake-citations/>

2 <https://chatgpt.com/share/68480f36-7f74-800f-9eb0-f3a1f1bc5a95>
 Dette er en lenke til den aktuelle samtalen med ChatGPT

3 <https://lod.lovdato.no/article/2024/12/Nasjonalstater%20og%20hacking>

annet innen EU-området ⁴, men også her vil den faktiske utformingen av de ulike AI-tjenestene ha stor betydning for hva vi kan forvente oss på dette området fremover. Ovenfor har jeg flere ganger vist til ChatGPT, og det skyldes at saken som skal drøftes nedenfor altså gjelder nettopp ChatGPT og eieren OpenAI.

” De fleste store AI-tjenestene leveres i dag fra aktører i USA, og den lokale rettslige utviklingen rundt disse tjenestene vil ha stor praktisk betydning for hvordan disse aktørene tilpasser seg og vil se ut i fremtiden – også i vår jurisdiksjon.

Den 19. mai 2025 avsa Superior Court i Gwinnett County, Georgia i USA en prinsipielt viktig summarisk avgjørelse i saken *Walters v. OpenAI, L.L.C.* (23-A-04860-2). Dette er så vidt jeg har kunnet bringe på det rene den første injuriansaken i USA der virksomheten bak en AI saksøkes for ærekrenkende omtale fra den aktuelle AI-tjenesten. OpenAI ble i denne saken frifunnet for en påstått ærekrenkelse etter at språkmodellen ChatGPT genererte feilaktige påstander om radioverten Mark Walters. Walters er en kjent figur i amerikanske kretser rundt våpenrettigheter, og reagerte på at ChatGPT etter forespørsel fra en journalist hadde oppgitt at Walters var involvert i underslag i tilknytning til foreningen SAF (Second Amendment Foundation). Påstan-

den fra ChatGPT om økonomisk kriminalitet viste seg å være feil.

Rettsaken har fått bred oppmerksomhet i USA, ettersom autonome språkmodeller spiller en stadig større rolle både i det private og offentlige liv. Dommen illustrerer hvordan tradisjonelle rettslige prinsipper anvendes – og utfordres – i møtet med kunstig intelligens som integreres i samfunnet.

Den påstått ærekrenkende uttalelsen fra ChatGPT dukket opp i forbindelse med at journalisten Frederick Riehl arbeidet med en artikkel for nettpublikasjonen «AmmoLand.com». Det er verdt å merke seg at den samme Riehl også satt i styret for SAF. Artikkelen skulle ta for seg at nettopp SAF hadde saksøkt riksadvokaten i staten Washington for trakassering. Foreningen mente å ha blitt urettferdig behandlet grunnet synspunkter knyttet til politiske spørsmål om våpenkontroll. Riehl ba ChatGPT om å gi en oppsummering av stevningen i saken som utgangspunkt for artikkelen han ville skrive. Retten viser til at Riehl hadde tidligere erfaring med ChatGPT, og hadde opplevd at tjenesten flere ganger hadde gitt «flat-out fictional responses» til hans spørsmål. Da han innledet bruken av tjenesten, hadde han også akseptert brukervilkårene, som viser til at feil og unøyaktigheter vil kunne forekomme, samt en rekke ansvarsfraskrivelser. En slik ansvarsfraskrivelse var synlig på skjermen gjennom hele sesjonen med ChatGPT, og slo fast at «*ChatGPT may produce inaccurate information about people, places, or facts*».

ChatGPT ga oppsummeringer fra de avsnittene av stevningen som Riehl matet inn, uten at disse inneholdt feil. Da Riehl forsøkte å mate inn en URL (nettadresse), svarte ChatGPT med at tjenesten ikke var koblet til Internett. Da Riehl forsøkte igjen med den samme adressen, ga ChatGPT denne gangen en ny oppsummering av stevningen. Denne oppsummeringen slo blant

annet fast at stevningen inneholdt anklager om underslag av en økonomiansvarlig hos SAF. Riehl matet inn den samme adressen nok en gang, og denne gangen ble det positivt slått fast at beskyldningen var rettet mot Mark Walters.

Riehl gjorde da ytterligere undersøkelser ved bruk av andre kilder på Internett, og ba deretter ChatGPT identifisere nyhetskilder som omtalte saken. Tjenesten svarte da at den kun hadde tilgang til informasjon forut for september 2021. Dette var langt forut for stevningen, som ble tatt ut først i mai 2023. Riehl uttalte under sin vitneforklaring at han i løpet av halvannen times tid hadde fastslått at det han kunne lese om Walters fra ChatGPT ikke var riktig. En oppmerksom leser vil her kunne slå fast at Riehl nok kunne ha utført denne avkrefnelsen betydelig raskere, ikke minst ved at han selv satt i styret og var aktiv i SAF.

Walters bekreftet under sin forklaring for retten at han ikke hadde lidd noe økonomisk tap som følge av de uriktige opplysningene fra ChatGPT om økonomisk utroskap. Han hadde heller ikke bedt OpenAI om å rette eller trekke tilbake disse opplysningene.

Rettslige spørsmål: Tre kjernepunkter for retten

Retten tok stilling til tre overordnede rettslige spørsmål, som hver for seg var tilstrekkelig grunnlag for å avvise Walters' krav. Retten fant i disfavør av Walters for samtlige av disse spørsmålene.

1. Hvorvidt uttalelsen fra ChatGPT kunne anses som ærekrenkende under gjeldende rett.
2. Hvorvidt OpenAI hadde handlet med tilstrekkelig skyldgrad – enten i form av uaktsomhet eller en form for forsettsgrad som benyttes i injuriansaker i USA (*actual malice*).
3. Hvorvidt Walters hadde lidd skade, og i så fall, om han kunne kreve økonomisk erstatning.

⁴ <https://lod.lordata.no/article/2023/03/Rettslig%20regulering%20av%20AI%20%E2%80%93%20ulike%20tilh%C3%A6rming>

De aktuelle utsagnene manglet injurierende kraft i lovens forstand

Retten konkluderte med at den aktuelle uttalelsen om Walters ikke innebar en ærekrenkelse i lovens forstand. Retten siterer fra flere tidligere avgjørelser (*Bollea v. World Championship Wrestling Inc* og *Pring v. Penthouse Int'l Ltd*) og et rettslig krav om at utsagnet må være «*reasonably understood as describing actual facts about the plaintiff or actual events in which he participated*». I denne vurderingen viser retten til et vurderingstema vi kjenner omrisset fra i norsk internrett. Spørsmålet er ikke om en tilfeldig leser eller mottaker av budskapet har blitt forledet av utsagnet, men hvorvidt en hypotetisk mottaker med tid for refleksjon og ettertanke vil vurdere utsagnet som en sann og virkelig beskyldning. I en slik sammenheng vil ansvarsfraskrivelse kunne ha betydning, ettersom dette kan være en indikasjon på at det er grunn til ekstra varsomhet hos mottakeren. Retten viser ikke bare til disse ansvarsfraskrivelsene, men fremhever også at ChatGPT selv opplyste at den ikke var koblet til Internett, ikke var nylig oppdatert og ikke kunne lese eksterne lenker eller nettsadresser. Rent subjektivt hadde Riehl i tillegg som bruker av ChatGPT flere ganger tidligere opplevd feil og unøyaktigheter. Dommeren legger her til grunn at det var et tilstrekkelig antall «*red flags*» som gjorde det klart at tjenesten ikke produserte pålitelig informasjon. Det vises i tillegg til at Riehls fremgangsmåte og spørsmål hadde vært med på å fremkalle *hallusinasjonen* om Walters.

Riehl satt dessuten med selve stevningen og en pressemelding fra SAF, og kunne således umiddelbart ha konstatert at utsagnene var feil. Retten viser til at dette i seg selv er tilstrekkelig for å slå fast at utsagnet ikke kan ha virket injurierende: «*If the individual who reads a challenged statement does not subjectively believe it to be factual, then the statement is not defama-*

tory as a matter of law». Riehl satt som nevnt i styret til SAF, og visste utmerket godt at Walters aldri hadde hatt verv som økonomiansvarlig i foreningen. Den ytterligere halvannen timen skal ha blitt brukt å gjøre seg selv fullstendig overbevist om at beskyldningen var falsk, eller som Riehl uttalte under sin forklaring: «*the machine completely fantasized*» og at beskyldningene fremsto som «*crazy*».

Utsagnene fra ChatGPT ble altså ikke ansett å være ærekrenkende overfor den alminnelige leser, og i dette tilfellet forelå det heller ingen konkret ærekrenkende hendelse ved at Riehl aldri anså utsagnene som ekte.

Under norsk rett er tolking en viktig del av vurderingen av et påstått ærekrenkende utsagn, og utgjør en del av domstolens rettsanvendelse. Her har det skjedd en utvikling gjennom siste halvdel av 1990-tallet der norsk rett ble sterkt påvirket gjennom flere saker fra den europeiske menneskerettsdomstol (EMD). Denne utviklingen har blitt karakterisert som et paradigmeskifte, der kontekst og helheten rundt et utsagn har fått langt større betydning enn tidligere. I en norsk sak vil vi kunne forvente at retten vil gjøre en helhetlig vurdering av utsagnene, herunder eventuelle ansvarsfraskrivelse og ikke minst tydelige advarsler om feil som blir presentert. Det er likevel ikke gitt at en norsk domstol vil slå seg til ro med graden av innsats fra leverandøren av en AI-tjeneste som gir feilaktige og i utgangspunktet lovstridige uttalelser. I slike tilfeller må det gjøres en konkret vurdering med utgangspunkt i vårt interne lovverk og rettstradisjon, uten noen garanti for at svaret ville bli sammenfallende med domstolen i Georgia.

Graden av skyld – verken uaktsomhet eller «*actual malice*»

Retten foretok deretter en sontring mellom to skyldformer som brukes ved vurderingen av ærekrenkelser i

Georgia, der Walters' status som privat eller offentlig person sto sentralt. Walters hadde selv argumentert for at han ikke var en offentlig person.

- **For private personer** kreves det vanlig uaktsomhet
- **For offentlige personer**, som etter rettens vurdering inkluderte Walters, kreves det «*actual malice*» – altså kunnskap eller grov likegyldighet om at utsagnet er falskt. Dette innebærer en høy terskel, og et krav om «*a subjective awareness of probable falsity when the material was published*».

Dommeren var ikke enig med Walters i at han var å anse som en privatperson. Riktignok hadde Walters vist til at han bare var blitt intervjuet to ganger av nasjonale medier, henholdsvis Fox News og NBC. Likevel ble det lagt vekt på at han var fast vert for to nasjonalt syndikerte radioprogrammer, og omtalte seg selv som «*the loudest voice in America fighting for gun rights*». Den ivrige lytter kan høre Walters radioprogrammer seks dager i uken i til sammen ti timer ukentlig, med en lytterbase på 1,2 millioner personer. Han har gitt ut flere bøker om det andre grunnlovstillegget, som altså står sentralt i våpendebatten i USA. I tillegg satt han i styret for foreningen «*Citizens Committee for the Right to Keep and Bear Arms*», samt at han var talsmann for SAF.

Til tross for at Walters anses som en offentlig person, som igjen innebærer en annen ansvarsterskel, drøfter retten først om det foreligger uaktsomhet i dette tilfellet. Retten legger i denne gjennomgangen vekt på at Walters ikke har vist til noen standard eller prosedyrer som OpenAI burde ha implementert eller fulgt opp for å avverge feilaktige påstander. Det var heller ikke forsøkt dokumentert fra Walters at OpenAI ikke hadde fullt opp slike rutiner eller opptråd klanderverdig. Retten viser til forklaring fra et ekspertvitne engasjert av OpenAI,

som slo fast at OpenAI er en ledende aktør innen AI-industrien i arbeidet med å unngå og redusere antall feil som genereres av AI-tjenesten.

Walters argumenterte med at det i seg selv var uaktsomt å tilby en AI-tjeneste som genererte denne typen feilmeldinger. Dette førte ikke frem. Retten viser til at en slik betraktning ville innebære at selv en liten mulighet for eventuelle feil skulle medføre at tjenesten måtte holdes stengt for allmenheten. Dette var det etter rettens mening ikke grunnlag for:

«Walters' argument would mean that an AI developer like OpenAI could not operate a large language model like ChatGPT at all, no matter the care it took to reduce the risk of errors, without facing liability for any mistaken output the model generated. That is not a negligence standard, and both Georgia law and federal constitutional law prohibit applying it to Walters' defamation claim.»

Walters argument har mye til felles med et objektivt ansvar, men han fikk altså ikke gjennomslag for denne tilnærmingen.

Som omtalt ovenfor landet retten på at Walters var en offentlig person, som igjen innebar en høyere terskel for å reagere på et ærekrenkende utsagn. I norsk rett dreier dette spørsmålet seg særlig om at en offentlig person utløser en sterkere grad av allmenn og offentlig interesse. I Georgia viser retten også til at den offentlige personen i tillegg vil ha tilgang til effektive kommunikasjonskanaler som gir en realistisk mulighet for å bøte på skaden. I denne saken landet retten på at Walters som et minimum var en «*limited purpose public figure*». I dette ligger at Walters innenfor debatt eller diskusjon på dette området må oppfattes å være en offentlig person, og må tåle mer enn en privatperson. Retten fant at debatten i dette tilfellet kretset rundt det politiske spørsmå-

let om våpenrettigheter, der Walters altså var en offentlig person.

Det neste spørsmålet ble dermed om det forelå en spesiell form for forsett fra OpenAI, såkalt «*actual malice*» som kreves for ærekrenkelser overfor offentlige personer. Det underliggende rettslige spørsmålet ble dermed om Walters kunne godtgjøre at OpenAI hadde positiv kunnskap om at de ærekrenkende utsagnene var uriktige, eller var klar over at det var sannsynlig at den aktuelle informasjonen var eller ville bli gjenstand for spredning. Retten omformulerte denne problemstillingen med et sitat fra en tidligere sak: Hvorvidt det foreligger «*a subjective awareness of probable falsity when the material was published*».

Retten slår umiddelbart fast at Walters ikke hadde fremlagt noe dokumentasjon som kunne underbygge noe slikt forsett fra OpenAI. Videre legger retten til grunn lignende betraktninger som vi allerede har sett i vurderingen ovenfor knyttet til uaktsomhet, der det konstateres at OpenAI har gjort mer enn andre i bransjen for å unngå feil og advare om de feil som likevel oppstår.

Den neste drøftelsen følger opp videre i samme spor. Walters anførte at OpenAI likevel var ansvarlig for ærekrenkelser fra ChatGPT – at virksomheten opererte vel vitende om at feil av denne typen ville kunne oppstå. Her legger retten til grunn en formalistisk tilnærming, og viser til at Walters ikke har fremlagt noe klart og entydig bevis knyttet opp mot det konkrete utsagnet (sitatene retten benytter er fra en annen rettsavgjørelse):

«The mere knowledge that a mistake was possible falls far short of the requisite 'clear and convincing evidence' that OpenAI actually 'had a subjective awareness of probable falsity' when ChatGPT published the specific challenged output itself.»

Rettens tilnærming til disse anførselene fra Walters er kanskje litt lettvint. Dommeren legger vekt på at

Walters ikke kunne legge frem bevis for juryen som viste at det konkrete utsagnet – «*the specified challenged output itself*» – ble publisert til tross for at OpenAI var kjent med at dette var feil. Problemstillingen virker her noe konstruert. Det aktuelle utsagnet har ikke eksistert før ChatGPT svarer på spørsmålet fra Riehl. OpenAI har med andre ord ingen kunnskap om utsagnet, og følgelig kan det ikke bevises at det foreligger *actual malice* opp mot denne ord-sammenstillingen. Det Walters anfører er imidlertid en form for *dolus eventualis*. I denne ansvarsnormen foreligger det en form for forsett der gjerningspersonen kan forutse en mulig skadelig konsekvens av sin handling, men likevel gjennomfører den. Det foreligger altså en aksept av konsekvensen som handlingen vil kunne medføre.

OpenAI vil være klar over at enhver kobling mellom en navngitt person og utsagn som formidles om eller i tilknytning til denne personen fra ChatGPT vil kunne inneholde feil. Dette reiser en rekke spørsmål som retten unnlater å gå inn på. Ett slikt spørsmål er om det er tilstrekkelig å vise til at OpenAI er ledende innen industrien når det gjelder å begrense feil og uklarheter i svarene fra sin AI-tjeneste. Dette er en relativisering som langt på vei pulveriserer ethvert ansvar under henvisning til hva andre aktører gjør. Deres bransje for øvrig gjør lite på dette området, vil det innebære en lavere standard til hva som kan forventes i den rettslige vurderingen. Dette kan være et relevant moment, men jeg stiller spørsmål ved – også under rettssystemet i Georgia som anvendes her – om dette skal tillegges så mye vekt som det ser ut til i dette tilfellet. Det er ikke vanskelig å se for seg at en kartlegging av denne type rutiner og praksis hos ulike konkurrerende virksomheter også vil kunne by på praktiske problemer, eksempelvis ved at en god prosess på verifikasjon vil kunne øn-

skes bevart som en forretningshemmelighet.

Ikke grunnlag for krav om skadeerstatning

Til sist avviste retten Walters' krav om erstatning grunnet et fullstendig fravær av dokumentert økonomisk eller omdømmemessig skade. Walters hadde selv innrømmet at han verken hadde mistet inntekter, sponsorer eller blitt utsatt for offentlig fordømmelse. Journalisten som mottok utsagnet, republiserte det aldri og anså selv utsagnet som «absurd».

Domstolen måtte også ta stilling til om det forelå grunnlag for såkalte «*punitive damages*», som vi kjenner som en form for straffeerstatning der det preventive elementet er viktig. Et vilkår for denne type erstatning er at den krenkede selv har krevd retting eller tilbakekall av utsagnet fra ytreren. Walters hadde ikke fremmet noe slikt krav, og argumenterte med at dette uansett vanskelig ville være vanskelig å etterkomme i dette tilfellet. Domstolen viser imidlertid til at kravet om retting er et absolutt vilkår, og at det er uten betydning om OpenAI rent faktisk kunne ha utbedret situasjonen. Dette kravet ble altså avvist.

Walters vant heller ikke frem med en ytterligere anførsel om at allerede ærekrenkelsens art tilsa at det måtte ha skjedd en skade som kunne gi hjemmel for et krav om erstatning. En slik anførsel er basert på en slags presumsjon for at utsagnet nødvendigvis må ha forårsaket noen form for skade, som derfor skal kompenseres. Retten viste igjen til at det overhodet ikke var påvist *noen* form for skade: «*It is undisputed that Walters could not have sustained any injury of any kind, whether a quantifiable economic loss or any 'injury to the reputation' that 'flow[ed]' from the challenged ChatGPT output*». Dermed var det ikke tilstrekkelig å vise til en presumsjon som etter internretten har en høy terskel for anvendelse.

Oppsummering

Denne avgjørelsen ble altså avgjort på flere separate grunnlag som alle hver for seg var tilstrekkelige til å frifinne OpenAI. Ved at dommeren drøfter alle punktene fullt ut får vi likevel her et dekkende bilde av hvordan de ulike elementene i en ærekrenkelsesvurdering slår ut i en konkret sak om AI-generert ærekrenkelse.

ChatGPT ble i denne saken betraktet som et verktøy snarere enn en personlig ansvarlig ytrer. Dermed legges hovedvekten av rettens vurdering på hvordan en rimelig mottaker oppfatter innholdet, hvorvidt det finnes tilstrekkelig kontekst som svekker utsagnets troverdighet og i hvilken grad tilbyderer har informert om risikoen for feil.

Retten anerkjente AI-modellers feilopplysninger og hallusinasjoner, men påpekte at utviklere som aktivt forsøker å redusere feil og varsler brukerne, ikke uten videre handler uaktsomt. Dermed blir vurderingen av aktsomhet og skyldgrad delvis avhengig av dokumenterbare prosesser for risikotiltak og -begrensning.

Retten behandlet ikke ChatGPT som en utgiver eller ytrer i tradisjonell forstand, men foretok en konkret vurdering basert på begrensningene som ligger i en maskinlæringsmodell av denne typen. Denne tilnærmingen har en del til felles med tidligere avgjørelser som fritar bokhandlere og nettplattformer fra innholdsansvar. En sak som gikk på dette temaet var *Smith v. California*, 361 U.S. 147 (1959) som gikk for USAs føderale siste instans. I denne saken var innehaveren av en bokhandel domfelt for brudd på et lokalt forbud mot en bok i sortimentet til tross for han ikke var kjent med innholdet. Mye av denne avgjørelsen dreier seg om spørsmål knyttet til *chilling effect* under ytringsfriheten, altså at en normativ regel kan virke dempende på ytringsfriheten utover det som er strengt nødvendig eller ønskelig:

«By dispensing with any requirement of knowledge of the contents of the book on the part of the seller, the ordinance tends to impose a severe limitation on the public's access to constitutionally protected matter. For if the bookseller is criminally liable without knowledge of the contents, and the ordinance fulfills its purpose, he will tend to restrict the books he sells to those he has inspected; and thus the State will have imposed a restriction upon the distribution of constitutionally protected, as well as obscene literature.»

Førstvoterende viser altså her til virkningen av en streng og objektiv tolkning av bokforbudet opp mot bokhandlerens aktsomhetsgrad. I den videre drøftelsen viser førstvoterende til den chilling effect som dermed virker videre ut i samfunnet:

«The bookseller's self-censorship, compelled by the State, would be a censorship affecting the whole public, hardly less virulent for being privately administered. Through it, the distribution of all books, both obscene and not obscene, would be impeded.»

Virkningen av en streng håndheving av forbudet vil altså ramme videre enn bare bokhandleren. Samfunnet som helhet vil rammes ved at bokhandlere generelt vil ha et insentiv til å selv-sensurere tilbudet av bøker, som igjen rammer befolkningen som helhet. Argumenter knyttet til chilling effect ser vi også klare spor av i norsk rett, og betraktningen har vært avgjørende i flere prinsippaker om ytringsfrihet, herunder Runesten-saken Rt-2010-1381, omtalt av undertegnede i LoD-2011-105-15 og LoD-2024-160-57. I bokhandler-saken siterer retten fra en tidligere sak om ytringsfrihet (*Roth v. United States*, *supra*, 354. U.S. 488), i et slikt malerisk språk som vi kanskje savner i blant fra vår egen dommerstand:

«The fundamental freedoms of speech and press have contributed greatly to the

development and wellbeing of our free society, and are indispensable to its continued growth. Ceaseless vigilance is the watchword to prevent their erosion by Congress or by the States. The door barring federal and state intrusion into this area cannot be left ajar; it must be kept tightly closed, and opened only the slightest crack necessary to prevent encroachment upon more important interests.»

Tilbake til vår sak om ChatGPT ser vi altså at det fremover vil stå sentralt å balansere flere ulike hensyn. I tråd med bokhandlersaken, ser retten på ChatGPT som et verktøy heller enn utgiver eller redaktør. Ansvar plasseres langt på vei hos brukeren, som må gjøre seg kjent med begrensninger, troverdighet og andre faktorer som har betydning for AI-verktøyet ytringer og leveranser. Det autonome AI-verktøyet

plasseres i samme kategori som bokhandleren, og er altså å betrakte som en mellommann i denne sammenhengen.

I den konkrete saken om Walters gikk det på ærekrenkelser og personlig omdømme opp mot behovet for å unngå en chilling effect, men vi ser en rekke andre, og kanskje større problemstillinger som ligger i samme retning. Vi kan forvente at i fremtidige saker vil den konkrete vurderingen stå helt sentralt, og at det vil danne seg ulike spor for ulike typer tjenester og bruksområder. Det er lettere å akseptere feil der dette nærmest ligger i dagen og ikke forårsaker noen skade. På områder som helse, nyhets- og faktaformidling, akademiske fag og lignende vil det raskt oppstå større problemer om det ikke utvikles klare retningslinjer og normer i tiden fremover.

Dommen i *Walters v. OpenAI* gir AI-utviklere et viktig, men betinget vern – forutsatt åpenhet, ansvarlig systemdesign og klare ansvarsfraskrivelser. For rettsanvendere og jurister gir saken en pekepinn på flere spørsmål som vil oppstå fremover, og som må behandles i et større perspektiv enn den konkrete saken retten her hadde til behandling. Teknologi kan som kjent ikke unndras rettslig kontroll, og er underlagt vårt eksisterende rettslige rammeverk. Samtidig kan den teknologiske utviklingen innebære at vi oppdaterer vår juridiske grammatikk og at vi kanskje må løfte blikket litt mer enn vanlig. Det er ønskelig ikke bare å få til gode løsninger, men forsøke å samordne regler og praksis mot aktører som opererer på en internasjonal arena og på tvers av landegrenser.



Av Peter Wahlgren

Peter Seipel 1939–2025

Peter Seipel, landets första professor i rättsinformatik, gick bort den 23 mars 2025. Peter Seipel var en pionjär som tidigt insåg betydelsen av informationsteknologin (IT) och förstod att tekniken skulle medföra långtgående konsekvenser för samhällsutvecklingen, den juridiska sektorn och det juridiska arbetet. Han hade förmågan att kombinera denna insikt med praktiska åtgärder och startade 1968 med stöd av professor Jan Hellner *Arbetsgruppen för ADB och juridik*. Arbetsgruppen blev världens första akademiska initiativ med denna inriktning och den omvandlades 1982 till *Institutet för rättsinformatik* (IRI). Detta skedde samtidigt som gruppens externa seminarieverksamhet avknoppades till den då nybildade *Svenska föreningen för ADB och juridik*, numera *Svenska föreningen för IT och Juridik* (SIJU). IRI blev ett renodlat forskningsinstitut, vilket tydligt angavs i den engelska beteckningen *The Swedish Law and Informatics Research Institute*.

Initiativet var ovanligt eftersom inte bara regleringsfrågor sattes i fokus, något som kunde förväntats då hemorten var den juridiska fakulteten vid Stockholms universitet. Projektet var uttryckligt tvärvetenskapligt. Det handlade lika mycket om att förstå de tekniska förutsättningarna som de juridiska implikationerna. Förståelsen var att de sätt på hur tekniska lösningar utformas medför olika problem och att det därför är nödvändigt att ta hänsyn till juridiken redan på designstadiet. I inbjudan till arbetsgruppens första seminarium angavs följaktligen att även strukturering av datafiler skulle diskuteras.



Peter Seipel 1939–2025

Peters intresse för ämnet var inte unikt, men att det blev IT och juridik var enligt hans egen förklaring en slump. Bakgrunden var att han första dagen som student på universitetet hamnade på fel introduktionsföreläsning. Avsikten var att studera matematik, men han hittade inte rätt byggnad utan hamnade på Juridiska fakultetens introduktion. Vi kan vara tacksamma för misstaget. Fröet såddes där och studierna resulterade i en jur. kand., en fil. kand., kurser i ADB, och en första anställning som amanuens på Juridicum, däremellan tolkskolan.

Idén att juridiken skulle samarbeta med informationsteknisk expertis och att detta motiverade etablerandet av ett nytt akademiskt ämne var inte okontroversiell. Kritik förekom och arbetet mötte motstånd. Andra valde att anamma en huvudet-i-sanden-strategi, och att i konkurrens

med etablerade juridiska discipliner uppbringa resurser för projektet var inte enkelt. Peters personlighet; sociala kompetens och förmågan att knyta kontakter blev nyckeln. Allt i kombination med en stor arbetskapacitet som till betydande del användes till att pedagogiskt motivera ämnets betydelse. Väl illustrerat i hans första artiklar i *Svensk juristtidning* 1970: *Om användning av automatisk databehandlingsteknik och automatiserad informationssökning inom juridiken*.

Artiklarna är en presentation av ämnet på 60 sidor där den första delen är en pedagogisk genomgång av databehandlingens terminologi, avgränsning och uppdelning av ämnesområdet, problemställningar, registervård, rättsstatistik med mera. Publiceringen är en prestation i sig. Inte bara för att den skedde i en tidskrift som vid den tiden inte var känd för nytänkande i ämnesvalet. Texten innehåller ett avsnitt betitlat *ADB-teknik i samband med normutformning och normtillämpning* som handlar om att utveckla lagstiftningstekniken, författad 55 år innan den svenska digitaliseringsmyndigheten DIGG 2024 publicerade vägledningen *Skapa automationsvänliga regelverk*.

Forskning i rättsinformatik har i hög grad varit beroende av extern finansiering och eftersom ämnets inhemska utveckling var trevande var det nödvändigt att söka inspiration från andra länder, vilket vid tiden före internet förutsatte korresponderande med hjälp av skrivmaskin och postverk. Peters språkkunskaper var här till en stor hjälp och litteratur på många språk anskaffa-

des. Ambitionen var initialt att täcka allt vad som publicerades på de nordiska språken, engelska, franska, ryska och tyska. En strävan som snart fick överges i takt med att publiceringstakten ökade.

Efter att 1971 hunnit med en licentiatavhandling om huruvida datorprogram kan och bör skyddas av upphovsrätt disputerade Peter 1977 på avhandlingen *Computing Law: Perspectives on a new Legal Discipline*. Ämnet presenterades med utförliga motiveringar och talrika exempel. Arbetet avslutades med ett klassifikationsschema över rättsinformatikens delämnen. Taxonomin användes praktiskt för att sortera litteraturen och utgör stommen i det omfattande bibliotek som byggts upp vid IRI. Klassifikationen går fortfarande att använda som bas, trots att många nya företeelser tillkommit. Forskningsbiblioteket och materialet från de talrika projekt som genomförts blev med tiden en unik dokumentation av ämnets tidigaste skede. Detta även internationellt och ett arbete med att överföra IRIs äldre forskningsmaterial och bibliotekssamlingar till det svenska riksarkivet är initierat.

Parallellt med att starta forskningsprojekt och delta i utvecklingsarbete verkade Peter för att etablera rättsinformatik som ett ämne i juristutbildningen. Något som successivt lyckades och kurser är numera också återkommande på data- och systemvetenskapliga utbildningar. Detta var ett viktigt arbete vilket gjorde det möjligt att få en bättre

kontinuitet i verksamheten genom att undervisningstjänster inrättades.

” Peter var därtill en bildad person, initierad och kunskapsrik med välbetänkta insikter, nära nog oavsett vilket ämne som samtalen kom att röra sig om. Han var i flera avseenden en förebild, och vi är många som har honom att tacka för mycket.

Organisatoriskt koncentrerades arbetet med att stärka samarbeten och utveckla nätverk, nationellt såväl som internationellt. Inhemskt illustrerat av Initiativet att etablera *Stiftelsen för rättsinformation* (1988), en sammanslutning av rättsväsendets centrala myndigheter, organisationer och företag. Peter var också vice ordförande i 1998 års IT kommission och ordförande för regeringens It-rättsliga observatorium 1995–2003.

Internationellt deltog Peter som expert i flera utredningar och han var medlem i EUs *Legal Advisory Board*. Som internationellt efterfrågad föreläsare kunde han också bygga upp ett brett internationellt kontaktnät. Speciell omsorg ägnades åt det nordiska samarbetet och betydelsefullt var de tidiga kontakterna med *Norwegian Center for Computers*

and Law vid *Oslo universitet*. Något som ledde till etablerandet av en serie nordiska konferenser i rättsinformatik och en *Nordisk årsbok i rättsinformatik* (1984). Peter utsågs till hedersdoktor vid *Lapplands universitet* i Rovaniemi i samband med dess etablerande av ett Institut för rättsinformatik.

Grunden som lades av Peters långsiktiga arbete resulterade i att rättsinformatik tidigt utsågs till ett profilämne vid Stockholms universitet och att IRI i två externa utvärderingen under de senaste åren omnämnts som världsledande inom området.

Peter Seipel blev ämnet trogen hela sitt yrkesverksamma liv. Ständigt aktiv med stort engagemang. Han var under en tid också Juridiska fakultetens dekanus. Även detta ett uppdrag skött med kreativitet och nogsamhet, där möten, beslut och samtal dokumenterades i löpande anteckningar. Omvittnad är därtill Peters vänliga personlighet, alltid beredd att stödja och uppmuntra yngre medarbetare. Peter var därtill en bildad person, initierad och kunskapsrik med välbetänkta insikter, nära nog oavsett vilket ämne som samtalen kom att röra sig om. Han var i flera avseenden en förebild, och vi är många som har honom att tacka för mycket. Peter Seipel blev 85 år.

*Peter Wahlgren,
peter.wahlgren@juridicum.su.se,
professor vid det svenska institutet för
rättsinformatik <http://irilaw.org/>.*



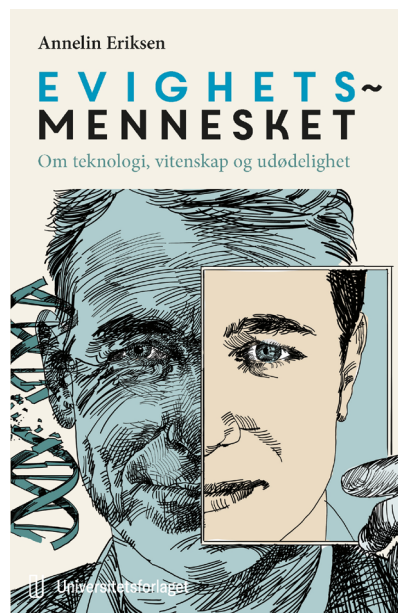
Evighetsmennesket

Om teknologi, vitenskap og udødelighet

Forfatter Annelin Eriksen

Oslo: Universitetsforlaget 2023, 168 s.

ISBN: 9788215065151



Bio-hackere, transhumanister, og utviklere av menneske-maskin-symbioser er i ferd med å flytte de fysiske grensene og rammene for et menneskes liv. Med dette utfordrer de også grunnleggende ideer knyttet til hva det vil si å være et menneske. Kan et menneske, gjennom vitenskap og teknologi, bli noe helt annet enn vi er i dag? Noe helt annet enn den biologiske kroppen? Er hjernen din et informasjonssystem som kan kopieres og lastes opp i maskiner? Vil i så fall bevisstheten også følge med, eller blir resultatet en maskin som bare tenker helt likt deg?

Spørsmålene som melder seg er ikke lette å svare på, hverken i vitenskapelig eller filosofisk forstand. Men at vi er i ferd med å forstå aldring som noe unaturlig og døden som noe unødvendig, er i seg selv en interessant kulturell utvikling. Hvor kommer dette behovet for å leve evig fra? Hvorfor skal mennesket bli noe annet?

Evighetsmennesket gir en kulturhistorisk og kulturanalytisk gjennomgang av tekno-vitenskapelige udødelighetsideer, prosjekter og bevegelser fra USA, Europa og Russland. Forfatteren gir et portrett av mennesket som ikke vil dø, som vil bli noe annet enn den aldrende, biologiske kroppen. Hun viser også hvordan dette ønsket om å leve evig har rot i noe som er mye mer allment enn bevegelsen selv - hvordan det er et ektefødt barn av en spesi-fikk kulturhistorie og samfunns-kontekst, med røtter i viktige internasjonale vitenskaps- og teknologi-miljøer.

Boken er skrevet som en populærvitenskapelig antropologisk monografi. Den retter seg mot studenter i sosialantropologi og andre samfunnsfag som arbeider med forholdet mellom mennesker, samfunn og teknologi, samt et bredere publikum med interesse for tematikken.



Lovdatas KI-søk er ikke bare et nytt verktøy – det er en ny standard

Vi kombinerer teknologi og tillit, og gir deg trygghet i møte med juridisk problemløsning.

Når du stiller et spørsmål i Lovdatas nye KI-søk, får du langt mer enn bare treff på nøkkelord, du får hjelp til å forstå – og løse – det juridiske spørsmålet du faktisk lurte på.

Ved å kombinere det beste fra våre strukturerte juridiske kunnskapsdatabaser med kraften i moderne kunstig intelligens, tilbyr vi en ny måte å finne og forstå rettskilder på. Kjernen i løsningen er en teknologi som kombinerer dokumentbasert søk med avansert språkmodellering.

Slik fungerer det:

Spørsmålet ditt forbedres automatisk

Uansett hvordan du formulerer deg, tolker systemet spørsmålet ditt og

oversetter det til et presist juridisk språk med rett terminologi og struktur. Eventuelle skrivefeil og forenklet språk håndteres sømløst.

Relevante rettskilder hentes frem

Søket gjøres i Lovdatas omfattende dokumentbaser etter rettskilder som ikke bare inneholder lignende ord, men som faktisk handler om det samme temaet. Vi finner frem til lover, forskrifter, forarbeider, rettsavgjørelser, rundskriv, nemnder og mye mer. Du får en oversikt over de relevante rettskildene sammenstillingen bygges på slik at du kan ettergå, på samme måte som før.

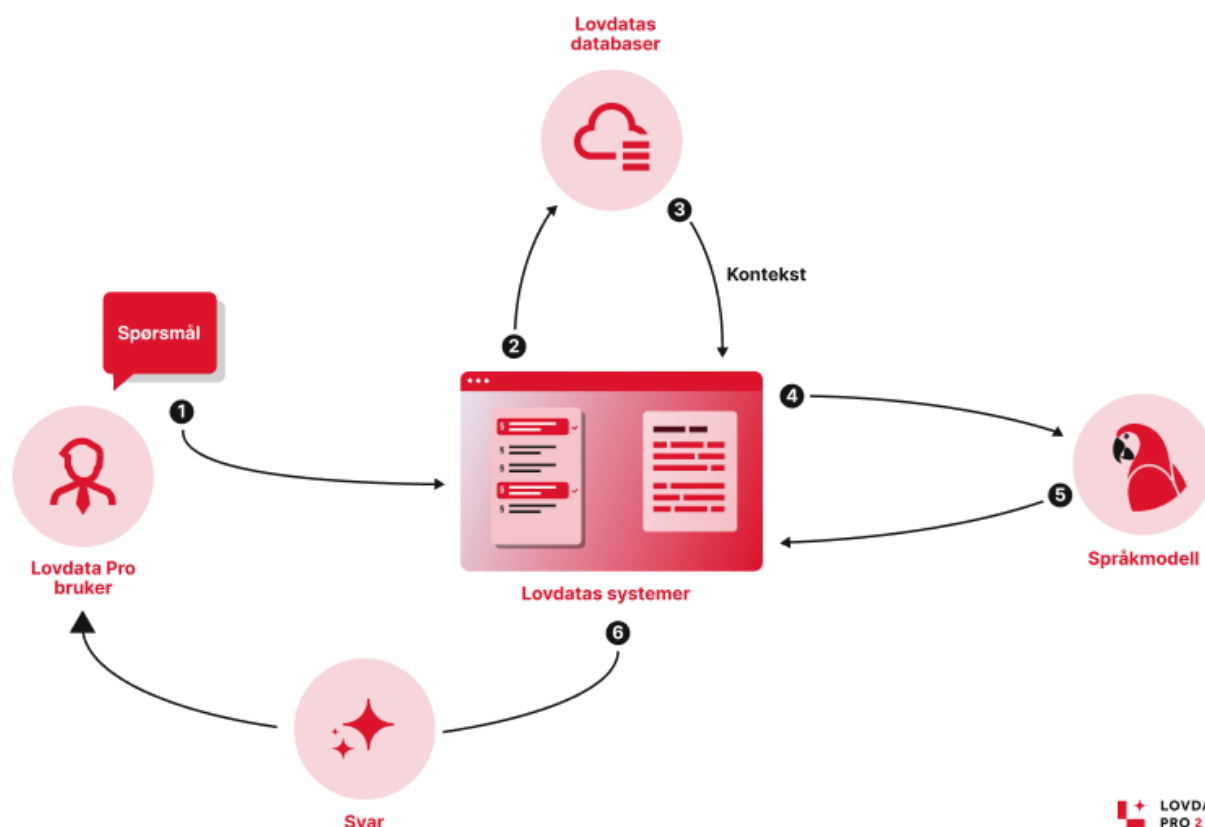
Kontekst og sammenheng analyseres

Systemet analyserer hvordan rettskilder henger sammen gjennom

henvisninger, juridiske begreper og tematiske koblinger. Dette gir en dypere forståelse av konteksten og sørger for at søket treffer både bredt og presist.

En stor språkmodell genererer svar

Det mest relevante materialet sendes videre til en språkmodell, som oppsummerer og forklarer rettskildene. Resultatet er en nyttig og informativ sammenstilling som hjelper deg å forstå hva rettskildene sier – og hva du bør gjøre videre.





Klarity: Jusstjenesten vi ikke visste vi trengte

Av Kristine Brokhaug, CMO, Klarity.

Kunstig intelligens møter jussen – og gir privatpersoner innsikt, trygghet og bedre beslutningsgrunnlag.

For mange privatpersoner kan møtet med det juridiske systemet oppleves som overveldende. Et komplekst og teknisk lovverk, høye terskler og usikkerhet rundt omfang og kostnader gjør at mange lar være å forfølge rettighetene sine. Samtidig har advokatbransjen selv etterlyst mer effektiv bruk av tid og ressurser, særlig i møte med et økende antall henvendelser og saker med uklart utgangspunkt. **Det er her Klarity kommer inn.**

Klarity er en ny norsk KI-basert plattform som lar privatpersoner få en objektiv evaluering av saken sin, før de eventuelt kontakter en advokat. Ved å kombinere kunstig intelligens med juridisk metode, gir Klarity brukerne et **klart, forståelig og strukturert bilde** av hvordan saken står juridisk sett. Tjenesten er ikke en erstatning for advokatbistand, men et filter og en veiviser: Den hjelper brukeren å forstå om det i det hele tatt er grunnlag for å gå videre, og hvordan man i så fall kan gjøre det.

Et digitalt første steg i rettsprosessen

Klarity er utviklet nettopp fordi mange i dag står uten verktøy til å vurdere egen situasjon.

«Skal jeg kontakte advokat?»

«Har jeg en sak?»

«Hva risikerer jeg?»

«Hva koster det?»

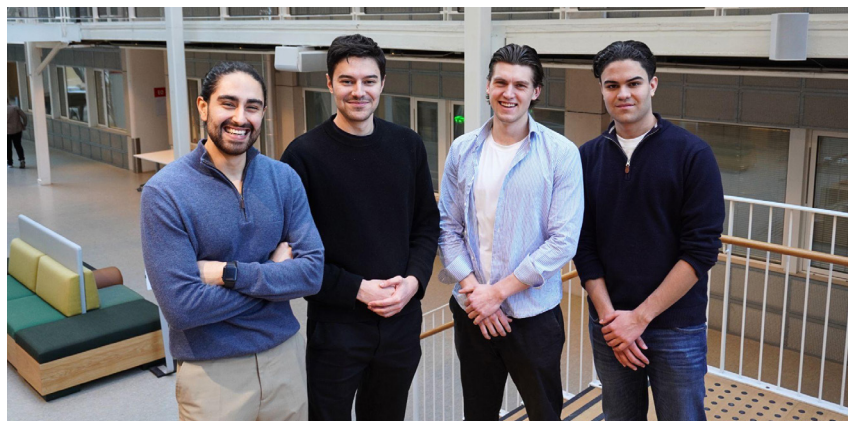


Foto: Kristine Brokhaug

Med Klarity kan man enkelt og trygt beskrive sin sak på egen hånd og få en evaluering basert på relevante rettsregler. Modellen som ligger bak er trent på norsk rettskildemateriale og har som mål å fange opp essensen i det brukeren beskriver og oversette dette til juridisk relevante evalueringer.

Bedre beslutninger, raskere prosesser

Klarity er laget med to formål:

1. Å gjøre jussen mer forståelig og tilgjengelig.
2. Frigjøre tid i vurderingsprosessen til advokater

Mange advokater bruker i dag tid på å avklare hvorvidt en potensiell sak i det hele tatt har juridisk grunnlag. Med Klarity som første steg vil slike evalueringer i større grad være gjort på forhånd. *Det gir både klient og advokat en bedre start.*

Dessuten jobber Klaritys modell raskt. På få minutter kan den gi en evaluering av en sak, basert på en inngående beskrivelse fra brukeren. Dette gir både effektivitet og tilgjengelighet, som bidrar til en mer bærekraftig bruk av juridiske ressurser.

Et viktig skritt mot tilgjengelig juss

Loverket gjelder oss alle, men er langt fra tilgjengelig for alle. Det er et demokratisk problem når store deler av befolkningen ikke forstår eller klarer å bruke rettighetene sine. Her kan Klarity gjøre en forskjell. **Ved å senke terskelen for juridisk innsikt**, bidrar plattformen til økt rettssikkerhet og til et **mer inkluderende rettssystem**.

Tjenesten er i stadig utvikling, og ambisjonen er klar: Klarity skal være inngangsdøren til jussen for folk flest. Ikke som erstatning for advokater, men som et lavterskeltilbud som gjør veien inn i rettssystemet mindre skremmende og mer håndterbar.

Om Klarity

Klarity.no er en norskutviklet juridisk KI-tjeneste som gir privatpersoner mulighet til å få en objektiv evaluering av saken sin. Plattformen er bygget på norsk rett og skreddersydd for norske forhold. Plattformen har evaluert 100+ saker, siden lansering 3. mars 2025.



Gorrissen Federspiel

Tue Goldschmieding

Nyt om persondataret i Danmark

Der forelå ikke en tilstrækkelig usikkerhed om hvorvidt indhentelse af teleoplysninger var i strid med EU-retten

Højesteret afsagde den 29. januar 2025 dom i sag SS-46/2024-HJR om den danske anklagemyndigheds (»Anklagemyndigheden«) anmodning om editionspålæg overfor teleselskaber, med henblik på udlevering af ikke-logningspligtige teleoplysninger.

Anmodningen om udlevering af teleoplysningerne skete i forbindelse med en narkokriminalitetsefterforskning, og teleselskaberne var i besiddelse af teleoplysninger vedrørende de mobiltelefoner, som anklagemyndigheden antog at tiltalte havde benyttet.

Der var tale om ikke-logningspligtige teleoplysninger, da de anmodede teleoplysninger ikke var omfattet af teleselskabernes registrerings- og opbevaringspligt efter den danske lov om rettens pleje, jf. lovebekendtgørelse nr. 1160 af 5. november 2024 (»retsplejeloven«) § 786 a - § 786 e. Retsplejelovens regler om registrerings- og oplysningspligt er fastsat i medfør af direktiv 2002/58/EF af 12. juli 2002 (»e-databeskyttelsesdirektivet«) artikel 15, stk. 1.

Tiltaltes advokat påstod, at afgørelsen på Anklagemyndighedens anmodning om at få udleveret teleoplysningerne måtte udsættes, indtil EU-domstolen havde taget stilling i den verserende sag C-241/22, da udleveringen kunne være i strid med EU-retten. Sag C-241/22 om-

handler retshåndhævende myndigheders adgang til trafik- og lokaliseringsdata, der ikke lagres på grundlag af retsfor skrifter, som er udstedt i medfør af databeskyttelsesdirektivet artikel 15, stk. 1.

Højesteret stadfæstede landsrettens resultat og fastslog, at afgørelsen om editionspålæg ikke skulle udsættes, da der ikke eksisterede en tilstrækkelig usikkerhed om, hvorvidt indhentelse af teleoplysningerne kunne være i strid med EU-retten.

Læs dommen fra Højesteret her: <https://domsdaten.dk/#/sag/7139/8577>

Oplysninger om parterers navne på retslisten var ikke oplysninger om den ene parts seksuelle forhold

Højesteret afsagde den 7. marts 2025 kendelse i sag BS-36701/224-HJR om et forbud mod publicering af en dokumentarfilm, som vedrørte sexisme i mediebranchen.

Forbudssagen blev behandlet ved Københavns Byret, og på byrettens hjemmeside blev retslisten offentliggjort på dagen. Parternes navne fremgik, samt at sagen drejede sig om en forbudssag vedrørende presse. Sagsøgeren anmodede om, at sagens oplysninger ikke skulle fremgå af denne retsliste. Dette afviste både byretten og landsretten.

Spørgsmålet for Højesteret var, hvorvidt sagens parterers navne ikke skulle være fremgået af byrettens retsliste med henvisning til, at der var tale om oplysninger om seksuel-

le forhold, der er beskyttet mod offentliggørelse efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 9, stk. 1.

Højesteret udtalte at den omstændighed, at det var offentligt tilgængeligt, at en sådan dokumentar var blevet produceret, og at der var rygtedannelse vedrørende den omhandlede part, ikke kunne medføre, at oplysninger på retslisten udgjorde sådanne oplysninger om seksuelle forhold.

Højesteret fandt på den baggrund, at retslisten ikke indeholdt oplysninger om partens seksuelle forhold efter bekendtgørelse nr. 546 af 18. juni 2004 (»retslistebekendtgørelsen«) § 5, stk. 3, som undtager de oplysninger, som er omfattet af GDPR artikel 9, stk. 1, der beskytter visse oplysninger fra at blive offentliggjort på internettet. Det var derfor berettiget, at byretten havde offentliggjort en retsliste på internettet med blandt andet sagens parterers navne. Højesteret stadfæstede herefter landsrettens kendelse.

Højesteret udtalte desuden, at forbudssager ikke skal undtages fra retslisten efter retslistebekendtgørelsens § 1, stk. 2, der som udgangspunkt undtager alle sager som behandles ved foged- eller skifteretten fra at fremgå af retslisten. Forbudssager var ikke omfattet af denne undtagelse.

Læs kendelsen fra Højesteret her: <https://www.domstol.dk/media/ctzqoodbn/36701-anonymiseret-kendelse-til-hjemmesiden.pdf>

Kommune blev idømt bøde på 50.000 kr. for videregivelse af personoplysninger på selvbetjeningsløsning

Østre Landsret afsagde den 19. februar 2025 dom i sag SS-2302/2023-OLR om strafudmålingen for overtrædelse af GDPR artikel 32 i forbindelse med ukorrekt videregivelse af personoplysninger i breve fra den kommunale tandpleje.

Tiltalte, Frederiksberg Kommune, havde på deres selvbetjeningsløsning, »Min Tandpleje«, givet adgang til tandplejens breve til umyndige patienter, for begge indehavere af forældremyndigheden. Dette skete uden i det enkelte tilfælde at vurdere om de pågældende oplysninger måtte videregives til den anden forælder. Det medførte at der for personer med navne- og adressebeskyttelse, opstod en risiko for, at der blev givet uberettiget adgang til oplysninger om den ene forælders og/eller barnets adresse. Oplysningerne var tilgængelige på selvbetjeningsløsningen i en uafbrudt periode på 3 år.

Spørgsmålet for Østre Landsret vedrørte strafudmålingen. Retten understregede at GDPR artikel 83, stk. 2 skal anvendes ved påleggelse af bødestraf for overtrædelse af GDPR artikel 32, jf. den danske databeskyttelseslov, jf. lovbekendtgørelse nr. 289 af 8. marts 2024 § 41, stk. 3 om strafudmåling. Det fremgår af forarbejderne til databeskyttelsesloven at bødeloftet for offentlige myndigheder er lavere end for private.

Retten lagde vægt på flere hensyn i strafudmålingen. Disse hensyn er oplyst i GDPR artikel 83, stk. 2. Retten bemærkede, at overtrædelsen medførte en risiko for sikkerhedsbrud for maksimalt 56 personer. Frederiksberg Kommune havde underrettet disse personer. Alle omfattede personer havde navne- og adressebeskyttelse af andre årsager end den pågældende anden forælders forhold.

Retten lagde herudover vægt på at Frederiksberg Kommune hurtigt rettede sig efter at sikkerhedsbruddet blev konstateret, samt at Frederiksberg Kommune selv indberettede overtrædelsen til Datatilsynet. Der blev ligeledes lagt vægt på, at overtrædelsen var begået ved simpel uagtsomhed, og at Frederiksberg Kommune, som offentlig myndighed, ikke har opnået økonomiske fordele ved overtrædelsen.

Retten stadfæstede herefter byrettens dom og fastsatte bøden til 50.000 kr.

Læs dommen fra Østre Landsret her: <https://domsdatabasen.dk/#-sag/7244/8738>

Datatilsynet udtaler alvorlig kritik af arbejdsgivers behandling af tidligere ansats private e-mailkonto

Det danske datatilsyn (»Datatilsynet«) har den 25. oktober 2024 truffet afgørelse i en sag med journalnummer 2024-31-0529. Sagen vedrørte en arbejdsgivers behandling af en tidligere ansats personoplysninger ved at arbejdsgiveren havde tilgået, downloadet og videregivet e-mails fra den ansattes private e-mailkonto.

Datatilsynets afgørelse udsprang af, at der mellem en arbejdsgiver og en tidligere ansat, blev ført en civil sag om dennes illoyale adfærd ved den tidligere ansættelse. Arbejdsgiveren havde også indgivet en politianmeldelse om den ansatte. I forbindelse med den civile sag og politianmeldelsen, havde arbejdsgiveren tilgået den ansattes personlige e-mailkonto via den ansattes arbejdscomputer. Arbejdsgiverens formål med dette var at sikre sig bevismateriale til at retsforfølge og politianmelde den ansatte.

Datatilsynet fandt først og fremmest, at arbejdsgiveren ved at tilgå, downloade og videregive e-mails fra den tidligere ansattes private e-mailkonto, havde behandlet personoplysninger som defineret i GDPR.

Datatilsynet slog herefter fast, at arbejdsgiverens interesse i bevissikring ikke vejede tungere end hensynet til den ansattes interesse i privatliv omkring sin private e-mailkonto. Behandlingen af den tidligere ansattes personoplysninger ved at søge, opbevare og videregive oplysninger fra den private e-mailkonto til retten, var derfor ikke lovlig efter GDPR artikel 6, stk. 1, litra f. På den baggrund udtalte Datatilsynet alvorlig kritik af arbejdsgiveren.

Datatilsynet lagde ved sin afgørelse vægt på, at der var tale om en privat e-mailkonto, som blev opdaget ved et tilfælde, og at dette ikke afholdt arbejdsgiveren fra at behandle oplysningerne, selv efter at arbejdsgiveren havde konstateret at der var tale om en privat e-mailkonto.

Læs pressemeddelelsen fra Datatilsynet her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/feb/virksomhed-faar-alvorlig-kritik-for-behandling-af-tidligere-ansats-personoplysninger>

Læs afgørelsen fra Datatilsynet her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/okt/virksomhed-faar-alvorlig-kritik-for-behandling-af-tidligere-ansats-personoplysninger>

Datatilsynet gav F.C. København tilladelse til brug af automatisk ansigtsgenkendelse

Det danske datatilsyn (»Datatilsynet«) har den 18. december 2024 truffet afgørelse i en sag med journalnummer 2024-51-0012. Sagen vedrørte F.C. Københavns behandling af følsomme oplysninger i henhold til den danske databeskyttelseslov, jf. lovbekendtgørelse nr. 289 af 8. marts 2024 § 7, stk. 3, om behandling af oplysninger der er nødvendige af hensyn til væsentlige samfundsinteresser.

Datatilsynet behandlede sagen efter ansøgning fra den danske 3F Superligaklub, F.C. København, som havde ansøgt om tilladelse til



Illustration: Colourbox.com

behandling af biometrisk data i form af anvendelse af automatisk ansigtsgenkendelse. F.C. København ønskede tilladelse til at anvende automatisk ansigtsgenkendelse ved ethvert arrangement i både Parken Stadion i København og på udebanestadioner.

Datatilsynet gav F.C. København tilladelse til at anvende en sådan automatisk ansigtsgenkendelse i visse situationer. Datatilsynets tilladelse omfattede klubbens fodboldkampe, herunder træningskampe og UEFA-fodboldkampe, på Parken Stadion, ved adgangskontrollen ved indgangene, på stadion og tilhørende mobile anlæg. Datatilsynet henviste til, at anvendelsen ville bidrage til at sikre effektiv håndhævelse af karantæner. Datatilsynet gav dog ikke tilladelse til anvendelsen ved øvrige arrangementer.

Datatilsynet behandler fortsat den del af ansøgningen, der vedrører fodboldlandskampe.

Læs pressemeddelelsen fra Datatilsynet her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/jan/fc-koeben->

havn-faar-tilladelse-til-brug-af-automatisk-ansigtsgenkendelse

Læs afgørelsen fra Datatilsynet her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/dec/fc-koeben-havn-faar-tilladelse-til-brug-af-automatisk-ansigtsgenkendelse>

Berlingske efterlevede Datatilsynets påbud vedrørende cookie wall

Det danske datatilsyn (»Datatilsynet«) har den 17. januar 2025 truffet afgørelse i en sag med journalnummer 2023-431-0010. Sagen omhandlede det danske dagblad, Berlingskes, efterlevelse af Datatilsynets påbud af 14. februar 2024 vedrørende brug af cookie wall på hjemmesiden www.berlingske.dk.

I 2024 var Datatilsynet blevet bekendt med, at brugere af www.berlingske.dk, alene fik adgang til sidens indhold, hvis de gav samtykke til behandling af deres personoplysninger til statistiske- og markedsføringsformål. Brugere havde dermed ikke et frivilligt valg om at samtykke, hvis de ønskede at tilgå

indholdet på hjemmesiden, hvilket var i strid med GDPR artikel 6, stk. 1, litra a, jf. artikel 4, nr. 11, om krav til gyldigt samtykke.

Datatilsynet konkluderede den 17. januar 2025, at Berlingskes cookie wall nu opfyldte GDPRs krav til gyldigt samtykke efter GDPR artikel 6, stk. 1, litra a, jf. artikel 4, nr. 11. Datatilsynet vurderede, at de brugere af hjemmesiden, der ikke ønskede at samtykke til behandling af deres personoplysninger til statistiske- og markedsføringsformål, nu fik adgang til indhold, der i vidt omfang svarede til det indhold, som ville være tilgængeligt, hvis brugeren havde givet et sådan samtykke, både i mængde, funktion og kvalitet.

Datatilsynet understregede, at det afgørende for vurderingen af et gyldigt samtykke er, om brugere har et rimeligt alternativ, hvis de ikke ønsker at samtykke til behandling af deres personoplysninger via en cookie wall. Datatilsynet gjorde gældende, at et rimeligt alternativ skal indebære, at de ikke-samtykkende brugere får adgang til indhold, der i det væsentlige svarer til det indhold,

som brugere, der giver samtykke, får adgang til.

Læs pressemeddelelsen fra Datatilsynet her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/jan/berlingske-efterlever-datatilsynets-paabud-i-sag-om-cookie-wall-paa-berlingskedk>

Læs afgørelsen fra Datatilsynet her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2025/jan/berlingske-efterlever-datatilsynets-paabud-i-sag-om-cookie-wall-paa-berlingskedk>

Datatilsynet har udgivet to nye sikkerhedsforanstaltninger om sikker transmission

Det danske datatilsyn (»Datatilsynet«) udgav den 27. januar 2025 to nye foranstaltninger i Datatilsynets katalog over sikkerhedsforanstaltninger. Kataloget indeholder tekniske og organisatoriske foranstaltninger, de danske myndigheder kan overveje, i forbindelse med iagttagelsen af deres datasikkerhed.

Datatilsynet udgav foranstaltningerne »sikker transmission« og »sikker transmission med valideret afsender, modtager og indhold«, som adresserer forskellige sikkerheds-trusler.

»Sikker transmission« imødekommer risikoen for, at transmitterende data tilgås af uvedkommende. »Sikker transmission med valideret afsender, modtager og indhold« fokuserer ikke kun på risikoen for, at data læses af uvedkommende, men sikrer at afsenderen af data kan valideres og bevises.

Læs pressemeddelelsen fra Datatilsynet her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/jan/to-nye-sikkerhedsforanstaltninger-om-sikker-transmission>

Læs Datatilsynets foranstaltning vedrørende sikker transmission her: <https://www.datatilsynet.dk/regler-og-vejledning/behandlingssikkerhed/katalog-over-foranstaltninger/sikker-transmission>

Læs Datatilsynets foranstaltning vedrørende sikker transmission med valideret afsender, modtager og indhold her: <https://www.datatilsynet.dk/regler-og-vejledning/behandlingssikkerhed/katalog-over-foranstaltninger/sikker-transmission-med-valideret-afsender-modtager-indhold>

Det danske datatilsyns fokusområder i 2025

Det danske datatilsyn (»Datatilsynet«) offentliggjorde den 7. januar 2025 hvilke tilsynsaktiviteter, som Datatilsynet planlægger i 2025.

Datatilsynet bemærker, at de særligt vil have fokus på at fremkomme med initiativer vedrørende følgende emner:

- Beskyttelse af børn
- Digital tracking i det virkelige liv
- Registreres ret til sletning
- Styring af adgang til FMK hos privatpraktiserende læger og tandlæger
- Kunstig intelligens – generativ AI og sundhedssektor
- Retshåndhævelsesloven
- Behandling af personoplysninger i fælleseuropæiske informationssystemer
- Forsøg med fælles tilsyn med Finanstilsynet

Læs pressemeddelelsen fra Datatilsynet her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/jan/datatilsynets-fokusomraader-i-2025>

Av Tue Goldschmieding, partner i Gorrissen Federspiel og dansk redaktør for Lov & Data.



Delphi

Klara Thyren

Integritetsskyddsmyndigheten inleder GDPR-tillsyn efter omfattande dataintrång

Integritetsskyddsmyndigheten (IMY) inledde den 15 april 2025 tillsyn mot Sportsadmin AB ("Sportsadmin") för att granska de säkerhetsåtgärder som företaget tillämpar i sin tjänst, mot bakgrund av artikel 32 i GDPR. Tillsynen omfattar de tekniska och organisatoriska säkerhetsåtgärder som vidtagits för att skydda personuppgifter som behandlas i det digitala verktyg som idrottsföreningar och andra organisationer använder sig av för administration. Verktyget används bland annat för fakturering, kommunikation och medlemshantering.

Tillsynen sker med anledning av ett omfattande dataintrång den 16 januari 2025 som ledde till att personuppgifter för omkring två miljoner svenska individer extraherades och publicerades av angriparen på darknet. En betydande del av de drabbade är barn som deltagit i olika föreningar, och vissa av de exponerade uppgifterna tillhör dessutom personer med skyddade identiteter.

Över 1 650 anmälningar från idrottsföreningar och andra organisationer som använder administrationsverktyget har nu inkommit till IMY. Sportsadmin agerar här som personuppgiftsbiträde, vilket innebär ett ansvar enligt artikel 28 GDPR att säkerställa att person-

uppgifter behandlas på ett sätt som uppfyller förordningens krav, skyddar den registrerades rättigheter samt att lämpliga tekniska och organisatoriska åtgärder vidtas. Enligt artikel 33 GDPR är personuppgiftsbiträdet dessutom skyldigt att utan onödigt dröjsmål anmäla personuppgiftsincidenter till den personuppgiftsansvarige. De personuppgiftsansvarige måste i sin tur, enligt samma bestämmelse, anmäla incidenter till IMY inom 72 timmar. Sportsadmin har även själva anmält incidenten till IMY.

Genom att inleda tillsyn har IMY skickat tillsynsskrivelse till Sportsadmin med en redogörelse för granskningens syfte och de frågor bolaget ska besvara. Myndigheten kommer att bedöma om de genomförda säkerhetsåtgärderna är proportionerliga i förhållande till riskerna vid personuppgiftsbehandling. Centralt för granskningen är därmed en utvärdering av de tekniska och organisatoriska åtgärderna som bolaget infört för att skydda uppgifterna i tjänsten. Om dessa åtgärder inte anses tillräckliga kan IMY besluta att utfärda en reprimand, förelägga bolaget att vidta ytterligare åtgärder eller påföra administrativa sanktionsavgifter.



Illustration: Colourbox.com

Detta ärende understryker vikten av att införa och upprätthålla adekvata säkerhetsåtgärder vid hantering av personuppgifter. Mot bakgrund av den stora mängden berörda individer och känslig information väntas IMY:s beslut kunna väcka betydande uppmärksamhet och få konsekvenser för hur liknande digitala tjänster förstår och tar ansvar för dataskyddsfrågor framöver. Vilket ställningstagande IMY slutligen gör återstår att se.

Klara Thyren arbetar som associate inom Tech & IP på Advokatfirman Delphi.



Gorrissen Federspiel

Tue Goldschmieding

Indstævntes varemærkeregistrering skulle ophæves, da det ikke var godtgjort, at varemærket »Kokkedal Slot« var indarbejdet ved brug

Den 8. januar 2025 afsagde Østre Landsret dom i en appelsag vedrørende gyldigheden af varemærket »Kokkedal Slot«. Sagen angik, om Kokkedal Slot ApS og Slotshotellet ApS (»appellanterne«) ved brug af betegnelsen »Kokkedal Slot Copenhagen« krænkede Kokkedal Slot v/A's (»indstævntes«) ret til det registrerede varemærke »Kokkedal Slot«. Sagen blev afsagt under sagsnummer BS-10389/2024-OLR.

Indstævnte havde den 2. december 2008 varemærkeregistreret »Kokkedal Slot« i registreringsklasse 41, der vedrører uddannelsesvirksomhed, undervisningsvirksomhed, underholdningsvirksomhed, sportsarrangementer og kulturelle arrangementer, og 43, der vedrører tilvejebringelse af mad og drikke, samt midlertidig indkvartering.

Appellanterne påstod, at der ikke forelå en krænkelse af det registrerede varemærke »Kokkedal Slot« og påstod i den forbindelse ophævelse af varemærkeregistreringen af varemærket »Kokkedal Slot« foretaget af indstævnte.

For at kunne tage stilling til om appellanterne havde krænket indstævntes ret til varemærket »Kokkedal Slot«, måtte retten først vurdere om varemærket »Kokkedal Slot« havde opnået særpræg som følge af brug, jf. den danske varemærkelov, jf. lovbekendtgørelse nr. 88 af 29. januar 2019 (»varemærkeloven«) § 13, stk. 2.

Retten lagde ved denne vurdering vægt på EU-Domstolens praksis, som viser, at særpræg skal anses for indarbejdet, såfremt de relevante omsætningskredse, eller i det mindste en betydelig andel af disse, som følge af det pågældende varemærke identificerer varen, som hidrørende fra en bestemt virksomhed.

Østre Landsret fandt, at indstævntes varemærkeregistrering i både klasse 41 og 43 skulle ophæves, da det ikke var godtgjort, at varemærket »Kokkedal Slot« var indarbejdet ved brug i disse klasser på tidspunktet for varemærkeansøgningen.

Ved vurderingen lagde retten vægt på, at der ikke i indstævntes fremlagte materiale blev anvendt en konsekvent brug af betegnelsen »Kokkedal Slot«, som kendetegn for indstævntes hotel- og restaurantvirksomhed, samt at en betydelig del af materialet stammede fra lokale og regionale medier, og betegnelsen »Kokkedal Slot« kun i begrænset omfang blev brugt til at betegne A's hotel- og restaurationsvirksomhed. Østre Landsret frifandt på den baggrund appellanterne i det hele.

Læs dommen fra Østre Landsret her: <https://pro.karnogroup.dk/b/documents/7000974645>

Standard essentielt patent medførte ikke i sig selv, at anmodning om bevissikring ikke kunne tages til følge

Østre Landsret afsagde den 9. januar 2025 kendelse i en sag B-672-24 vedrørende CommScope Inc of North Carolina's (»CommScope«) anmodning om bevissikring efter den danske lov om rettens pleje, jf.

lovbekendtgørelse nr. 1160 af 5. november 2024 (»retsplejeloven«) § 653.

CommScope gjorde gældende at en dansk virksomhed (»A«) havde krænket CommScopes patent EP 0 901 201. A påstod heroverfor, at CommScopes patent EP 0 901 201 var et standard essentielt patent. A gjorde i den forbindelse gældende at bevissikring ville være i strid med proportionalitetskravet i retsplejelovens § 653, stk. 4, da patentet var et standard essentielt patent, samt at det var nødvendigt for A at benytte opfindelsen for at opfylde Cat6- og Cat6A-standarden.

Spørgsmålet for retten angik navnlig, om der kunne anmodes om bevissikring, selv hvis patentet var et standard essentielt patent.

Retten henviste til EU-Domstolens sag C-170/13 (Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH), som udtalte at hvis et patent, som er omdrejningspunkt for en bevissikrings-sag, er et standard essentielt patent, så vil det ikke i sig selv medføre, at bevissikringsanmodningen ikke kan tages til følge.

Retten udtalte på den baggrund at det af A anførte om, at patent EP 0 901 201 var et standard essentielt patent, ikke kunne føre til, at anmodningen om bevissikring ikke skulle tages til følge.

Retten udtalte yderligere at det var sandsynliggjort at A havde krænket CommScopes patent, og at der var grund til at antage at bevis for krænkelsen kunne findes i A's lokaler. Betingelsen for bevissikring i retsplejelovens § 653, stk. 1 var derfor opfyldt. Retten tog derfor

CommScopes anmodningen om bevissikring til følge og stadfæstede fogedrettens kendelse.

Læs kendelsen fra Østre Landsret her: <https://pro.karnovgroup.dk/b/documents/7000974625>

Uautoriseret afspilning og eksemplarfremsstilling af musikværker resulterede i fængselsstraf og konfiskation af royalties

Vestre Landsret afsagde den 5. februar 2025 dom i ankesag nr. S-0685-24 mellem T og T ApS over for den danske anklagemyndighed (»Anklagemyndigheden«).

Sagen omhandlede databedrageri og krænkelse af ophavsrettigheder, hvor de tiltalte, T og T ApS, blev fundet skyldige i at manipulere afspilningsdata for at opnå uberettigede royalties.

Sagen blev tidligere behandlet ved retten i Aarhus den 21. marts 2024 under sagsnummeret SS 2-971/2021. Retten i Aarhus fandt, at T og T ApS havde begået databedrageri af særlig grov beskaffenhed ved at generere automatiske afspilninger af musikværker på forskellige streamingtjenester. Dette resulterede i uretmæssig udbetaling af royalties. Retten lagde til grund, at T havde registreret sig som rettighedshaver til et betydeligt antal musikværker hos Koda, og at afspilningerne var autogenererede med det formål at opnå økonomisk vinding. T blev desuden fundet skyldig i krænkelse af ophavsretten til 37 musikværker ved at have ændret og registreret disse værker under eget navn, i strid med den danske lov om ophavsret, jf. lovbekendtgørelse nr. 1093 af 20. august 2023 (»ophavsretsloven«) § 2, der giver rettighedshaveren eneret til ændring og distribution af værker.

Retten i Aarhus idømte T fængsel i 1 år og 6 måneder, hvoraf 3 måneder skulle afsones, mens resten blev gjort betinget. T ApS blev idømt en bøde på 200.000 kr., og der blev konfiskeret 1.000.000 kr.

fra både T og T ApS som følge af de uberettigede indtægter.

Vestre Landsret ændrede byrettens dom ved at forhøje straffen for T til fængsel i 2 år, hvoraf 3 måneder skulle afsones, mens resten blev gjort betinget. Straffen for T ApS blev forhøjet til en bøde på 300.000 kr. Landsretten fandt, at de autogenererede afspilninger havde resulteret i udbetaling af ikke under 3.500.000 kr. i royalties, hvoraf en betydelig del var uberettiget. Landsretten stadfæstede byrettens afgørelse om konfiskation, men forhøjede beløbene til 1.500.000 kr. fra T og 2.000.000 kr. fra T ApS.

Læs dommen fra Vestre Landsret her: <https://vidensbasen.anklagemyndigheden.dk/b/6dfa19d8-18cc-47d6-b4c4-3bd-07bc15ec0/VB/c30173ba-6440-4eed-9873-39f2eb2b1b-0f?showExact=true#iaecdb2dc1>

Østre Landsret stadfæster ophavsretlig beskyttelse af Gannis »Buckle Ballerina« efter modstridende kendelser fra Sø- og Handelsretten

Østre Landsret afsagde den 17. marts 2025 kendelse i en kæresag mellem det danske modebrand GANNI A/S (»GANNI«) og Steve Madden Ltd og Steve Madden Europe B.V. (samlet »Steve Madden«) vedrørende den immaterialretlige beskyttelse af GANNI's skomodel »Buckle Ballerina«. Kendelsen er offentliggjort under sagsnummeret BS-43774/2024-OLR.

Spørgsmålet for retten angik, om modellen var tilstrækkeligt selvstændig og nyskabende til at være omfattet af ophavsretsloven, og herefter om Steve Madden med skoene »GRAND AVE« krænkede GANNI's rettigheder til skoene »Buckle Ballerina«.

Retten fandt, at »Buckle Ballerina«, var ophavsretligt beskyttet efter den danske lov om ophavsret, jf. lovbekendtgørelse nr. 1093 af 20. august 2023 (»ophavsretsloven«) § 2 om ophavsmandens enerettigheder

og den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«) § 3 om god markedsføringskik. Retten lagde vægt på, at skoene, selvom den var sammensat af kendte designelementer, havde en original og kreativ samlet udformning, og at der forelå dokumentation for designerens frie og kreative valg.

Retten stadfæstede på den baggrund Sø- og Handelsrettens kendelse og pålagde Steve Madden at betale GANNI 250.000 kr.

Læs dommen fra Østre Landsret her: <https://www.domstol.dk/oestrelandsret/aktuelt/2025/3/midlertidigt-forbud-vedr-krænkelser-af-ganni-as-buckle-ballerina/>

Spørgeundersøgelse foretaget fem år efter en varemærkeansøgning, kunne indgå i vurderingen af figurmærkets særpræg på ansøgningstidspunktet

Sø- og Handelsretten afsagde den 8. januar 2025 dom i sag BS-53836/2023-SHR mellem Rigo Trading S.A. (»Rigo«) og Ankenævnet for Patenter og Varemærker (»Nævnet«). Sagen omhandlede Nævnets afslag på Rigos ansøgning om registrering af et tredimensionelt figurmærke i varemærkeklasse (Nice) 30, der vedrører konfekturvarer. Rigo, der ejer Haribo-koncernens danske driftsselskaber, havde søgt om at registrere deres vingummibamse, »Guldbamsen«, som varemærke i denne kategori.

Spørgsmålet for retten var navnlig, hvorvidt figurmærket havde et tilstrækkeligt særpræg til at opnå varemærkebeskyttelse. Både Patent- og Varemærkestyrelsen og Nævnet afviste, at Guldbamsen havde det fornødne særpræg, idet de mente, at den ikke adskilte sig væsentligt fra branchens normer og sædvaner. De vurderede også, at Guldbamsen ikke havde opnået et særpræg gennem brug, der ville få gennemsnitsforbrugeren til at

associere figurmærket specifikt med Rigo / Haribo.

Retten afviste indledende Rigos argument om, at der ved vurderingen skulle lægges vægt på forholdene på tidspunktet, hvor produktet første gang blev taget i brug. Derimod gav retten Rigo ret i, at der skulle lægges vægt på en spørgeundersøgelse, selvom denne blev udarbejdet fem år efter ansøgnings-tidspunktet for varemærkere-gistreringen. Retten fandt, at selvom spørgeundersøgelsen var udarbejdet efter ansøgningstidspunktet, udelukkede det ikke undersøgelsen fra at kunne sige noget om situationen på tidspunktet for ansøgningen.

Retten konkluderede, at der ikke var grundlag for at tilsidesætte Nævnets skønsmæssige vurdering af, at Guldamsen manglede det fornødne særpræg på tidspunktet for ansøgningen. Dog fandt retten, at der med spørgeundersøgelsen var fremkommet nye væsentlige oplysninger i sagen, idet resultaterne viste, at en stor del af respondenterne associerede figurmærket med Haribo. Spørgeundersøgelsen skulle derfor indgå i vurderingen af om figurmærket havde det fornødne særpræg, hvorfor retten hjemviste sagen til fornyet behandling ved Nævnet.

Læs dommen fra Sø- og Handelsretten her: <https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-53836-2023-SHR.2570.aspx>

Dansk virksomhed krænkede tysk virksomheds varemærkeret til emballage på dåsesodavand

Sø- og Handelsretten afsagde den 13. januar 2025 dom i sag BS-52211/2023-SHR mellem Ayyo Vertriebs GmbH (»Ayyo«) og Kon Import ApS (»Kon«) vedrørende designet på emballagen til en dåse-sodavand. Ayyo, et tysk selskab, solgte sine dåsesodavand, kaldet Gazoz, på det danske marked. Kon, et dansk selskab, distribuerede blandt andet Gazoz i Danmark.

Sagens kerne var, hvorvidt Ayyo havde opnået varemærkeret til Gazoz' emballage i Danmark i henhold til den danske varemærkelov, jf. lovbekendtgørelse nr. 88 af 29. januar 2019 (»varemærkeloven«) § 3, stk. 1, nr. 3, samt om Kon herefter havde krænkede Ayyos varemærkeret-tigheder efter varemærkeloven og den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsførings-loven«) ved også at sælge Gazoz-so-davand på det danske marked, men efter en distributionsaftale med Confeti GmbH (»Confeti«).

Retten afviste indledningsvist, at Ayyo i det hele taget skulle være forhindret i at stifte denne varemærkeret, som følge af, at ordmærket Gazoz var registreret i EU's varemærkeklasse 29, der vedrører »soft drinks based on milk products«, og tilhørte Mustafa Karadeniz (»Karadeniz«), der ejede Confeti.

Kon påstod, at de som licensha-vere efter distributionsaftalen med Karadeniz og Confeti, havde en fortrinsret til varemærket gennem afledt ret fra Karadeniz og Confeti, hvilket skulle forhindre Ayyo i at stifte rettigheder til emballagen. Retten afviste dette, idet hverken Karadeniz eller Confeti havde anvendt deres EU-varemærkeret i Danmark før Ayyos første salg, og Ayyo ikke havde handlet i ond tro med hensyn til eventuelle modstri-dende rettigheder.

På den baggrund fandt retten vedrørende det første spørgsmål, at Ayyo havde stiftet varemærkeret til varemærkeudstyret (emballagen) efter varemærkelovens § 3, stk. 1, nr. 3, ved deres ibrugtagen, fra deres første salg i Danmark.

Da parterne i øvrigt var enige om, at der var en forvekslingsrisiko mellem de omstridte mærker, nedlagde retten forbud mod Kons anvendelse af emballagen i henhold til varemærkelovens § 4, stk. 2. Retten fandt også, at Kon havde handlet i strid med markedsføringslovens § 3 og § 22.

Som følge af krænkelse blev Kon pålagt at betale 400.000 kr. til Ayyo. Derudover blev Kons varemærkere-gistrering af figurmærket Gazoz Zero og ordmærket Gazoz erklæret ugyldige i henhold til varemærkelovens § 15, stk. 1, nr. 2, jf. stk. 2, nr. 4.

Læs dommen fra Sø- og Handelsretten her: <https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-52211-2023-SHR.2572.aspx>

Sø- og Handelsretten afviser ophavsretlig beskyttelse af GANNIs sko, men stadfæster markedsføringsforbud

Sø- og Handelsretten afsagde den 14. januar 2025 dom i sag BS-44774/2024-SHR mellem GANNI A/S (»GANNI«) og Bianco Footwear A/S (»Bianco«) angående en påstået krænkelse af GANNIs rettigheder i forbindelse med Biancos produktion og salg af sko, som GANNI hævdede var nærgående efterligninger af deres skomodeller.

Sagens kerne var, hvorvidt Biancos sko krænkede GANNIs rettigheder i henhold til den danske lov om ophavsret, jf. lovbekendtgørelse nr. 1093 af 20. august 2023 (»op-havsretsloven«), den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«), den danske designlov, jf. lovbekendtgørelse nr. 89 af 29. januar 2019 (»design-loven«) og forordning (EF) 6/2002 af 12. december 2001 (»designfor-ordningen«). GANNI gjorde gæl-dende, at Biancos produktion og markedsføring af »Biavictoria San-dal« samt tre andre skodesigns krænkede GANNIs rettigheder til modellen »Buckle Ballerina« samt yderligere to skomodeller.

Retten vurderede, at GANNIs sko ikke opfyldte originalitetskravet for at opnå ophavsretlig beskyttelse, idet den blev betragtet som brugs-kunst uden tilstrækkelig nyskabelse efter ophavsretsloven. Retten lagde vægt på, at i) skoen fremstod som en sammensætning af kendte desig-

nelementer, ii) de valg, der var foretaget i designprocessen, måtte anses for sædvanlige i en designproces i modeverdenen, og iii) der ikke var tale om en sådan nyskabelse, at skoen kunne anses som en intellektuel frembringelse, der kunne nyde ophavsretlig beskyttelse.

Imidlertid fandt retten, at skomodellen besad den nødvendige kommercielle adskillelsesevne, hvilket medførte beskyttelse i henhold til markedsføringsloven. På denne baggrund blev der alene nedlagt forbud mod Biancos markedsføring af »Biavictoria Sandal« skoen, da den blev anset som en nærgående efterligning af GANNIs design.

Retten fastslog, at Bianco skulle ophøre med produktion, markedsføring og salg af »Biavictoria Sandal« skoen i Danmark.

Læs dommen fra Sø- og Handelsretten her: <https://domstol.fe1.tangora.com/Domsoversigt.16692/-BS-44774-2024-SHR.2573.aspx>

Europart blev pålagt at betale vederlag på 2 mio. kr. til Volvo for uberettiget brug af Volvos varemærker

Sø- og Handelsretten afsagde den 21. februar 2025 dom i sag BS-47174/2021-SHR mellem Volvo Lastvagnar AB (»Volvo«) og Europart Danmark A/S (»Europart«) vedrørende Volvos ret til ordmærkerne »VOLVO«, »FL«, »FM«, »FH« og »FMX«.

Sagen angik, hvorvidt Europarts brug af Volvos ordmærker i 39 kataloger var i strid med den danske varemærkelov, jf. lovbekendtgørelse nr. 88 af 29. januar 2019 (»varemærkeloven«) § 4, forordning (EU) 2017/1001 af 14. juni 2017 (»varemærkeforordningen«) artikel 9, og om anvendelsen falder indenfor reservedelsreglen i varemærkelovens § 10, stk. 1, nr. 3 og varemærkeforordningens art. 14, stk. 1.

Volvo var indehaver af ordmærkerne »VOLVO«, »FL«, »FM«, »FH« og »FMX«, alle registreret for landkøretøjer. Retten bemærkede, at

Europart brugte mærkerne for at vise reservedelernes tilknytning til Volvo, hvilket som udgangspunkt krænkede Volvos rettigheder efter varemærkelovens § 10, stk. 1, nr. 3 og varemærkeforordningens artikel 9, stk. 2, litra a. Retten skulle dog vurdere, om brugen var tilladt under reservedelsreglen, som krævede nødvendighed og god markedsføringskik.

Retten fandt, at brugen var nødvendig for at vise reservedelernes anvendelse til Volvo lastbiler. Dog bemærkede retten, at den fremtrædende brug af »VOLVO« i katalogtitlerne kunne give indtryk af en forbindelse mellem Volvo og Europart, hvilket skabte vildfarelse hos forbrugerne. Dette var i strid med god markedsføringskik, og retten fandt brugen retsstridig.

Retten forbød Europart at anvende mærkerne på den måde, jf. den danske lov om rettens pleje, jf. lovbekendtgørelse nr. 1160 af 5. november 2024 (»retsplejeloven«) § 413 og pålagde dem at betale 2.055.000 kr. til Volvo som kompensation.

Læs dommen fra Sø- og Handelsretten her: <https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-47174-2021-SHR.2580.aspx>

Anvendelse af ordmærkerne »Coop«, »Irma« og figurmærket Irmapien på produkter krænkede Coops varemærkerettigheder

Sø- og Handelsretten afsagde den 21. februar 2025 dom i sag BS-62403/2023-SHR om hvorvidt Artpusher Gallery ApS (»Artpusher Gallery«) og kunstneren Love Party har krænkede Coop Danmark A/S' (»Coop«) varemærkerettigheder.

Sagen angik, hvorvidt Artpusher Gallery og Love Partys salg og markedsføring af produkter med varemærkerne Coop, Irma og Irmapien, var i strid med den danske varemærkelov, jf. lovbekendtgørelse nr. 88 af 29. januar 2019 (»varemærkeloven«) § 4, stk. 2, nr. 2 og nr.

3 samt den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«). Coop ejede varemærkerne, som var registreret i alle Nice-klassifikationens klasser.

Retten bemærkede, at produkterne blev solgt med et kommercielt formål, og at Coops varemærker var centrale elementer i motiverne. Retten afviste, at motiverne var parodier, da der ikke var tilstrækkelige ændringer eller et fremmed formål. Artpusher Gallery og Love Party kunne ikke bevise, at motiverne var humoristiske. Retten afviste også, at Love Partys ytringsfrihed kunne retfærdiggøre brugen af varemærkerne over Coops ophavsret, jf. lovbekendtgørelse nr. 1093 af 20. august 2023 (»ophavsretsloven«) § 2 og § 3, stk. 2.

Retten fandt risiko for forveksling med Coops produkter og konstaterede, at Artpusher Gallery og Love Party havde draget fordel af Coops forretningskendetegn, særligt Irmapien og ordmærket »Irma«. Derfor var deres salg og markedsføring af motiverne i strid med markedsføringslovens § 3, stk. 1, § 4, §20, stk. 1 og § 22.

Retten nedlagde forbud mod, at Artpusher Gallery og Love Party gjorde brug af varemærkerne og pålagde dem at udlevere alle produkter til Coop og fjerne dem fra sociale medier. Retten pålagde Artpusher Gallery og Love Party at betale vederlag til Coop på 750.000 kr. samt idømte dem en bøde på 15.000 kr.

Læs dommen fra Sø- og Handelsretten her: <https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-62403-2023-SHR.2579.aspx>

Varemærkerettigheder til ordmærket »MULTIAIR« var ikke krænkede

Sø- og Handelsretten afsagde den 24. februar 2025 kendelse i sag BS-48344/2024-SHR mellem Kongskilde Industries A/S (»Kongskilde«) og Klimablock Herning APS (»Kli-

mablock») angående Kongskildes ret til ordmærket »MULTIAIR«.

Sagens immaterialretlige kerne var, hvorvidt Klimablock havde krænket sagsøgers rettigheder til ordmærket efter den danske varemærkelov, jf. lovbekendtgørelse nr. 88 af 29. januar 2019 (»varemærkeloven») § 4, stk. 1, nr. 2, og forordning (EU) 2017/1001 af 14. juni 2017 (»varemærkeforordningen») artikel 9, stk. 2, litra b.

Kongskilde var indehaver af ordmærket »MULTIAIR«. Ordmærket var beskyttet efter dansk varemærkeregistrering og EU-varemærkeregistrering, og var begge steder registreret i varemærkeklasse (Nice) 7, som omfatter maskiner og udstyr hertil.

»MULTIAIR« var siden 1994 blevet brugt både på Kongskildes maskiner og i markedsføring, herunder på hjemmesiden. Kongskilde anvendte ordmærket »MULTIAIR« på højtryksblæsere, mens Klimablock anvendte mærket »MultiAir« til ventilations- og udsugningsløsninger.

Retten fandt, at det ikke var tilstrækkelig sandsynliggjort, at der bestod en risiko for forveksling mellem de to mærker i offentlighedens bevidsthed. Det ændrede ikke herved, at der kunne indgå samme typer komponenter i de to virksomheders produkter. Retten lagde vægt på at MultiAir-mærket blev anvendt på andre produkter end ordmærket »MULTIAIR«, som der desuden ikke var konkrete eksempler på, var blevet forvekslet. Retten lagde desuden vægt på, at der var tale om produkter, der havde en karakter og prisklasse, der måtte antages at forudsætte, at målgruppen foretog undersøgelser om forskellige løsninger og leverandører, inden køb.

På den baggrund frifandt retten Klimablock, da betingelserne for at nedlægge forbud og påbud efter den danske lov om rettens pleje, jf. lovbekendtgørelse nr. 1160 af 5. november 2024 (»retsplejeloven») § 413, nr. 1, herefter ikke var opfyldt.

Sø- og Handelsretten lagde vægt på de samme omstændigheder, da de konkluderede, at der heller ikke var sket en krænkelse af sagsøgers rettigheder efter markedsføringslovens §§ 3 og 22, om god markedsføringsskik og risiko for forveksling.

Læs kendelsen fra Sø- og Handelsretten her: <https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-48344-2024-SHR.2581.aspx>

Formodning for patentets gyldighed var ikke svækket i sådan grad at sagsøger ikke kunne støtte ret på patentet

Sø- og Handelsretten afsagde den 25. februar 2025 dom i to sambehandlede sager om anmodning om midlertidige forbud og påbud vedrørende lægemiddel til behandling af multipel sklerose på baggrund af en påstået krænkelse af patentrettigheder. Afgørelsen blev afsagt med sagsnumrene BS-43205/2023-SHR og BS-55247/2024-SHR.

Sagsøger var i begge sager Biogen International GmbH og Biogen (Denmark) A/S (herefter tilsammen »Biogen«). Sagsøgte var henholdsvis Sandoz A/S og Glenmark Pharmaceuticals Nordic AB (»sagsøgte«).

Biogen anførte at sagsøgte lægemidler krænkede patentrettigheder til det danske stridspatent DK/EP 2 653 873 med benævnelsen »Sammensætninger til behandlingen af multipel sklerose«. På den baggrund nedlagde sagsøger i medfør af den danske lov om rettens pleje, jf. lovbekendtgørelse nr. 1160 af 5. november 2024 (»retsplejeloven») § 413, nr. 1, påstand om, at de sagsøgte blev forbudt at fremstille deres lægemiddel, så længe stridspatent DK/EP 2 653 873 var i kraft, samt påstand om at lægemidlet skriftligt skulle tilbagekaldes, og afregistreres på det danske prisregister.

Spørgsmålet for retten var herefter, om stridspatentet var ugyldigt, og særligt om stridspatentets krav 1 var ugyldigt.

Retten udtalte at patentets gyldighedsformodning svækkedes af EPO's Opposition Division's vurdering af 11. december 2024, som påpegede, at kravet om tilstrækkelig beskrivelse ikke var opfyldt, da der kunne rejses tvivl om virkningen af 480 mg DMF pr. dag ved PPMS.

Retten fandt, at stridspatentet var gyldigt i begrænset form. Formodningen for stridspatentets gyldighed var ikke svækket i en sådan grad, at Biogen ikke kunne anmode om forbud og påbud i medfør af retsplejeloven § 413, nr. 1.

Læs dommen fra Sø- og Handelsretten her: <https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-43205-2023-SHR-og-BS-55247-2024-SHR.2582.aspx>

»Annalysen« var en efterligning af Alterlyset ApS' lys og en krænkelse af markedsføringsloven

Sø- og Handelsretten afsagde den 20. marts 2025 kendelse i sag BS-50402/2024-SHR mellem Alterlyset ApS mod ASP-HOLMBLAD A/S og Liljeholmens Stearinfabrik AB (»Liljeholmens«) vedrørende en mulig efterligning af stearinlys efter den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. februar 2024 (»markedsføringsloven«).

Den danske virksomhed Alterlyset ApS havde siden 2012 produceret og solgt håndstøbte lys på fod, herunder lysene Alterlyset, Hyggyset og Kalenderlyset. Sagens kerne var, hvorvidt den danske virksomhed, ASP-HOLMBLAD A/S, og dennes svenske ejerselskab, Liljeholmens, havde krænket Alterlyset ApS's rettigheder efter markedsføringsloven ved salg og markedsføring af flere lys, herunder »Annalysen« som udgjorde mulige efterligninger.

Retten fandt, at Alterlyset, Hyggyset og Kalenderlyset nød beskyttelse efter markedsføringsloven, da lysene havde særpræg samt adskilte sig fra de øvrige lys på marke-

det. Retten lagde vægt på, at lysene var udformet med en bestemt højde og vinkel på foden af lyset, samt blev produceret i bestemte støvede og antikke farver, hvilket gjorde lysene genkendelige. Retten lagde yderligere vægt på, at lysene i mere end 10 år kontinuerligt var blevet markedsført i blandt andet eksklusive interiørbutikker, museumbutikker og boligmagasiner.

Retten fandt, at Liljeholmens produkt »Annalysset« i det væsentlige havde samme udtryk som Alterlyset, Hyggelyset og Kalenderlyset i henhold til lysets form, højde, farveskala og prissætning, hvorfor der forelå en forvekslingsrisiko. Retten bemærkede, at forskellene mellem de nævnte lys udgjorde detaljer, som kun kunne bemærkes, når lysene placeres ved siden af hinanden, hvilket ikke var tilfældet i en købsituation. Retten fandt ikke, at ASP-HOLMBLADs og Liljeholmens andre lys, herunder Påskelyset, udgjorde efterligninger.

På den baggrund slog retten fast, at ASP-HOLMBLAD og Liljeholmens ved markedsføring og salg af Annalysset havde krænket Alterlyset ApS' rettigheder efter markedsføringslovens § 3, stk. 1, § 5, stk. 2, nr. 10 og § 20, stk. 1, og meddelte forbud mod, at sælge eller markedsføre »Annalysset« i Danmark i medfør af den danske lov om rettens pleje, jf. lovbekendtgørelse nr. 1160 af 5. november 2024 (»retsplejeloven«) § 413.

Læs kendelsen fra Sø- og Handelsretens her: <https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-50402-2024-SHR.2585.aspx>

Forbrugerombudsmanden indskærper at stegepandeproducenter ikke må markedsføre sig som fri for forbudte stoffer

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) bragte den 6. januar 2025 nyheden om, at Forbrugerombudsmanden havde indskærpet vildledningsforbuddet i

den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«) over for flere producenter af stegepander.

Sagen drejede sig om otte virksomheder, som i 2022 havde markedsført deres stegepander som fri for stoffet PFOA og PFOS. Begge stoffer er forbudte i forbrugerprodukter efter forordning (EU) 2019/1021 af 20. juni 2019 (»POP forordningen«). Forbrugerombudsmanden fandt derfor, at det er vildledende, når virksomheden bruger fraværet af PFOA og PFOS i sin markedsføring, da det giver indtrykket af, at der er en særlig fordel ved produktet.

Forbrugerombudsmanden understregede, at virksomheder ikke må give forbrugerne indtryk af, at en miljø- eller sundhedsfordel er særlig for virksomhedens produkter, når det gælder på baggrund af et krav eller forhold, der følger af lovgivningen.

Læs pressemeddelelsen fra Forbrugerombudsmanden her: <https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20250106-vildledende-markedsfoering-af-stegepander>

Fitnesskæde idømt bøde på 600.000 kr. for vildledende markedsføring samt modtaget kritik af Forbrugerombudsmanden for urimelige vilkår

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) har behandlet to sager mod fitnesskæden Arca ApS (»Arca«), hvori Københavns byret den 7. januar 2025 har afsagt dom i den ene sag med sagsnr. 24/04821. Den første sag er en straffesag vedrørende vildledende markedsføring af tilbud, og den anden sag omhandler urimelige medlemsvilkår og uautoriseret opkrævning af et energitillæg.

Den første sag angik, at Arca i perioden 22. februar 2019 til 3. juli 2023 havde markedsført tilbud om

2 måneders gratis træning eller træning til kraftigt nedsat pris, uden klart at oplyse forbrugerne om tilbuddets vilkår. Disse vilkår indebar, at forbrugerne automatisk ville blive tilmeldt et løbende betalingsmedlemskab, som forbrugerne først kunne melde sig ud af, når der var blevet betalt minimum én måned til fuld pris.

Forbrugerombudsmanden udtalte, at der var tale om vildledning i strid med den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«) § 5 og § 6 og indgav politianmeldelse i sagen. Københavns Byret afsagde den 7. januar 2025 dom i sagen, hvor Arca ApS blev idømt en bøde på 600.000 kr. for vildledende markedsføring. Arca har anket dommen til landsretten.

Den anden sag udsprang af, at Arca havde vilkår i deres medlemsbetingelser, som efter Forbrugerombudsmandens opfattelse var urimelige og i strid med den danske lov om aftaler og andre retshandler på formuerettens område, jf. lovbekendtgørelse nr. 193 af 2. marts 2016 (»aftaleloven«) og hæderlig forretningsskik.

Et af Arcas vilkår gav Arca ret til at ændre sine medlemsbetingelser med to ugers varsel på ethvert tidspunkt. Derudover havde Arca et vilkår, som medførte, at forbrugerens opsigelse af medlemskab først var gyldigt, når de havde modtaget en kvittering fra Arca. På baggrund af disse vilkår ændrede Arca sine medlemsbetingelser og hævdede priserne på allerede indgåede aftaler om medlemskaber og opkrævede forbrugerne et engangsbetalt for et energitillæg uden forbrugernes samtykke.

Forbrugerombudsmanden udtalte, at Arcas vilkår var ugyldige, da de var i strid med aftalelovens § 38 c og § 36, hvorfor forbrugerne kunne kræve tilbagebetaling af beløbet.

Læs pressemeddelelse fra Forbrugerombudsmanden her: <https://forbrugerom->

budsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20250123-fitnesskaede-idoemt-boede-paa-600000-kroner-for-vildledende-markedsfoering

Læs afgørelsen fra Forbrugerombudsmanden her: <https://forbrugerombudsmanden.dk/find-sager/sager/markedsfoeringsloven/sager-efter-markedsfoeringsloven/vildledning/2404821-fitnesskaede-idoemt-boede-for-vildledende-tilbud-om-traening>

Virksomhed kunne ikke lovligt benytte en række klima- og miljøudsagn på baggrund af en livscyklusvurdering som dokumentation

Den 10. januar 2025 udtalte den danske forbrugerombudsmand (»Forbrugerombudsmanden«) sig i en sag vedrørende klima- og miljøudsagn og dokumentation for klima- og miljøudsagn. Afgørelsen blev truffet med sagsnummer 24/13563.

En virksomhed havde fået foretaget en ekstern livscyklusvurdering, som skulle fungere som dokumentation for, at virksomhedens leveringsservice var mindre belastende for både klima og miljø end andre relevante alternativer.

Forbrugerombudsmanden udtalte, at livscyklusvurderingen ikke kunne bruges som dokumentation for virksomhedens generelle klima- og miljøudsagn uden forklaring, da den kun omhandlede klima og derfor ikke var tilstrækkelig, da miljø består af flere aspekter end blot klima.

Forbrugerombudsmanden udtalte, at selv hvis virksomhedens miljøudsagn blev ændret til kun at omhandle klima, ville livscyklusvurderingen stadig ikke opfylde dokumentationskravet. Den dokumenterede ikke, at virksomhedens service var væsentligt mindre belastende end tilsvarende produkter. Derudover manglede der en sammenligning med relevante alternativer, i stedet for blot at vise, at virksomhedens service skånede kli-

maet isoleret set. Forbrugerombudsmanden henviste til vildledningsbestemmelserne i den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«), § 5 og § 6, sammenholdt med § 8, samt § 13, der omhandler dokumentation af oplysninger i markedsføringen.

Læs afgørelsen fra Forbrugerombudsmanden her: <https://forbrugerombudsmanden.dk/find-sager/sager/markedsfoeringsloven/sager-efter-markedsfoeringsloven/miljoeogetik/2413563-virksomhed-kunne-ikke-lovligt-benytte-en-raekke-klima-og-miljoedsagn-paa-baggrund-af-en-livscyklusvurdering>

Elgiganten og Santander politianmeldt for overtrædelse af markedsføringsloven i forbindelse med annoncering af lån

Den 16. januar 2025 har den danske forbrugerombudsmand (»Forbrugerombudsmanden«) politianmeldt Elgiganten A/S (»Elgiganten«) og Santander Consumer Bank A/S (»Santander«) for overtrædelse af den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«) i forbindelse med virksomhedernes annoncering af lån. Elgiganten havde samarbejdet med Santander om forbrugslån til køb af Elgigantens produkter.

Markedsføringen drejede sig om udsagn såsom »Finansier din Macbook helt uden omkostninger«. Når forbrugerne ville gøre brug af tilbuddet ved onlinekøb på Elgigantens hjemmeside, var der imidlertid kreditomkostninger forbundet med de lån, som Elgiganten udbød i samarbejde med Santander. Forbrugerombudsmanden udtalte at udsagnene var vildledende, da de gav forbrugerne indtryk af at de kunne have fået et gratis lån.

Forbrugerombudsmanden henviste i sin udtalelse til markedsføringslovens § 5 og § 6, sammenholdt

med § 8, om vildledende markedsføring, samt til markedsføringslovens § 9, sammenholdt med pkt. 20 i lovens bilag 1, vedrørende omtale af produkter som gratis, selvom der kræves uundgåelige udgifter.

Forbrugerombudsmanden udtalte at Elgiganten og Santander havde overtrådt pligten i markedsføringslovens § 18 til at vise bestemte standardoplysninger i deres markedsføring af de annoncerede lån, hvilket drejede sig om manglende oplysninger om debitorrenten, samlede omkostninger for lånet, samlet kreditbeløb, årlige omkostninger i procent (ÅOP) og det samlede beløb, som forbrugeren skulle betale.

Læs pressemeddelelsen fra Forbrugerombudsmanden her: <https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20250116-elgiganten-og-santander-politianmeldt-for-overtraedelse-af-markedsfoeringsloven>

Forbrugerombudsmanden politianmelder flyselskabet KLM for vildledende bæredygtighedsudsagn

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) indgav den 22. januar 2025 en politianmeldelse på KLM for vildledende markedsføring i deres radioreklame. Sagen drejede sig om, at KLM i reklamen var kommet med udsagn om bæredygtighed, som Forbrugerombudsmanden vurderede, var egnede til at vildlede forbrugerne.

Reklamen indeholdt blandt andet udsagn om, at KLM var »et stort skridt mod at rejse lidt mere bæredygtigt«, på grund af »en del bæredygtigt flybrændstof«. Derudover, at hvis forbrugerne »vil flyve mere bæredygtigt og accelerere udviklingen«, kunne de vælge at tilkøbe mere »bæredygtigt flybrændstof«.

Forbrugerombudsmanden mente ikke, at udsagnet om, at KLM havde »taget et stort skridt« mod bæredygtighed, var retvisende henset til, at KLM kun tilsatte 1% bæredygtigt flybrændstof på deres fly. Udsagnet

gjorde det ikke tydeligt for forbrugeren, hvor lille en rolle bæredygtigt brændstof spiller i luftfartsselskabers generelle klimapåvirkning. Forbrugerombudsmanden mente på den baggrund, at udsagnene gav forbrugerne anledning til at forvente større klima- og miljømæssige fordele ved at flyve med KLM, end hvad KLM's tilføjelse af 1% bæredygtigt brændstof reelt bidrog med.

Forbrugerombudsmanden understregede med sagen, at virksomhederne ikke må give forbrugerne indtryk af, at deres bæredygtigheds tiltag er større end de er.

Læs pressemeddelelse fra Forbrugerombudsmanden her: <https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20250122-forbrugerombudsmanden-politianmelder-fly-selskabet-klm-for-vildledende-udsagn-om-baeredygtighed>

Klimaudsagn var vildledende da markedsføringens udformning var egnet til at give forbrugeren et fejlagtigt indtryk af den markedsførte klimafordel

Den 3. februar 2025 udtalte den danske forbrugerombudsmand (»Forbrugerombudsmanden«) sig i sag 24/06791 om vildledningsforbuddet i den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«) § 5 og § 6 i forbindelse med en virksomheds markedsføring af formalet hovedemel. Spørgsmålet i sagen vedrørte hvorvidt klimaudsagnet »CO₂e neutral formalet – via grøn strøm og klimakompensation« var egnet til at vildlede forbrugeren.

På baggrund af oplysninger i en rapport fra virksomheden kunne det beregnes, at formalingen udgjorde maksimalt 5,17 % af produktets samlede klimaaftryk, og dermed at hvis formalingens klimaaftryk helt blev fjernet, ville reduktionen således aldrig overskride 5,17 % af det samlede produkts klimaaftryk.

Forbrugerombudsmanden udtalte at udsagnet »CO₂e-neutral« var vagt formuleret og gav forbrugerne indtryk af at produktet havde væsentlige klimamæssige fordele. Den klimamæssige fordel ved virksomhedens produkter var mindre væsentlig og udgjorde derfor vildledende grøn markedsføring, da klimaudsagnet var overdrevet.

I den forbindelse udtalte Forbrugerombudsmanden yderligere at selvom det fremgik af udsagnet, at det var formalingen, som var CO₂e-neutral, kunne det ikke forventes, at gennemsnitsforbrugeren var klar over, at formalingen, og dermed CO₂e-neutraliteten, kun angik maksimalt 5,17% af det samlede produkt.

Forbrugerombudsmanden indskærpede derfor markedsføringslovens § 5 og § 6, sammenholdt med § 8, overfor virksomheden.

Læs afgørelsen fra Forbrugerombudsmanden her: <https://forbrugerombudsmanden.dk/find-sager/sager/markedsfoeringsloven/sager-efter-markedsfoeringsloven/miljoegetik/2406791-indskaerpelse-af-vildledningsforbuddet-for-markedsfoering-med-klimaudsagn-grundet-markedsfoeringens-fremstillingsform>

Forbrugerombudsmanden politianmelder Taster Wine A/S for greenwashing

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) indgav den 26. februar 2025 en politianmeldelse på Taster Wine A/S for vildledende markedsføring af vin. Sagen drejede sig om, at Taster Wine A/S siden 2019 havde brugt grønne labels med udsagn om CO₂-venlighed på to vin seriers emballage. Forbrugerombudsmanden havde undersøgt sagen på baggrund af en klage fra Forbrugerrådet Tænk.

Forbrugerombudsmanden fandt, at Taster Wine A/S havde en CO₂-besparelse på transporten af vinen, men at denne besparelse kun udgjorde en meget lille del af vinen

samlede klimabelastning. På den baggrund vurderede Forbrugerombudsmanden, at markedsføringen af vinen var egnet til at vildlede forbrugerne, da mærkaterne, navnlig den grønne farve og udsagnet »CO₂-friendly [bulk] wine«, gav indtrykket af, at vinen var mere klimavenlig end den reelt var. Forbrugerombudsmanden understregede, at virksomheder generelt skal være påpasselige med at overdrive hvor bæredygtige deres produkter er.

I forbindelse med Forbrugerombudsmanden anmeldelse, oplyste Taster Wine, at mærkaterne ikke vil anvendes efter den 1. januar 2025.

Læs pressemeddelelse fra Forbrugerombudsmanden her: <https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20250226-forbrugerombudsmanden-politianmelder-vin-og-spiritusvirksomhed-for-greenwashing>

Tøjkæde Boii Studios politianmeldt af Forbrugerombudsmanden for markedsføring af vildledende tilbud

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) har den 20. marts 2025 politianmeldt selskabet MASH 16 ApS, som står bag tøjbutikskæden Boii Studios.

Politianmeldelsen sker på baggrund af en mulig overtrædelse af den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. februar 2024 (»markedsføringsloven«) § 5 og § 6, som omhandler vildledningsforbuddet.

Boii Studios havde i vinduet af tre butikker i henholdsvis København, Odense og Aarhus skiltet med teksten »ALT UDSALG I BUTIKKEN 50%«. På skiltene fremstod ordene »ALT« og »50%« fem gange større end den øvrige del af teksten. Ifølge Forbrugerombudsmanden havde forbrugerne nemt kunne overse udsalgets begrænsning, da dette fremgik med den mindre skriftstørrelse.

Det var Forbrugerombudsmandens opfattelse, at skiltningen derfor har været egnet til at vildlede forbrugerne og give dem en opfattelse af, at tilbuddet omfattede alle varerne i butikken, selvom dette ikke var tilfældet.

Forbrugerombudsmanden understregede, at begrænsninger i et markedsført besparelsesudslag udgør en væsentlig oplysning, som skal markedsføres på en tilstrækkelig klar, forståelig og hensigtsmæssig måde.

Læs pressemeddelelse fra Forbrugerombudsmanden her: <https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20250320-forbrugerombudsmanden-politianmelder-toej-butikskaden-boii-studios-for-at-overtraede-markedsfoeringslovens-vildledningsforbud>

Om den danske ophavsretslovs § 31

To danske advokater, Steen Lassen og Terese Foged, har i en artikel un-

dersøgt Højesterets fortolkning af den danske lov om ophavsret, jf. lovbekendtgørelse nr. 1093 af 20. august 2023 (»ophavsretsloven«) § 31 i Højesterets Dom af 5. november 2022 i sag 98/2001 (»Harddisk-sagen«).

Artiklen diskuterer, om Højesterets fortolkning i sagen er i overensstemmelse med EU-retten. Harddisk-sagen drejede sig om, hvorvidt ophavsretsloven § 31 kunne anvendes på Dansk Radios (»DR«) kopiering af musik fra CD'er til en digital version på en computer harddisk. Ophavsretsloven § 31 giver radio- og fjernsynsforetagender ret til at anvende efemære optagelser i forbindelse med deres udsendelser.

Artiklen fokuserer på, hvilken tidsgrænse, som begrebet efemær dækker over, og hvornår en optagelse har den kortvarige karakter, som er en betingelse for anvendelsen af ophavsretsloven § 31. Artiklen forholder sig til en kritik i litteraturen, der hævder, at Højesteret i sagen ikke tog tilstrækkeligt hensyn til

EU-rettens betingelse om, at der skal være tale om efemære optagelser.

Artiklen afviste denne kritik og konkluderede, at EU-retten ikke fastsætter en specifik tidsgrænse, men at denne grænse bør findes inden for den naturlige begrænsning af udsendelsesretten, som i sig selv kun gælder for udsendelsen af det pågældende værk. Artiklen konkluderede på den baggrund, at Højesteret foretog en korrekt fortolkning af ophavsretslovens § 31, som er i overensstemmelse med EU-retten.

Læs artiklen udgivet i Ugeskrift for Retsvæsen her: <https://pro.karnovgroup.dk/b/documents/7000973831#UB20250001-01>

Av Tue Goldschmieding, partner i Gorrissen Federspiel og dansk redaktør for Lov & Data.





Bird & Bird

Gunnar Hjalt

Upphovsrättsliga avtals särprägel ges mindre företräde vid avtalstolkning

Högsta domstolen (HD) har i en den 28 februari 2025 dom i mål T 5449-23 kommit till slutsatsen att avtalstolkning inom upphovsrättens område visserligen innebär att det ska tas hänsyn till de syften och särdrag som är typiska för upphovsrätten, men dessa hänsyn ska inte betraktas som några speciella och överordnade tolkningsprinciper. Snarare ska upphovsrättens syften och särdrag vägas in som precisrande och kompletterande omständigheter, i en helhetsbedömning där först och främst försök gjorts att fastställa den gemensamma partsavsikten och att tolka avtalet utifrån dess ordalydelse.

Utgången i målet, som avsåg rätten till ersättning och namngivning för ett litterärt verk, den s.k. "Gran Canaria-serien", innebär att avsteg från en uppfattning som sedan länge gällt bland många praktiserande jurister i Sverige inom upphovsrättsområdet, nämligen att särskild hänsyn ska tas till omständigheten att det föreligger ett verk, i förhållande till dess natur, den ideellrättsliga prägeln, reproducerbarheten samt till att upphovspersonen kan ha haft en svag avtalsposition.



Illustration: Colourbox.com

Avgörandet speglar en förändring som pågår inom svensk upphovsrätt på flera punkter, från nationell särreglering till en anpassning relativt EU-rättsliga principer.

Se avgörandet i dess helhet här:
<https://www.domstol.se/globalassets/filer/domstol/hogstodomstolen/avgoranden/2025/t-5449-23.pdf>

Gunnar Hjalt, Senior Counsel,
 Bird & Bird Advokat.



Selmer

Kine Emilie Helgeneseth og Henriette Solbakke Jørgensen

EU-kommisjonen slår ned på teknologigiganter: Apple og Meta ilegges betydelige bøter for brudd på DMA

Innledning

Den 23. april 2025 kunngjorde EU-kommisjonen historiske vedtak mot to av verdens største teknologiselskaper. Apple og Meta ble ilagt bøter på henholdsvis 570 millioner euro og 228 millioner euro for brudd på EUs Digital Markets Act (DMA). Dette representerer et viktig skritt i EUs innsats for å regulere store teknologiselskaper og sikre rettferdig konkurranse i det digitale markedet.

Bakgrunnen for botene er EUs mål om å skape et mer balansert og konkurransedyktig digitalt landskap, og styrke forbrukervernet på området. DMA, som trådte i kraft i EU i 2022, har som formål å forhindre at store teknologiselskaper misbruker sin markedsposisjon til å hindre konkurranse og begrense forbrukerens valgmuligheter. Forordningen pålegger blant annet såkalte «gatekeepers» – selskaper med betydelig innflytelse på det digitale markedet – å følge spesifikke regler for å sikre at mindre aktører også kan konkurrere på mer like vilkår.

DMA har ennå ikke trådt i kraft i Norge, men forventes å gjøre det.

Vedtaket mot Apple

Kommisjonens vedtak mot Apple gjelder brudd på DMA artikkel 5 (4).

Det følger av bestemmelsen at «gatekeepers» skal tillate bedriftsbrukere, som apputviklere, å gratis kommunisere og promotere tilbud til sluttbrukere «acquired via its core platform service or through other channels, and to conclude contracts with those end users, regardless of whether, for that purpose, they use the core platform services of the gatekeeper».

Bestemmelsen sikrer at apputviklere og andre bedriftsbrukere som distribuerer via for eksempel App Store, fritt kan informere sine kunder om alternative tilbud utenfor App Store, lede kundene dit, og forklare hvor de kan gjøre kjøp. Kommisjonen fant at Apple ikke overholdt denne forpliktelsen i App Store på grunn av en rekke restriksjoner som hindret bedriftsbrukere i å benytte seg av alternative distribusjonskanaler. Dette resulterte i at forbrukere ikke kunne dra nytte av alternative og potensielt billigere tilbud.

Som konsekvens av bruddet ble Apple ilagt en bot på 570 millioner euro og beordret til å fjerne de ulovlige restriksjonene. Apple har allerede varslet anke av vedtaket.

Vedtaket mot Meta

For Meta gjaldt vedtaket brudd på DMA artikkel 5 (2), som regulerer

hvordan «gatekeepers» kan behandle personopplysninger. Bestemmelsen forbyr behandling av personopplysninger fra sluttbrukere for annonseringsformål, kombinasjon av personopplysninger fra ulike tjenester, kryssbruk av personopplysninger mellom tjenester, og innlogging av brukere på andre tjenester for å kombinere personopplysninger. Slik behandling av personopplysninger kan kun gjøres dersom sluttbrukeren har samtykket til dette. Samtykket må være i tråd med kravene til samtykke i GDPR.

I november 2023 introduserte Meta en binær «samtykke eller betale»-annonsemodell for EU-brukere av Facebook og Instagram. Brukerne fikk valget mellom å samtykke til kombinasjon av deres personopplysninger for bruk til personlig tilpasset annonsering, eller å betale et månedlig abonnement for en annonsefri tjeneste.

Kommisjonen fant at denne modellen bryter med DMA fordi den ikke ga brukerne muligheten til å avstå fra å gi samtykke samtidig som de ble gitt tilgang til en tjeneste uten personlig tilpassede annonser, men som ellers er tilsvarende tjenesten med personlig tilpassede annonser. Metas modell tillot ikke brukerne å

avgi frivillig samtykke til behandling av deres personopplysninger for personlig tilpasset annonsering.

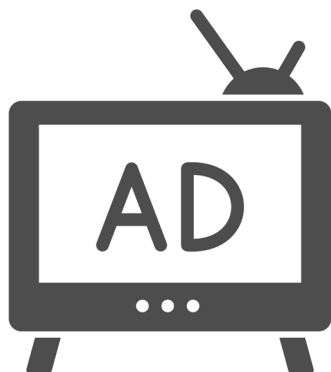
I november 2024, etter dialog med Kommisjonen, introduserte Meta en ny versjon av modellen som angivelig bruker mindre personopplysninger for personlig tilpassede annonser. Til tross for denne endringen ga Kommisjonen en bot på 228 millioner euro for perioden mellom mars 2024, som er da DMA-forpliktelsene ble juridisk bindende, og november 2024, som er tidspunktet da den nye modellen ble introdusert.

Metas Chief Global Affairs Officer, Joel Kaplan, har uttalt at vedtaket er et forsøk på å handikappe suksessfulle amerikanske selskaper. Ifølge medieoppslag forventes det at Meta vil anke vedtaket til EU-domstolen. Det er verdt å merke seg at Metas nye annonsemodell ikke ble vurdert i dette vedtaket, men at det pågår en undersøkelse om den nye modellen også bryter med DMA.

Øvrige beslutninger fra Kommisjonen

Samtidig med disse vedtakene kunngjorde Kommisjonen også at de avslutter etterforskningen av Apples brudd på forbrukerens valgfrihet etter DMA artikkel 6 (3), som blant annet pålegger «gatekeepers» å gjøre det enkelt for brukeren å avinstallere apper og endre standardinnstillinger. Etter samtaler med Kommisjonen har Apple nemlig gjort det mulig for brukere i EU å avinstallere Safari-nettleseren, bilder-appen og andre forhåndsinstallerte apper på Apple-produkter.

Videre kunngjorde Kommisjonen at Facebook Marketplace ikke lenger skal betraktes som en tjeneste som faller inn under reglene i DMA. Beslutningen begrunnes med at Marketplace hadde færre enn 10 000 bedriftsbrukere i 2024, og dermed ikke lenger er en slik viktig portal i det digitale markedet.



Illustrasjon: Colourbox.com

Konsekvenser for norske virksomheter

Selv om ingen norske virksomheter er underlagt de samme strenge reglene under DMA som Apple og Meta, vil disse vedtakene indirekte kunne påvirke norske virksomheter på flere måter:

1. App-utviklere og teknologiselskaper:

Norske virksomheter som distribuerer apper gjennom App Store bør være oppmerksomme på at Apple nå må tillate kommunikasjon om alternative betalingsløsninger og distribusjonskanaler. Dette kan åpne for nye forretningsmuligheter og reduserte kostnader. Denne plikten som pålegges Apple innebærer at norske virksomheter bør revurdere sine prisstrategier for digitale produkter og tjenester, og kan medføre mer fleksibilitet i prissetting og promotering overfor europeiske kunder.

2. Annonserer på Meta-plattformer:

Norske virksomheter som annonserer på Facebook og Instagram bør følge nøye med på utviklingen rundt Metas nye annonsemodell, ettersom dette kan påvirke hvor effektivt norske virksomheter kan målrette annonser til europeiske borgere. Dagens annonsemodell vil kunne måtte endres i fremtiden. Kravene til samtykker under DMA samsvarer med kravene under GDPR, og det er dermed også grunn til å tro at dersom samtykket innhentet fra Meta under den

nye annonsemodell er ugyldig under DMA, vil det også være ugyldig under GDPR. Norske virksomheter som utfører persontilpasset annonsering på Facebook og Instagram bør dermed være forsiktige med å bygge på samtykker innhentet fra Meta, men anbefales i stedet å innhente sine egne samtykker til slik persontilpasset markedsføring.

3. Konkurransesituasjon: Norske virksomheter som konkurrerer med store teknologiplattformer kan potensielt dra nytte av et mer balansert digitalt marked i Europa, med reduserte barrierer for konkurranse. For flere norske virksomheter kan det bli nødvendig å revurdere distribusjonsstrategier og kundeakkvisisjon. Dersom norske virksomheter er oppmerksomme på disse fortrinnene vil man i større grad aktivt kunne sørge for at de utnyttes maksimalt.

Konklusjon

EU-kommisjonens vedtak mot Apple og Meta representerer en tydelig håndhevelse av DMA og sender et kraftfullt signal om at digitale «gatekeepers» må respektere reglene. For norske virksomheter betyr dette potensielt nye muligheter i et mer åpent digitalt marked, men også begrensninger i adgangen til å markedsføre egne tjenester på plattformene til «gatekeepers».

Selskapene har antydnet at de vil anke vedtakene, noe som betyr at den juridiske prosessen kan fortsette i flere år fremover. Norske virksomheter bør derfor følge utviklingen nøye, særlig hvis de har interesser som direkte eller indirekte berøres av disse plattformenes vilkår og praksis.

Kine Emilie Helgeneseth, fast advokat i avdelingen HITEK i Advokatfirmaet Selmer, Oslo og Henriette Solbakke Jørgensen, fast advokat i samme avdeling.



Wikström
& PARTNERS

Anton Karlsson och Karin Tilly

Uppdaterade modellavtalsklausuler för upphandling av AI

EU:s Community of Practice on Public Procurement of AI har den 5 mars 2025 publicerat en ny version av sina modellavtalsklausuler för upphandling av AI ("EU AI Model Contractual Clauses")¹. Klausulerna utgår från kraven och skyldigheterna i EU:s AI-förordning², huvudsakligen de krav och skyldigheter som framgår av kapitel III om AI-system med hög risk, och är framtagna för att användas av offentliga aktörer vid upphandling av AI-system med externa leverantörer. Modellklausulerna är avsedda att användas fram till att AI-förordningen blir tillämplig i sin helhet,



Illustrasjon: Colourbox.com

och medför att aktörer som inkorporerar modellavtalsklausulerna i sina avtalsrelationer säkerställer efterlevnad av AI-förordningen. Modellavtalsklausulerna framtagna av Community of Practice är inte officiellt antagna av EU-kommissionen, utan ska betraktas som ett arbetsdokument som EU-kommissionen givit stöd till.

Det har tagits fram två versioner av modellklausulerna, en anpassad för AI-system med hög risk enligt klassificering i AI-förordningen, samt en förenklad version anpassad för AI-system utan hög risk, men som fortfarande kan anses medföra

en risk för hälsa, säkerhet och grundläggande rättigheter. Den förenklade versionen kan också användas vid upphandling av andra algoritmiska system som inte kvalificeras som AI-system enligt AI-förordningen. Modellklausulerna kompletteras med en kommentar, med vägledning för praktisk tillämpning av modellklausulerna.

Modellavtalsklausulerna är anpassade för offentliga aktörer, men visst innehåll kan även lämpa sig att användas av privata aktörer, efter en bedömning i det enskilda fallet. Modellklausulerna utgör dock inte i sig fullständiga avtal och bör därför inte användas uteslutande för att reglera ett avtalsförhållande, utan bör i stället biläggas befintliga avtal tillsammans med allmänna villkor.

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

¹ <https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/updated-eu-ai-model-contractual-clauses>.

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



Gorrissen Federspiel

Tue Goldschmieding

Andet nyt i Danmark

Nye tiltag skal øge sikkerheden i det danske Superliga miljø

To danske 3F Superliga klubber, Brøndby IF og F.C. København, har tidligere fået tilladelse fra det danske datatilsyn (»Datatilsynet«) til at anvende ansigtsgenkendelse på deres stadioner. Foreningen af Divisionsklubber i Danmark (»Divisionsforeningen«), som er branche-, interesse- og arbejdsgiverorganisationen for danske fodboldklubber, har nu ansøgt Datatilsynet om tilladelse til, at de resterende danske 3F Superliga klubber også kan benytte ansigtsgenkendelse. Ansøgningerne

og nedenstående initiativer fra den danske justitsminister sker i lyset af en række uroligheder, der har præget danske Superligakampe i efteråret 2024.

I forlængelse af disse uroligheder afholdt justitsministeren møder med fodboldens aktører og politiet, for at drøfte nye tiltag, der skal sikre mod fremtidige problemer. Justitsministeren foreslog på mødet, at man gør det muligt fra lovgivers side at give strakskarantæner. Derudover at det bliver muligt for fodboldklubberne at dele videooptagelser fra deres overvågning med

hinanden. Formålet er at give klubberne bedre mulighed for at identificere og registrere hooligans, så de kan forhindre dem i at deltage i fodboldkampe og dermed øge sikkerheden.

Læs pressemeddelelse fra Justitsministeriet her: <https://www.justitsministeriet.dk/pressemeddelelse/efter-fodboldmøde-i-parken-nye-forslag-fra-justitsministeren-og-klubberne-skal-tackle-problemer-paa-tribunerne/>

Av Tue Goldschmieding, partner i Gorrissen Federspiel og dansk redaktør for Lov & Data.



