

Lov & Data

Desember 2025

Nr. 164 4/2025

Innhold

Leder	2
<i>Artikler</i>	
Veikko Vauhkonen Implementing the NIS 2 Directive in Finland: The New Cybersecurity Act	4
Veronika Lundqvist Kreativitet i KI-alderen: et opphavsrettslig perspektiv	7
Anna Stensrud The COMPAS case's impact on the EU's AI Act ..	11
Ole Martin Moe og Trine Smedbold Bedre (over)føre var? Latombe-sakens betydning for EU-US Data Privacy Framework	17
Hanne Pernille Gulbrandsen, Anniken Meuche Henriksen og Veronika Lundquist Datadelingsloven og veien mot et åpnere Norge ..	19
Rune Opdahl og Håvard Sveier Ottemo Nye retningslinjer for melding til Datatilsynet ved brudd på personopplysningsikkerheten	22
Olav Torvund 40 år med nordiske konferanser i rettsinformatikk ..	24
Stein Schjølberg United Nations Convention against Cybercrime and The Signing Ceremony	27
Ove A. Vanebo og Anne Buan Exit-regulering av skytjenester	33
Jurgita Lapienytė We Need to Talk About China. You Either Keep the Costs Low or Keep Control	39
JusNytt	40
Halvor Manshaus AI på treningsrommet – Getty Images vs. Stability AI Limited	46
<i>Rettsinformatisk litteratur med mer</i>	<i>46</i>
<i>Nytt om personvern</i>	<i>47</i>
<i>Nytt om immaterialrett</i>	<i>54</i>
<i>Nytt om annet</i>	<i>61</i>



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, rettsinformatiker, 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

Layout: Aksell AS

Leder

Risiko og Nordisk samarbeid

I begynnelsen av november gikk Nordisk konferanse for rettsinformatikk av stabelen. For 40. gang samlet nordiske jurister og teknologer med interesse for de etter hvert mange møtepunktene mellom jus og teknologi seg for å dele kunnskap og erfaring. Gode diskusjoner og samtaler mellom deltakerne er en viktig del, og et av temaene som var gjenstand for livlig diskusjon, var risikobasert lovgivning.

På «vårt» område har risikobasert lovgivning blitt den nye normen, der tydelige krav eller forbud er erstattet med større fleksibilitet, der målet er å tilpasse tiltak til den risiko som faktisk gjelder den aktuelle virksomheten.

Det er lett å se fordelene ved et risikobasert system; spesifikke regler som skjærer alle virksomheter over en kam er forutsigbare, men også trege og lite egnet til å møte rask teknologisk utvikling og et økende trusselbilde. At den enkelte virksomhet derfor best selv kan vurdere hvilken risiko som er av størst betydning for dem, gir mening. At en offentlig tilbyder av helsetjenester har et annet risikobilde enn en lokal blikkenslager eller en internasjonal produksjonsbedrift er åpenbart.

GDPR, Digitalsikkerhetsloven, DORA-loven, KI-forordningen og NIS2 er alle eksempler på risikobasert lovgivning der kravene til den enkelte virksomhet varierer med



Sara Habberstad

den risiko som er relevant for dem. Modellen gir en mulighet for fleksibilitet og pragmatisme som er en klar fordel i dagens verden der man ønsker innovasjon og fremskritt på mange områder. Imidlertid er det også lett å peke på utfordringer; risikovurderingen krever ikke bare innsikt i lovens krav, det krever også dyp kompetanse på fagområdet og virksomheten man arbeider innenfor, og det krever jevnlig oppfølging. Risikovurdering i seg selv er ikke minst også et fag som i langt større grad enn tidligere er noe de fleste jurister må forholde seg til i det daglige.

Forventningen til tilsynene er ikke lenger å føre tilsyn med oppfyllelse av en fastsatt liste med tekniske krav. Tilsyn må utvikle metoder for tilsyn som er effektive, rettferdige og proporsjonale, og som i like stor grad som tiltak og gjennomføring tar for seg selve risikovurderingen som er gjennomført, og vurderingen av den i lys av virksomheten.

Forventningene til virksomheter er ikke lenger å etterleve tydelige krav, men å gjennomføre kompetente risikovurderinger som gir et fornuftig grunnlag for de tiltak virk-

somheten skal iverksette for å overholde regelverket. Det er ikke lenger nok å kjenne rettsreglene i seg selv; man må også forstå sannsynlighet, konsekvens, og trusselaktører i eget marked.

Kravene som stilles til selve risikovurderingen vil i seg selv kunne være omfattende, om man må kunne spørre om alle omfattede virksomheter vil være i stand til å ta del i den fleksibiliteten som lovgivningen åpner for. Offentlige og private virksomheter har i dag et stort behov for kompetanse for å kartlegge risiko, for å sikre at tiltak som implemente-

res er gode nok, og ikke for omfattende. Målet er at risikoen til syvende og sist er akseptabel, uten at hindringene oppleves for store.

” Deling av kompetanse i Norden er nettopp det du også tar del i nå når du sitter med en utgave av Lov & Data foran deg.

Risikobasert lovgivning har reist, og kommer til å reise, en rekke problemstillinger i tiden som kommer;

- Vil større krav til investering i tverrfaglig kompetanse og dokumentasjon skape større ulikhet mellom virksomheter?
- Vil standarder for risikovurdering utover de vi kjenner i dag utformes?
- Vil tilsynsmyndighetenes tilsyn med risikovurderinger føre til nye metoder for tilsyn?
- Vil domstolenes vurderinger påvirke standarder og metoder?

I likhet med alle de problemstillinger vi møter på vårt område, er den beste veien mot god mulig håndtering og forståelse nettopp samarbeid, dialog og deling av kompetanse, som vi fikk ta del i sammen med nordiske kolleger sist uke.

Deling av kompetanse i Norden er nettopp det du også tar del i nå når du sitter med en utgave av Lov & Data foran deg. Et knippe av problemstillinger ligger klar for å gi et innblikk i det som beveger seg på området i våre Nordiske land.

*Sara Habberstad,
advokat, VP Legal & Compliance
i LINK Mobility Group.
Hovedredaktør for Lov & Data.*



Illustrasjon: Colourbox.com

Implementing the NIS 2 Directive in Finland: The New Cybersecurity Act

By Veikko Vauhkonen

This article continues the series of articles on the NIS2 directive and its implementation in the Nordic countries. Previous article from Sweden:

- Agne Lindberg, Petri Dahlström, Klara Thyren: Ny cybersäkerhetslag – den svenska regeringens förslag till införlivande av NIS2-direktivet *Lov & Data* nr. 163 3/2025

On April 8th 2025, Finland's new Cybersecurity Act (124/2025) entered into force, implementing the NIS 2 Directive in Finland. This marks a milestone, as it is the first act in Finland to impose horizontal cybersecurity-related obligations for essential and important entities.

At the same time, several implementing provisions of NIS 2 Directive's predecessor, the NIS Directive, were revoked in relevant sectoral acts as those became unnecessary and duplicator after adoption of the new Cybersecurity Act. The new Act has been in force for roughly six months and both entities and supervisory authorities are gathering experiences on applying it.

The Cybersecurity Act concentrates the provisions regarding NIS 2 obligations in Finland. It covers essential and important entities in



Veikko Vauhkonen

all sectors within the scope of the Directive except Banking, Financial market infrastructure and Public administration. For the Banking and Financial market infrastructure the DORA-regulation (EU) 2022/2554 applies instead of the Cybersecurity Act. For public administration entities the NIS 2 obligations are incorporated into the Act on Information Management in Public Administration (906/2019). The act regulates cybersecurity related aspects of public administration information management in Finland. NIS 2 obligations were included into new Chapter 4 a of the Act and are similar to the Cybersecurity Act.

” The Cybersecurity Act concentrates the provisions regarding NIS 2 obligations in Finland.

The Finnish implementation follows mainly the NIS 2 Direc-

tive's level of minimum harmonization. This has been justified particularly from the perspective of operators engaged in cross-border activities. For those entities, following the level of minimum harmonization makes it easier to align obligations or requirements with those in other Member States – and vice versa should it become necessary.

Scope and definition of an “entity”

Obligations of the Cybersecurity Act apply to an “entity”. In accordance with the NIS 2 Directive, an entity may be any legal or natural person who engages in an activity referred to in the annex of the Act. In addition, it requires that the entity is larger than a medium-sized enterprise, or that an exception applies which brings the operator within the scope of the Act regardless of its size. Such an exception applies, for example, to certain digital infrastructure entities. However, small and micro-sized operators are generally excluded from the scope of the Act.

Furthermore, the Cybersecurity Act will apply to all “critical entities” defined as such in the future in accordance with the CER Directive. The Cybersecurity Act will apply to all critical entities regardless of the sector of their activities or their size. The CER Directive requires critical entities to be defined for the first time by July 2026.

Due to its broad scope, the Cybersecurity Act affects a great number of Finnish companies both directly and indirectly. A significant

proportion of medium-sized and larger companies fall directly within the scope of the Cybersecurity Act. For companies that the Act does not directly cover, it may still have indirect effects where company is part of the supply chain of an essential or important entity. In those cases, it's likely that the risk management measures of a NIS 2 entity may have indirect effects for companies that are suppliers for NIS 2 entities (or even customers in some situations).

Obligations for entities

Risk management

The Cybersecurity Act requires entities to identify, assess, and manage risks posed to the security of networks and information systems used for their operations or for the provision of their services. Generally the provisions on risk management stay loyal to Article 21 of the NIS 2 Directive. The Cybersecurity Act obliges entities to prepare and maintain an up-to-date cybersecurity risk management model. Through the cybersecurity risk management model, entities must identify and evaluate the risks affecting networks and information systems, and their physical environment, applying an all-hazards approach. Entities must also define, describe and implement appropriate and proportionate risk management measures. The risk management model must be prepared within three months from the date on which the Act becomes applicable to an entity.

The Cybersecurity Act requires entities to implement proportionate technical, operational, or organizational safeguards in accordance with the cybersecurity risk management model, in order to manage risks to the security of communications networks and information systems and to prevent or minimize adverse effects. In regard to risk management measures, entities must take into account at least the list of items mentioned in Article 21(2) in the

NIS 2 Directive. The Cyber Security Act also sets the purpose of the risk management: to protect networks and information systems, as well as their physical environment, from incidents and their impacts. In addition to that, sectoral competent authorities may require that sector-specific items are included as well.

Incident notifications

Entities are obliged to report any significant incidents in accordance with article 23 of the NIS 2 Directive. In practice, incident reports are submitted via an online portal maintained by NCSC-FI. The incident reports are made to the competent authority, which forwards them to the CSIRT unit. The CSIRT unit may provide technical guidance or support for the entity upon request.

Incident reporting consists of three stages. Early warning must be submitted within 24 hours of becoming aware of the significant incident. Incident notification must be submitted within 72 hours of becoming aware of the significant incident. Both notifications may be submitted at once if it's possible within 24 hours. Final report must be submitted within one month after the submission of the incident notification. Where that is not possible or upon the competent authority's request, the entity must also submit an intermediate report.

The threshold for "significant incident" follows the threshold set in the NIS 2 Directive. There is no obligation for entities to report other events than significant incidents. On a voluntary basis entities may also report other incidents or events and competent authorities will process all notifications. If an early-warned-incident turns out to not to be a significant incident, entities are not obliged to submit an incident report or a final report.

Registry of entities

Entities must also submit and update their contact information to

the competent authorities. Competent authorities keep a list of NIS 2 entities within their respective sectors – "registries of entities". Entities must provide their information for the competent authority and the register for the first time within one month after the Act becomes applicable to them.

The Cybersecurity Act and other legislation

The Cybersecurity Act is a general act with respect to the obligations it imposes. It sets a minimum level for risk management measures and incident notification obligations. Following a similar logic as the NIS 2 Directive, the Cybersecurity Act does not impede applying sector-specific obligations concerning cybersecurity risk-management or incident notifications to the entities. Where those sectoral obligations exist and are at least equivalent in effect to the obligations laid down in the Cybersecurity Act, those will apply instead of the Cybersecurity Act.

The Cybersecurity Act also recognizes the Commission's power to adopt implementing acts on cybersecurity risk management measures or significant incident's threshold as per articles 21 and 23 of the NIS 2 Directive. Where the Commission has adopted such implementing acts, they apply as such to entities that are within its scope, together with and complementing the provisions of the Cybersecurity Act. Therefore, the Commission Implementing Regulation (EU) 2024/2690 concerning certain digital infrastructure entities applies as such to entities within its scope prior to the Cybersecurity Act.

Jurisdiction and territoriality

The Cybersecurity Act applies to entities that are established in Finland. Therefore, as regards to jurisdiction, the act follows the provisions of article 26 of the NIS 2 Directive. The Cybersecurity Act does not apply to entities that are

established in other EU member states even if they offer goods or services in Finland. An exception to that are providers of public electronic communications networks or providers of publicly available electronic communications services. Those entities will be subject also to the Finnish Cybersecurity Act based on provision of services in Finland.

Competent authorities and supervision

The supervision of the Cybersecurity Act is decentralized to sector-specific competent authorities. The competent authorities responsible for supervision are Finnish Transport and Communications Agency (Traficom), Finnish Energy authority, Finnish Safety and Chemicals Agency (Tukes), National Supervisory Authority for Welfare and Health (Valvira, after 1.1.2026 Finnish Supervisory Agency) One regional ELY Centre (after 1.1.2026 Economic Development Centre), Finnish Food Authority and Finnish Medicines Agency (Fimea). Additionally, the Financial Supervisory Authority (FIN-FSA) oversees the NIS 2 Directive and the DORA regulation for Banking and Financial market infrastructure sector entities. Competent authorities are obliged to cooperate especially where an entity is subject to more than one supervisory power of more than one competent authority.

In accordance with the NIS 2 Directive, supervision is focused by default to essential entities. If a competent authority has a justified reason to suspect that an important entity has not complied with the Cybersecurity Act, it may enforce supervision to that entity as well.

CSIRT unit (CERT-FI) is located within the National Cyber Security Centre Finland (NCSC-FI). CSIRT and NCSC-FI are within the Finnish Transport and Communications Agency Traficom. Traficom also oversees and facilitates the cooperation between competent authorities



Illustrasjon: Colourbox.com

and is the single point of contact in Finland for the NIS 2 Directive.

Based on infringement of the Cybersecurity Act an administrative fine may be imposed to an entity. The maximum level of administrative fines in Finland is the minimum allowed by the NIS 2 Directive. For an essential entity it means that administrative fines may rise to up to EUR 10 000 000 or to a maximum of at most 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher. The administrative fine is imposed by a special board that composes of members appointed by the competent authorities. An entity may appeal to an administrative court against a decision that imposes administrative fines. Such an appeal is an administrative case and subject to provisions of the Finnish Administrative Judicial Procedure Act.

Conclusions

Finland has decided to follow the minimum level harmonization of the NIS 2 Directive with the newly

adopted Cybersecurity Act. The Act leaves leeway for entities on how to organize and adopt risk management measures as it is highly risk-based and does not introduce detailed risk management measures that would cover all entities in scope. It lays down objectives for risk management, minimum list of matters to be considered and criteria for evaluating acceptable level of risk management. As legislation is a slow and inefficient way to increase cybersecurity in general, the risk-based approach of the Act might seem like a self-explanatory approach. However, while the Cybersecurity Act leaves essential and important entities a lot of room to organize their risk management, it might also increase compliance costs or regulative burden, especially if the minimum level of risk management measures proves to be too unclear for entities. The practical effects of the Act remain to be seen in the near future.

Veikko Vauhkonen is a Senior Officer for Legal Affairs at the Ministry of Transport and Communications of Finland.

Kreativitet i KI-alderen: et opphavsrettslig perspektiv

Av Veronika Lundqvist

Innledning

Flere av oss bruker generativ KI til å hjelpe oss med ulike oppgaver i hverdagen og i jobbsammenheng. Blant de mest vanlige er bruk av språkmodeller som Open AIs Chat GPT til å utforme tekster som e-poster, arbeidsdokumenter, o.l. Dermed kan man spare seg for den tankeprosessen som kreves for å sammenstille informasjon til et gitt formål.

Den utbredte bruken av generativ KI reiser flere spørsmål, blant annet hva det gjør med vår vilje og evne til å tenke kreativt. Utviklingen har derfor reist flere diskusjoner innenfor kunst- og kulturbransjen som nettopp livnærer seg på kreativ skaperkraft. Rettslig sett er det opphavsretten som skal tilrettelegge for kulturell produksjon,¹ og som dermed er det nærmeste vi kommer et regelsett som skal bidra til å ivareta menneskelig kreativitet.

I denne artikkelen vil jeg undersøke forholdet mellom opphavsrett, KI og kreativitet, med et særskilt fokus på vurderingen av hva som kreves for at noe kan regnes som et åndsverk («verkshøydevurderingen»). Jeg vil undersøke hvilken rolle kreativitet spiller i verkshøydevurderingen, og basert på dette vurdere om KI-generert innhold kan regnes som et åndsverk. Til slutt vil jeg kort vurdere den praktiske betydningen av å tillegge særegne trekk ved menneskelig kreativitet vekt i opphavsrettslig sammenheng.



Veronika Lundqvist

Kreativitet, opphavsrett og KI

Kreativitet er en grunnleggende ingrediens for menneskelig nyskaping, og en evne som brukes hver gang vi skaper innhold. Opphavsretten gir rettigheter til de som skaper kreativt innhold, og fungerer dermed som et insentiv til kulturell produksjon. Det er først og fremst kunstnere og skapere av kulturuttrykk som nyter godt av opphavsrettens vern. Opphavsretten har imidlertid betydning også utenfor kunstbransjen: innhold skapt av arbeidstakere som rapporter, markedsføringsmateriale, design, programvare og koder, vil typisk utgjøre del av arbeidsgiverens immaterielle verdier.

Generativ KI utfordrer ideen om at kun mennesker kan skape kreativt innhold. KI-verktøy kan generere resultater av høy kvalitet, mye mer effektivt enn oss selv. Forskning viser imidlertid at bruk av språkmodeller kan redusere hjerneaktiviteten betydelig, svekke eierskap til det som produseres, og gi dårligere evne til å gjengi informasjonen man har skre-

vet om.² Med kunnskap om at kreativitet er en muskel som må trenes opp, er det grunn til bekymring for at ukritisk bruk av generativ KI svekker vår evne til å tenke kreativt.³

Det opphavsrettslige verkshøydekravet kan sees som en terskel eller minimumsstandard for når noe regnes som et åndsverk som er beskyttet av opphavsrett. Når KI-verktøy kan skape innhold som er like bra, eller bedre, enn det vi kan, og prosessen tilsynelatende imiterer det som skjer i hjernen når vi skaper innhold, blir det utfordrende å definere hva som skiller menneskelig skaperkraft fra maskinell produksjon. Dette gjenspeiles i de mange diskusjonene om KI-skapt innhold kan regnes som kunst, og om KI-systemer i seg selv kan anses som kreative.⁴

” Det opphavsrettslige verkshøydekravet kan sees som en terskel eller minimumsstandard for når noe regnes som et åndsverk som er beskyttet av opphavsrett.

1 Se åndsverkloven (åvl.) § 1, bokstav a

2 Nataliya Kosmyna m.fl. (Cornell University), “Your Brain on ChatGPT: Accumulation of Cognitive Debt when Using an AI Assistant for Essay Writing Task”: <https://arxiv.org/pdf/2506.08872> s. 2

3 Se f.eks. <https://psykologisk.no/2025/08/kunstig-intelligens-truer-menneskelig-kreativitet/>

4 Se f.eks. <https://www.forskning.no/kunstig-intelligens/kan-kunstig-intelligens-naere-kreativ-chatgpt-var-bedre-enn-mennesker-pa-en-klasse-test/2253296>

Med dette som bakgrunn får verkshøydevurderingen en ny dimensjon. Dersom KI-generert innhold ikke kan regnes som åndsverk fordi tilblivelsesprosessen mangler menneskelig kreativitet, blir verkshøydevurderingen ikke bare en terskel, men også en definisjon av hva som kvalifiserer som en menneskelig kreativ prosess. Dette vil igjen kunne bidra til å skape et insentiv til å opprettholde en kreativ rolle ved bruk av KI, heller enn å overlate skapelsesprosessen til verktøyet. Slik kan opphavsretten bidra til å bevare og stimulere menneskelig kreativitet i møte med teknologi som ellers kan erstatte den.

Betydningen av kreativitet for opphavsrettslig vern Begrepet «åndsverk»

Det er kun åndsverk som er beskyttet av opphavsrett.⁵ Et åndsverk er litterære eller kunstneriske verk av enhver art, som er «uttrykk for original og individuell skapende åndsinnsett». ⁶ Sistnevnte gir uttrykk for verkshøydekravet. Kravet er i rettspraksis for Høyesterett og EU-domstolen uttrykt som at verket må være resultat av en individuelt preget skapende innsats, og fremstå som originalt.⁷ Verket må være originalt i den forstand at det er opphaverens egne intellektuelle frembringelse,⁸ og prosessen må avspeile opphaverens personlighet, noe som forutsetter at vedkommende har kunnet uttrykke sine frie og kreative valg.⁹ Terskelen er imidlertid lav, og det stilles ingen kvalitetskrav.

Til å være et juridisk krav er innholdet av verkshøydekravet slik det er formulert i loven og rettspraksis relativt abstrakt. Det er kanskje uunngåelig når kravet knytter seg til den komplekse eller mystiske – ref.

henvisningen til noe åndelig – prosessen som utspiller seg i hjernen når vi skaper innhold. Dette tyder ironisk nok på at kravet knytter seg til noe særegent menneskelig, og ikke en mekanisk prosess. Det er da også bred enighet om at maskiner, inkl. KI-systemer, ikke kan være opphavere av åndsverk.¹⁰

Verkshøydekravet retter seg altså mot skapelsesprosessen og ikke sluttresultatet. Mens teknologisk utvikling generelt har gjort det enklere å skape innhold, representerer generativ KI noe nytt ved at verktøyene i mye større grad enn andre digitale verktøy kan overta betydelige deler av skapelsesprosessen. Dette reiser et grunnleggende spørsmål: Hvor mye kreativ innsats kreves for at noe kan regnes som et åndsverk – og hva er det unike ved den menneskelige skapelsesprosessen som gjør at den kvalifiserer for opphavsrettslig vern?

Kreativitet som del av verkshøydekravet

Kreativitet er utvilsomt et sentralt element i verkshøydekravet, men samtidig det vanskeligste å knytte et konkret innhold til. Kreativitetsbegrepet brukes i ulike sammenhenger med varierende betydning, men i opphavsrettslig sammenheng forstås det primært som en prosess hvor det har vært rom for frie og personlig pregede valg.¹¹ Prosessen må videre resultere i et konkret uttrykk, da ideer ikke kan beskyttes av opphavsrett.¹² Utover dette gir ordlyden og rettspraksis begrenset med veiledning.

Juridisk teori kan bidra til ytterligere konkretisering. Jane C. Ginsburg publiserte i 2003 en komparativ studie av hva som kjennetegner

en «skaper»¹³ i opphavsrettslig forstand på tvers av rettssystemer, kalt «The Concept of Authorship in Comparative Law».¹⁴ Ginsburg konkluderte med at den kreative skaperen kjennetegnes av «sinn over muskler» – det er personen som former verkets uttrykk og deretter foretar en kontrollert styring av utviklingen av verket som er skaperen, ikke personen som bare følger ordre for å skape verket.¹⁵ Forenklet innebærer dette at man både må utvikle konseptet/ideen og ha kontroll over verkets endelige uttrykk, for å kunne regnes som verkets skaper. Dette kan sees som en konkretisering av prinsippet om at det kun er konkrete uttrykk som har vern og ikke ideer.

I en nyere artikkel publisert via SSRN, «Struggling for creativity and the beauty of human error – copyright authorship meets generative AI and neuroscience», foretar Alina Trapova en tverrfaglig analyse av kreativitetsbegrepet i kontekst av den opphavsrettslige verkshøydevurderingen.¹⁶ Hun argumenterer for at ufullkommenheter, frustrasjon og emosjonell kompleksitet er sentrale kjennetegn ved kreative prosesser, og at dette kan bli en viktig del av verkshøydevurderingen i møte med KI-utviklingen.¹⁷ Ved

13 Den mest passende oversettelse av det engelske begrepet «author», som er videre enn forfatter

14 Jane C. Ginsburg, «The Concept of Authorship in Comparative Law», (2003) 52 DePaul Law Review 1063: https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1695&context=faculty_scholarship

15 Ibid. s. 1072

16 Alina Trapova, «Struggling for Creativity and the Beauty of Human Error - Copyright Authorship Meets Generative AI and Neuroscience» (July 23, 2025). Faculty of Laws University College London Law Research Paper No. 11/2025, Tilgjengelig på SSRN: <https://ssrn.com/abstract=5363523> or <http://dx.doi.org/10.2139/ssrn.5363523>

17 Ibid. s. 1

5 Åvl. § 2 (1)

6 Åvl. § 2 (2)

7 Se f.eks. HR-2017-2165-A, avsnitt 66

8 C-5/08 Infopaq, avsnitt 37

9 C-145/10 Painer, avsnitt 94

10 Se f.eks. Ole-Andreas Rognstad, Opphavsett (2. utgave 2019), s. 87

11 Ref. gjennomgangen ovenfor

12 Se f.eks. Rt. 2013 s. 822 (Ambassadør), avsnitt 49

å støtte seg på Ginsburgs prinsipper fra 2003-artikkelen og tverrfaglige perspektiver fra nevrologien, konkluderer hun med at KI-generert innhold ikke kan regnes som åndsverk.¹⁸

Både Ginsburg og Trapova tar til orde for et økt fokus på opphavsrettens rolle i å ivareta menneskelig kreativitet.¹⁹ Som nevnt innledningsvis er det et implisitt formål i opphavsretten å tilrettelegge for menneskelig kreativ utfoldelse. I møte med teknologi som har potensiale til å erstatte menneskelig kreativitet, fremstår det som i tråd med opphavsrettens formål å tillegge psykologiske og nevrologiske særtrekk ved menneskelig kreativitet vekt i vurderingen av verkshøydekravet. Dette vil ikke bare bidra til å klargjøre og konkretisere det noe uklare verkshøydebegrepet, men også skape insentiv til å opprettholde kreativiteten ved bruk av KI-verktøy.

Kan KI-generert innhold regnes som åndsverk?

Tekster skapt av språkmodeller

Det finnes ulike måter å bruke KI på, men blant de vanligste er bruk av språkmodeller til å generere tekstinnhold ved hjelp av ledetekster (prompts). Den videre fremstillingen vil kun fokusere på språkmodeller, men tilsvarende vurdering vil være relevant ved bruk av annen generativ KI, som bildegenereringsprogrammer.

Prosessen med å utforme en ledetekst kan innebære en hel del kreativitet. Brukeren må ha en forestilling om hva som skal produseres, og ta valg og vurderinger for å utforme en ledetekst som i størst mulig grad fanger det ønskede resultatet fra språkmodellen. At det finnes såkalte «prompt engineers» som arbeider profesjonelt med å utforme effektive ledetekster, er illustrere-

rende. Jo mer detaljert og beskrivende ledeteksten er, jo bedre vil typisk resultatet bli. Gode ledetekster kan derfor etter omstendighetene i seg selv utgjøre et åndsverk.²⁰

Innholdet som deretter genereres av språkmodellen, skapes gjennom en teknisk prosess som avhenger av hvilke data modellen er trent på, hvordan den er finjustert, og statistiske beregninger av hvilket svar som best samsvarer med ledeteksten. Samtidig er det mye vi ikke vet om hvordan denne prosessen fungerer, og selv med identisk ledetekst kan resultatene variere. Det er også dokumentert at språkmodeller kan hallusinere og gi feilaktige svar. Selv med en detaljert ledetekst har brukeren altså verken kontroll over det endelige innholdet eller innsikt i hvorfor og hvordan de konkrete ordvalgene ble foretatt.

Som følge av dette vil det være en distanse mellom de konkrete ordene som genereres og brukerens eventuelle kreative innsats i forkant av den maskinelle prosessen. Brukerens mulighet til å ta frie og kreative valg er forbeholdt prosessen med å utforme en passende ledetekst. Hvordan språkmodellen deretter tolker ledeteksten, er bestemt av en teknisk prosess uten rom for frie valg fra brukerens side. Dermed mangler tilsynelatende den nødvendige koblingen mellom brukerens opprinnelige idé og det konkrete uttrykket.

Ginsburgs to-delte standard underbygger dette. Utformingen av ledetekster kan kvalifisere som den første delen av en kreativ prosess, der brukeren former tekstens uttrykk gjennom subjektive vurderinger og valg. Men den andre delen – den kontrollerte utformingen av verkets konkrete uttrykk – overtas av språkmodellen. Sagt på en annen måte så overtar språkmodellen

delen av den kreative prosessen som knytter seg til konkretiseringen av verket, som er en viktig del av det opphavsrettslige verkshøydekravet.²¹

Trapovas forståelse av kreativtetsbegrepet bidrar også til å underbygge dette. Ufullkommenheter, frustrasjon og emosjonell kompleksitet i en kreativ prosess kommer blant annet til uttrykk gjennom frustrasjonen ved skrivesperre, og motstandskraften involvert i å bearbeide tidlige utkast eller ideer²² – faktorer som medfører at det kan ta lang tid å skrive selv en kort e-post, og at den konkrete utformingen av en tekst kan avhenge av dagsform. Ved bruk av en språkmodell unnslipper brukeren å forholde seg til denne delen av skaperprosessen, og resultatet kan dermed heller ikke knyttes til brukerens emosjonelle kompleksitet eller personlighet.

Konklusjonen blir dermed at KI-genererte tekster ikke kan regnes som et åndsverk.

Kort om aktiv bearbeiding av KI-genererte tekster

Situasjonen vil være annerledes dersom brukeren av språkmodellen har en mer aktiv interaksjon med teksten. Ved å for eksempel endre deler av teksten med egne ord, omstrukturere innholdet, og/eller legge til nytt innhold, kan den endelige teksten potensielt uttrykke brukerens personlighet og frie, kreative valg.²³ Illustrativt åpner åndsverkloven § 6

21 Se en dypere analyse av årsakssammenhengen mellom ledetekster og KI-generert innhold i Ole-Andreas Rognstad, «Copyright Protection for Output Resulting from Use of Generative AI Systems – Some Reflections», NIR utgave 1 2025: <https://www.nir.no/en/journals/viewsection/26282>

22 Trapova, s. 2

23 Se illustrativt TONOs retningslinjer: <https://www.tono.no/faq-items/retningslinjer-for-forvaltning-og-registrering-av-ki-generert-musikk/>, og BONOs retningslinjer: <https://bono.no/hva-mener-bono-om-ki-kunst-og-opphavsrett/>

18 Ibid. Se konklusjonen på s. 21-22

19 Se Trapova s. 22 og Ginsburg s. 1063

20 Se f.eks. C-5/08 (Infopaq) hvor EU-domstolen kom til at en sammenstilling av 11 ord kunne ha opphavsrettsvern



(2) for at endringer av allerede eksisterende verk etter omstendighetene kan regnes som nye og selvstendige verk. Utgangspunktet vil imidlertid være at de delene av teksten som eventuelt ikke er bearbeidet, mangler opphavsrettsvern.²⁴ Ved lengre tekster vil det trolig kreves omfattende endringer for at hele teksten kan anses som resultat av brukerens åndsinnsett. Dette må imidlertid vurderes konkret i hvert enkelt tilfelle.

Praktisk betydning

Vurderingen ovenfor viser at innhold generert av generativ KI normalt ikke vil ha opphavsrettsvern. Konsekvensen er at kunstnere, bedrifter og andre som nyter godt av opphavsrettens eksklusivitet, ikke vil kunne regne slikt innhold som del av deres enerett med de økonomiske og ideelle fordelene dette innebærer. Konklusjonen kan bli annerledes dersom brukeren har en mer aktiv interaksjon med det som genereres.

For å sikre opphavsrettsvern for tekster og annet innhold skapt ved hjelp av KI, kan det være hensiktsmessig å starte med å utarbeide innholdet på egenhånd. Deretter kan KI brukes som et verktøy for å foreta forbedringer, utvikle ideer, o.l. Det kan i denne forbindelse trekkes en sammenheng til forskningen nevnt innledningsvis. Stu-

dien sammenlignet tre grupper som løste skriveoppgaver på ulike betingelser: én gruppe uten hjelpemidler, én med tilgang til søkemotorer, og én med tilgang til en språkmodell. Resultatene viste at gruppen som brukte språkmodeller hadde vesentlig redusert hjerneaktivitet, svakere eierskap til det som ble produsert, og dårligere evne til å gjengi informasjonen de hadde skrevet om.²⁵ Studien viste imidlertid også at deltakere som først løste oppgavene uten hjelpemidler, fikk betydelig større utbytte av språkmodeller når de fikk tilgang til dem etterpå.²⁶ Dette tyder på at tidspunktet for når KI introduseres i oppgaveløsning, kan ha vesentlig betydning for vår evne til å opprettholde grunnleggende hjernefunksjoner.

Studien underbygger at måten språkmodeller brukes på har betydning for graden av kreativitet i skapelsesprosessen, og at bruk av KI som hjelpemiddel *etter* innledende selvdrevet arbeid innebærer større grad av hjerneaktivisering. Med dette som bakteppe kan verkshøydekravet få en praktisk funksjon utover det rent juridiske: Uten en tolkning som vektlegger faktorer som kjennetegner menneskelig kreativitet, risikerer man å gi opphavsrettsvern til inn-

hold skapt på måter som svekker – snarere enn fremmer – kreativ kapasitet. Andre insentiver enn opphavsrettsvern vil åpenbart i større grad påvirke hvordan folk bruker KI-verktøy. Men nettopp fordi opphavsretten er ment å fremme menneskelig kreativ skaperkraft, bør verkshøydevurderingen konkretisere denne egenskapen – særlig i møte med teknologi som har potensiale til å svekke vår kollektive kreative kapasitet.

Konklusjon

Generativ KI utfordrer opphavsrettens grunnleggende premiss om at kreativt innhold springer ut av en menneskelig skapelsesprosess. Gjennomgangen ovenfor viser at tekstinnhold generert av språkmodeller normalt ikke vil oppfylle verkshøydekravet, da brukeren mangler kontroll over den konkrete utformingen av verket – en essensiell del av den kreative prosessen.

Verkshøydekravet retter seg mot skapelsesprosessen, ikke sluttresultatet. I møte med teknologi som kan overta betydelige deler av denne prosessen, blir det avgjørende å tolke kravet i lys av hva som kjennetegner menneskelig kreativitet: frie og personlig pregede valg, kontrollert utforming, og den emosjonelle kompleksiteten som følger med kreativ innsats. En slik tolkning av verkshøydekravet kan ha praktisk betydning. Forskning viser at ukritisk bruk av språkmodeller reduserer hjerneaktivitet, svekker eierskap og gir dårligere læringsutbytte. Ved å kreve aktiv menneskelig kreativitet for opphavsrettsvern, kan opphavsretten fungere som et insentiv til å bruke KI på måter som ivaretar – snarere enn truer – vår kollektive kreative kapasitet.

Veronika Lundqvist er advokatfullmektig i Deloitte Advokatfirma, tilhørende teamet Intangibles, Data and Technology. Har særskilt kunnskap om skjæringspunktet mellom opphavsrett og teknologi, og jobber nå hovedsakelig med problemstillinger knyttet til immaterialrett, teknologirett og personvern.

24 Bearbeiderens opphavsrett er begrenset til resultatet av hans skapende åndsinnsett, jf. HR-2017-2165-A (Tempo), avsnitt 75

25 Nataliya Kosmyna m.fl. (Cornell University), "Your Brain on ChatGPT: Accumulation of Cognitive Debt when Using an AI Assistant for Essay Writing Task": <https://arxiv.org/pdf/2506.08872> s. 2

26 Ibid., s. 139

The COMPAS case's impact on the EU's AI Act

Av Anna Stensrud

This article addresses key findings from my Master thesis, which examined how the controversy of the COMPAS recidivism algorithm in the US directly and indirectly shaped requirements for AI used by law enforcement and judiciary within the EU AI Act.¹

First, a brief explanation of the COMPAS revelation will be given. From now on it will be described as “the COMPAS case”, understood as a case not in the legal sense, but as a concrete case study. Furthermore, a short introduction to the AI Act (AIA) is presented. Due to space limitation, the paper will not dig into the academic debate sparked by the COMPAS case and the regulatory works leading up to the AIA, where the COMPAS case was referenced.² Instead, the direct impact of the COMPAS case found through references in the AIA's Impact Assessment part 1 and 2 is at the center of this article. After presenting the findings, the pros and cons of the transnational influence of regulatory approaches will be discussed. The aim of the article is to illustrate how a local challenge, rooted in a particular jurisdiction,



Anna Stensrud

informed regulatory efforts in an entirely different legal and cultural context – and to question the fruitfulness of this influence.

COMPAS – the not so trustworthy AI

The COMPAS algorithm, used in several US court systems, was shown in ProPublica's landmark 2016 study to disproportionately label Black defendants as high risk despite equivalent reoffending rates—a finding that sparked new global debates about algorithmic bias and trust in AI-driven judicial tools.³ The investigative research looked at over “10,000 criminal defendants in Broward County, Florida, and compared their predicted recidivism rates with the rate that actually occurred over a two-year period[...and] compared the recidivism risk categories predicted by the COMPAS tool to the actual

recidivism rates.”⁴ They found that Black defendants were disproportionately classified as high-risk for reoffending, while White defendants were more likely to be incorrectly categorized as low-risk.⁵ This bias was rooted in the algorithm's reliance on historical data that reflected systemic inequalities, perpetuating discrimination through automated decision-making processes.

The defendants had to answer a questionnaire asking about employment, education, family background, friends and crime in their neighborhood.⁶ These are variables which combined could lead to racial bias according to scholars.⁷ “A guy who has molested a small child every day for a year could still come out as a low risk because he probably has a job. [...] Meanwhile, a drunk guy will look high risk because he's homeless,” a Superior Court Judge commented about COMPAS.⁸ Additionally, the opaque nature of COMPAS' “black box” algorithm raised concerns about transparency and accountability, as neither defendants nor legal professionals could understand or challenge its outputs.⁹ This opacity undermines due process rights and

1 Stensrud (2025).

2 See Stensrud (2025) Chapter 4 and 5 for this research.

3 Angwin et al. (2016).

4 Larson et al. (2016).

5 Angwin et al. (2016) and Larson et al. (2016).

6 Angwin et al. (2016) and Northpointe (2011).

7 Baker (2025).

8 Angwin et al. (2016).

9 The term “black box” in the context of AI and machine learning refers to systems whose internal workings are opaque or not easily understandable, even to their creators.

the ability to challenge potentially erroneous or biased assessments.

The COMPAS case is a helpful case study in several ways. For one, it is a tool used by law enforcement and judges in the US. It revealed the challenges the use of AI imposes in in these fields. Secondly, there is evidence of the COMPAS case influencing specific parts of the AIA, as this article will go to show.

The AIA and the protection of fundamental rights

On the other side of the Atlantic Ocean, the work on trustworthy AI begun in the European Union (EU).¹⁰ In 2023 this would culminate into the pioneering AI-regulation the “Artificial Intelligence Act” (Regulation (EU) 2024/1689). The AIA is significant, because it tries to adapt to present and future society’s use of AI, based on challenges that have already occurred and predictions of what might come. The shift from ethical guidelines to binding regulations came when Ursula von der Leyen became president of the European Commission in 2019. Under her rule, the Commission highlighted the need for a unified EU legislation on AI to protect fundamental rights.¹¹ This marks an important shift within AI governance in the EU, from voluntary ethical guidelines to protecting fundamental rights, which are foundational to the EU through the European Convention on Human Rights (ECHR).¹² After debates among the EU leaders in October 2020, the Commission formally proposed the AIA on April 21st 2021, accompanied by an Impact Assessment, which is a central source for this article. After intense dialogue discussions in December 2023, a political agreement

was reached, and the Act was adopted by the European Parliament on March 13th 2024, approved by the Council on May 21st 2024, and entered into force on August 1st 2024.

The heart of the Act lies in Chapter III, which focuses on high-risk AI systems.¹³ Chapter III is subdivided into 5 sections that detail how high-risk systems are classified (Section 1), the strict requirements they must meet (Section 2), and the obligations placed on various actors in the AI value chain, such as providers, deployers, importers, and distributors (Section 3). It also establishes the roles of notifying authorities and notified bodies (Section 4) and standards, conformity assessments, certification, and registration processes (Section 5). This structure aims to ensure that the most potentially harmful AI applications are subject to robust *ex-ante* scrutiny before entering the market. Chapter III, Section 2 is central to this thesis’ analysis. Section 2 details the essential requirements that high-risk AI systems must meet before being placed on the market or put into service.¹⁴ These requirements include e.g. the need for a robust risk management system in Article 9, high standards for data quality and governance in Article 10, thorough technical documentation in Article 11, and effective record-keeping in Article 12. Additionally, providers must ensure transparency and provide adequate information to deployers after Article 13, implement human oversight measures as stated in Article 14, and guarantee accuracy, robustness, and cybersecurity according to Article 15. These obligations are designed to make sure that high-risk AI systems operate safely and reliably, with clear accountability throughout

their lifecycle. Article 10 and 14 are especially important to mitigating bias in AI systems like COMPAS and several studies have also connected the COMPAS case to these articles,¹⁵ an argument backed by the findings in this paper.

The findings in the Impact Assessment

The European Commission conducts impact assessments for its legislative and non-legislative initiatives that are expected to have significant economic, environmental, or social impacts – like the AIA.¹⁶ The Impact Assessment accompanying the AIA therefore gives us valuable insight “behind the scenes” of the Act. We find the COMPAS case listed in both the first and the second part of the Impact Assessment. Part 1 identifies bias and discrimination as significant risks posed by AI systems, stating that discriminatory AI systems used in judiciary or law enforcement may “lead to broader societal consequences, reinforcing existing or creating new forms of structural discrimination and exclusion”.¹⁷ Further on in part 1, the European Commission outlines a “baseline scenario” in chapter 5.1. Here they state that in the absence of the AIA the risks identified with e.g. discriminatory AI, would remain unaddressed”.¹⁸ The “baseline scenario” described in the Impact Assessment therefore reflects the policy landscape before the AIA; a patchwork of general product safety rules, sectoral laws, and voluntary guidelines, with no harmonized, risk-based EU framework for

10 2015/2103(INI) point 16.

11 European Commission (2020) “Whitepaper on AI” p. 2.

12 See AI HLEG (2019) “Ethics Guidelines for Trustworthy AI”.

13 AIA, Article 6-49.

14 AIA, Article 8-15.

15 Carnat (2024), Chroust (2025) and van Dijck (2022).

16 Robertson (2008) p. 17.

17 European Commission (2021) part 1/2 p. 14, 19-20.

18 European Commission (2021) part 1/2 p. 37-29.

AI.¹⁹ COMPAS is referenced in this part of the Impact Assessment, as one of four examples “where claims of discrimination have already led to pressure from public opinion.”²⁰ The COMPAS case is referenced together with these three cases: facial recognition discrimination, Amazon’s hiring model and the ‘sexist’ Apple card.²¹ All the examples listed had their origin in the US, which underscores the transnational influence of American cases of claimed discrimination.

The Impact Assessment cites the COMPAS case as an example of how algorithmic tools can perpetuate discrimination and undermine trust. It warns that, without EU-level action, member states would likely adopt divergent national rules in response to public outcry over AI harms, leading to market fragmentation and inconsistent protection of fundamental rights.²² The Act is designed to harmonize rules across the EU for high-risk AI systems, ensuring a consistent level of protection and legal certainty for both providers and users. This harmonization is a key departure from the baseline scenario, where such fragmentation is a likely outcome. The baseline scenario relies heavily on voluntary codes and ethical guidelines, such as those developed by the AI HLEG.²³ However, the Impact Assessment notes that these mechanisms lack enforceability and public oversight. In contrast, the AIA establishes binding obligations for high-risk AI systems, with oversight by national authorities and the

European Commission, thus moving beyond the limitations of soft law. Under the baseline, discriminatory issues would be addressed only indirectly, if at all, through general anti-discrimination law or sectoral regulation, not through targeted AI legislation. The Act, through Annex III number 6(d)-(e), directly addresses these concerns by classifying AI systems used for risk assessment and profiling in law enforcement as high-risk, thereby subjecting them to strict requirements for e.g. transparency in Article 13, human oversight in Article 14, and bias mitigation in Article 10.²⁴ This regulatory approach is arguably a direct response to the shortcomings exposed by cases like COMPAS, which the Impact Assessment highlights as a justification for moving beyond the baseline.

The Impact Assessment’s part 2 show that the high-risk categorization of the AIA was based on 132 use cases, stakeholder feedback and alignment with existing EU law such as the GDPR, product safety directives, and fundamental rights frameworks.²⁵ The COMPAS case heavily impacted one of the high-risk use cases studied by the Commission.²⁶ The Impact Assessment does not speak of specific articles or annexes of the AIA, as they were not yet settled upon in 2021. Annex III is therefore not explicitly mentioned by name in the Impact Assessment. However, Section 5.4 in the second part of the Impact Assessment cover high-risk AI systems that are not covered by sectoral product safety legislation, and have mainly implications with fundamen-

tal rights.²⁷ The high-risk AI systems considered in 5.4 are what came to be listed in Annex III; 1) biometrics, 2) critical infrastructure, 3) education and vocational training, 4) employment, 5) access to essential services, 6) law enforcement, 7) migration and 8) administration of justice and democratic processes.²⁸ It is in the Impact Assessment part 2’s Annex 5 section 5.4, we find the COMPAS case connected to one of the use cases.²⁹ The COMPAS case is listed as one of the five evidence sources under “AI systems used to assist judicial decisions, unless for ancillary tasks.”³⁰ However, the impact of the COMPAS case is also evident in three of the four other sources listed. One of them being the CoE Charter written by the CEPEJ.³¹ Another source is the Supreme Court case *State v. Loomis*, where the COMPAS case’s findings was a matter of debate.³² Two specific pages of a fourth source named “Algorithms and human rights” published by the CoE in 2017 is also listed. Within these two pages the COMPAS case is again used as an example of judicial bias.³³ In fact, there is only one out of five sources listed which the COMPAS case is not a part of.³⁴ The potential harms listed under

19 For example the Machinery Directive, General Product Safety Directive, the forthcoming Digital Services Act, voluntary industry codes, and soft law.
20 European Commission (2021) part 1/2 p. 38.
21 European Commission (2021) part 1/2 p. 38.
22 European Commission (2021) part 1/2 p. 38.
23 AI HLEG (2019).

24 AIA, Article 8-15.
25 European Commission (2021) part 2/2 Annex 2, 4 and 5. A use case is an example of how an AI system is used to do a specific job or help with a certain task, for example AI systems used for recruitment or to assist judicial decisions.
26 European Commission (2021) part 2/2 p. 46.

27 European Commission (2021) part 2/2 p. 40.
28 European Commission (2021) part 2/2 p. 41-46 and AIA, Annex III number 1-8.
29 European Commission (2021) part 2/2 p. 46.
30 European Commission (2021) part 2/2 p. 46.
31 CEPEJ (2018).
32 *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S. Ct. 2290 (2017). See paragraph 63 for one of several references to the COMPAS case.
33 European Commission (2021) part 2/2 p. 46 and CoE (2017) p. 12.
34 The reference is to a decision of the French Conseil Constitutionnel of June 12th 2018, Decision no 2018-765 DC.

“AI systems used to assist judicial decisions, unless for ancillary tasks” are “[i]ntense interference with a broad range of fundamental rights (e.g. effective remedy and fair trial, non-discrimination, right to defence, presumption of innocence, right to liberty and security, human dignity as well as all rights granted by Union law that require effective judicial protection)” and “systemic risk to rule of law and freedom”.³⁵ Five “especially relevant indicative criteria” are also listed;

- Increased possibilities for use by judicial authorities in the EU
- Potentially very severe impact and harm for all rights dependent on effective judicial protection
- High potential to scale and adversely impact a plurality of persons or groups (due to large number of affected individuals)
- High degree of dependency (due to inability to opt out) and high degree of vulnerability vis-à-vis judicial authorities)
- Indication of harm (high probability of historical biases in past data used as training data, opacity).³⁶

The COMPAS case’s influence here is evident, directly and indirectly through three of the four other sources. Not only did the COMPAS case reveal the severe personal consequences of algorithmic bias, increasing systemic bias and racism. It also highlighted how AI could weaken the trustworthiness of the justice system, with the lack of competent human oversight and overreliance on AI tools in decision-making. The potential harms and especially relevant indicative criteria show that the Commission has taken the lessons learned from

the COMPAS case very seriously, which is also reflected in specific articles of the AIA’s Chapter III, Section 2. The Commission also states that “AI systems used for judicial decision-making, in the law enforcement sector and in the area of asylum and migration should comply with standards relating to increased transparency, traceability and human oversight which will help to protect the right to fair trial, the right to defense and the presumption of innocence.”³⁷ This links what came to be Annex III number 6 of the AIA, to requirements of transparency in Article 13, traceability in Article 12 and human oversight in Article 14.

Transnational Influence – a blessing or a curse?

Although the COMPAS case’s impact on Annex III number 6(d) is evident, the Act’s structure and content are shaped primarily by the EU’s internal policy process, legal precedents, and stakeholder consultations, with the COMPAS case serving as an illustrative example rather than a foundational influence. The COMPAS case is deeply embedded in the context of the US criminal justice system, which differs significantly from European systems in terms of legal standards, data practices, and the role of risk assessment tools. While the study is often cited as a cautionary tale, its specific findings may not be directly transferable to the European context. The EU’s high-risk classification for AI in law enforcement and justice is based on broader concerns about power imbalances and fundamental rights, not solely or primarily on cases like COMPAS. Nevertheless, the sum of cases like the COMPAS case, together pave the way for new policies. The ProPublica publication is one of many inter-

national examples considered in the global debate on algorithmic bias, informing one of 132 use cases. The AIA’s provisions on bias, transparency, and human oversight reflect a synthesis of many sources, with no single study or case alone, being decisive, but several being influential. The references to COMPAS in consultations and assessments are part of a broader pattern of drawing on international experiences to inform, but not dictate, the EU policy.³⁸

” By framing regulation around a case like COMPAS, policy-makers might overlook EU-specific risks, while over-regulating areas where existing safeguards already mitigate harm.

Scholars note that the EU’s approach to AI regulation is intentionally distinct from US models, thus aiming for a “Brussels Effect” where the EU sets global standards through its own regulatory philosophy.³⁹ In this way, the transnational influence might go “full circle” - from the EU being influenced by AI bias in the US, to impacting companies through the AIA. Europe has been the most important market for many US tech-companies such as Google.⁴⁰ This means that American AI giants and SMEs also must adapt to European regulations to take part in the lucrative market, possibly changing the overall procedures of AI developers.

Given the stark differences in legal, cultural, and institutional con-

35 European Commission (2021) part 2/2 p. 46.

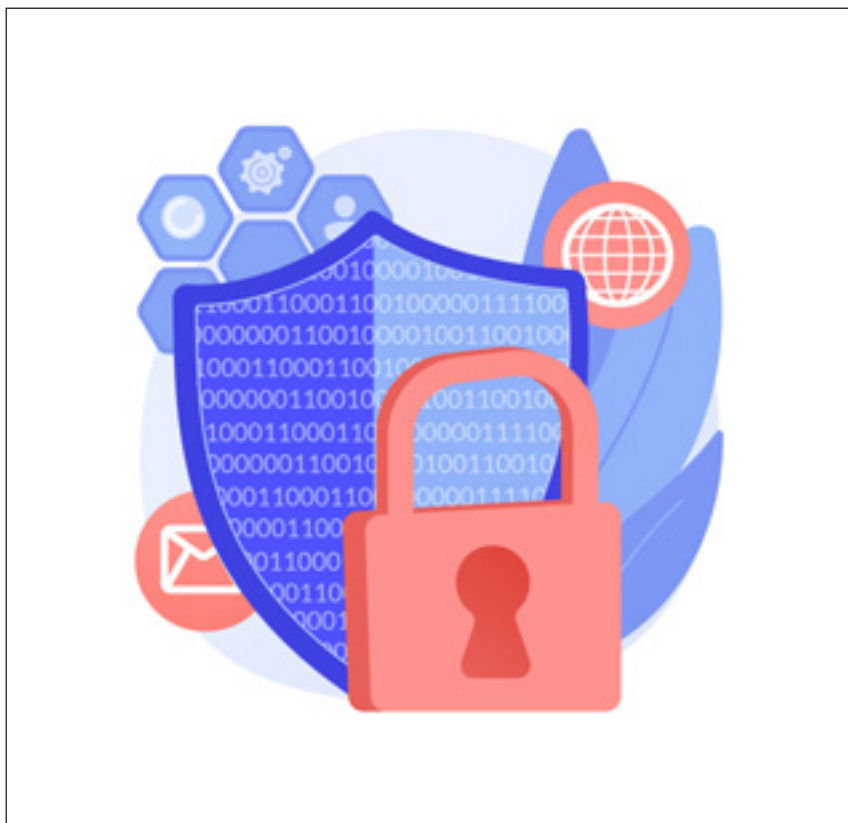
36 European Commission (2021) part 2/2 p. 46.

37 European Commission (2021) part 2/2 p. 48 and ECHR, Article 47 and 48.

38 AI HLEG (2018).

39 Ceimia (2023) p. 2-4 and 11.

40 Bradford (2020) p. 27.



Illustrasjon: Colourbox.com

texts between the US and Europe the COMPAS case might not be transferable to the European context. The use of risk assessment tools in Europe are not widespread either, but the Impact Assessment's part 2 lists the "increased possibilities for use by judicial authorities in the EU."⁴¹ There is for example a Harm Assessment Risk Tool (HART) in use in the UK already.⁴² The AI tool was developed for helping police make custodial decisions, but the researchers are clear; it is for guidance only, and it needs to be fed updated data and be under constant scrutiny.⁴³ The EU countries Germany and the Netherlands prioritize rehabilitation over risk prediction, often integrated into broader social service frameworks.⁴⁴

In the US, COMPAS operates within a legal framework with weak data protection laws, limited transparency requirements for proprietary algorithms, and judicial practices that more often defer to algorithmic outputs, as seen in cases like *State v. Loomis*. By contrast, the EU's regulatory landscape, anchored in the GDPR Article 22's restrictions on automated decision-making and the AIA's prohibition in Article 5(1)(d) and high-risk regulation in Annex III number 6(d), reflects a fundamentally different approach.⁴⁵ The EU prioritizes ex-ante safeguards, human oversight, and procedural fairness, reducing the likelihood of a European COMPAS controversy. For example, AI systems in EU law enforcement must now undergo

conformity assessments, provide technical documentation, and ensure human intervention, all of which address COMPAS' core flaws; opacity, bias, and flawed oversight.⁴⁶ Nevertheless, relying on COMPAS as a justification for EU regulation on recidivism tools used in law enforcement, risks over-emphasizing a foreign example and interpreting evidence to fit preexisting concerns. By framing regulation around a case like COMPAS, policy-makers might overlook EU-specific risks, while overregulating areas where existing safeguards already mitigate harm.

Anna Stensrud er nyutdannet jurist, med en tverrfaglig studiebakgrunn fra internasjonale studier og historie. De siste årene har jeg jobbet som journalist, og nå har jeg inntatt rollen som personvernserådgiver i DSS.

Table of reference

Laws and regulations:

ECHR *Convention for the Protection of Human Rights and Fundamental Freedoms*, Rome 4 November 1950.

Legislative initiative procedure 2015/2103(INL) European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics [Civil Law Rules on Robotics].

Regulation (EU) 2024/1698 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence [Artificial Intelligence Act].

Regulation (EU) 2016/679 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and

41 European Commission (2021) part 2/2 p. 46.

42 Barnes et al. (2018) p. 33.

43 Barnes et al. (2018) p. 33.

44 Subramanian and Shames (2013) p. 7-14.

45 AIA, Article 5(1)(d) prohibits AI systems that assess criminal risk based solely on profiling or personality traits, with exceptions only if used to support human judgment.

46 AIA, Article 43, 11 and 14.

repealing Directive 95/46/EC (General Data Protection Regulation) [General Data Protection Regulation].

Court cases:

Judgement of Wisconsin Supreme Court of 13 July 2016, State v. Loomis, 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S. Ct. 2290 (2017).

Judgement of French Conseil Constitutionnel of 12 June 2018, Decision no. 2018-765 DC.

Reports and documents:

AI HLEG. Draft Ethics guidelines for trustworthy AI. Brussels: 2018. Available for download through: <https://digital-strategy.ec.europa.eu/en/library/draft-ethics-guidelines-trustworthy-ai>

AI HLEG. Ethics guidelines for trustworthy AI. Brussels: 2019. Available for download through: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

CEPEJ. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. Strasbourg: CoE, 2018. <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>

Ceimia. A Comparative Framework for AI Regulatory Policy. Montréal: 2023. <https://ceimia.org/wp-content/uploads/2023/05/a-comparative-framework-for-ai-regulatory-policy.pdf>

European Commission. *White Paper on Artificial Intelligence - A European approach to excellence and trust*. COM(2020) 65 final. Brussels: 2020. https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

European Commission. *Commission Staff Working Document Impact Assessment*. SWD(2021) 84 final (part 1/2). Brussels: 2021. https://eur-lex.europa.eu/resource.html?uri=cellar:0694be88-a373-11eb-9585-01aa75e-d71a1.0001.02/DOC_1&format=PDF

European Commission. *Commission Staff Working Document Impact Assessment Annexes*. SWD(2021) 84 final (part 2/2). Brussels: 2021. https://eur-lex.europa.eu/resource.html?uri=cellar:0694be88-a373-11eb-9585-01aa75e-d71a1.0001.02/DOC_2&format=PDF

Northpointe. Risk Assessment. 2011. <https://embed.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE/>

Subramanian, Ram and Alison Shames. Sentencing and Prison Practices in Germany and the Netherlands: Implications for the United States. New York: VERA Institute of Justice, 2013. <https://www.prison-policy.org/scans/vera/european-american-prison-report-v3.pdf>

Literature:

Angwin, Julia, Jeff Larson, Surya Mattu and Lauren Kirchner. "Machine bias." ProPublica, May 23rd 2016. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

Baker, Steven. "Ensuring Procedural Fairness in AI-Driven Criminal Sentencing: A Focus on Transparency and The Right to Explanation." NHSJCS, 2025. <https://nhsjcs.com/2025/02/27/ensuring-procedural-fairness-in-ai-driven-criminal-sentencing-a-focus-on-transparency-and-the-right-to-explanation/>

Barnes, Geoffrey, Lawrence Sherman and Sheena Urwin. "Needles and haystacks: AI in criminology." Research Horizons no. 35 (2018) p. 32-33. https://www.cam.ac.uk/system/files/issue_35_research_horizons_new.pdf

Boskovic, Marina M. Matic. "IMPLICATIONS OF EU AI REGULATION FOR CRIMINAL JUSTICE." Regional Law Review (2024) p. 111-120. DOI:10.56461/iup_rlrc.2024.5.ch8

Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press, 2020.

Carnat, Irina. "Addressing the risks of generative AI for the judiciary: The accountability framework(s) under the EU AI Act." Computer Law & Security Review vol. 55 (2024) 106067.

Chroust, Tomas. "The AI Act requires human oversight." Bearingpoint, 2025. <https://www.bearingpoint.com/en/insights-events/insights/the-ai-act-requires-human-oversight/>

Larson, Jeff, Surya Mattu, Lauren Kirchner and Julia Angwin. "How We Analyzed the COMPAS Recidivism Algorithm." ProPublica, May 23rd 2016. <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>

Robertson, Craig. "Impact Assessment in the European Union." EI-PASCOPE vol 2 (2008) p. 17-20.

Stensrud, Anna. Bias Beyond Borders: Decoding Transnational Influence in the EU's AI Act - An analysis of how US experiences informed the AI Act, and how it regulates recidivism tools like COMPAS [Master thesis]. Oslo: University of Oslo, 2025.

The Decision Lab. "Why do we think some things are related when they aren't?" N.d. <https://thedecisionlab.com/biases/illusory-correlation> Last used May 22nd 2025.

Van Dijck, G. "Predicting Recidivism Risk Meets AI Act." European Journal on Criminal Policy and Research vol. 28, no. 3 (2022) p. 407-423. <https://doi.org/10.1007/s10610-022-09516-8>

Whitehead, Orlando. "€250 on the spot fines for bicycle thieves." The Brussels Times, December 27th 2021. <https://www.brusselstimes.com/199457/e250-on-the-spot-fines-for-bicycle-thieves>

Bedre (over)føre var? Latombe-sakens betydning for EU-US Data Privacy Framework

Av Ole Martin Moe og Trine Smedbold

Den 3. september 2025 avsa Underretten i EU-domstolen (General Court) dom i saken **T-553/23, Latombe v. Commission**. Dommen bekrefter gyldigheten av EU-kommisjonens beslutning om at USA tilbyr et adekvat beskyttelsesnivå for personopplysninger som overføres fra EØS til USA under EU-USA Data Privacy Framework.

Dette innebærer at adekvansbeslutningen har bestått den første prøvingen i rettsapparatet, og at virksomheter fortsatt kan benytte den som grunnlag for overføring av personopplysninger til USA. Hva handlet dommen om, hva blir veien videre, og hvordan kan man være (over)føre var?

1. Bakgrunn

Saken ble reist av Philippe Latombe, en fransk parlamentariker, som



Ole Martin Moe

utfordret EU-kommisjonens gjennomføringsbeslutning (EU) 2023/1795. Adekvansbeslutningen slo fast at USA gir et tilstrekkelig beskyttelsesnivå for personopplysninger som overføres under EU-USA Data Privacy Framework.

Latombe viste til tidligere avgjørelser fra EU-domstolen, som Schrems I og Schrems II, hvor de lignende adekvansbeslutningene Safe Harbor og Privacy Shield ble kjent ugyldige. Latombe hevdet blant annet at The Data Protection Review Court ("DPRC"), en sentral del av klagemekanismen som tilbys EØS-borgere i forbindelse med amerikanske etterretningsaktiviteter under EU-USA Data Privacy Framework, ikke kan anses som uavhengig.

Videre argumenterte han for at fraværet av forhåndsgodkjenning fra en domstol eller en uavhengig administrativ myndighet for amerikanske etterretningsaktiviteter knyttet til masseinnsamling av personopplysninger, ikke er forenlig med kravene for adekvansstatus.



Trine Smedbold

Før vedtakelsen av adekvansbeslutningen ga EDPB sin Opinion 5/2023. Der anerkjente de det nye rammeverkets forbedringer sammenlignet med Privacy Shield, men pekte samtidig på gjenstående bekymringer – særlig knyttet til myndigheters tilgang til personopplysninger og effektiviteten av rettsmidler. Dette bakteppet illustrerer hvorfor Latombe-saken ble fulgt med så stor interesse.

2. Hovedpunkter fra dommen

I dommen avviser Underretten påstanden om at DPRC mangler uavhengighet. Retten viser til flere forhold som understøtter DPRCs uavhengige status: dommere utnevnes under omfattende garantier, kan kun avsettes av USAs justisminister på saklig grunnlag, og hverken justisministeren eller etterretningsorganisasjoner kan hindre eller påvirke DPRCs arbeid på en upassende måte. Videre understreker retten at EU-kommisjonen plikter å overvåke det amerikanske rettslige rammever-

ket og iverksette tiltak dersom det er nødvendig, for eksempel ved å suspendere adekvansbeslutningen.

Det er her viktig å notere seg at Underretten tar utgangspunkt i de faktiske forholdene og gjeldende lovgivning på tidspunktet da EU-kommisjonens adekvansbeslutning ble vedtatt sommeren 2023. Mye har skjedd i USA siden den gang, og særlig under Trump-administrasjonen fra januar 2025 og frem til i dag. Administrasjonen har blant annet avskjediget medlemmer av Privacy and Civil Liberties Oversight Board (PCLOB) og har ikke erstattet disse.

Pro et contra:

- *Pro (Underretten)*: institusjonelle og prosessuelle garantier sikrer DPRCs uavhengighet og upartiskhet.
- *Contra (NOYB m.fl.)*: DPRCs rammer skriver seg primært fra Executive Order 14086 og forskrift, ikke føderal lovgivning, og kan derfor være mer sårbare for politiske endringer.

Når det gjelder masseinnsamling av personopplysninger for etterrettingsformål, konkluderer Underretten med at Schrems II-dommen ikke stiller krav om forhåndsgodkjenning av slike aktiviteter. Retten aksepterer et system med etterfølgende kontroll (ex post) gjennom DPRC, og vurderer at dette sikrer at USA tilbyr et beskyttelsesnivå som er vesentlig likt som i EØS.

3. Rettslig ramme og prøvingsintensitet

Retten anvender «essentially equivalent»-standarden fra Schrems II-avgjørelsen, og vurderer om den samlede beskyttelsen under amerikansk rett – sett i lys av adekvansbeslutningen – er vesentlig lik den i EØS. Innenfor rammen av personvernforordningen artikkel 45 anerkjenner retten EU-kommisjonens skjønnsmargin, men kontrollerer samtidig at de rettslige garantiene faktisk foreligger og fungerer. Retten

legger særlig vekt på DPRC som ex post-mekanisme, fremfor krav om generell forhåndsgodkjenning.

4. Kunne Latombe i de hele tatt reise søksmål?

Et av spørsmålene mange lurte på i forkant var om Latombe ville oppfylle kravet til rettslig interesse for EU-domstolen. Domstolen valgte overraskende å ikke behandle dette spørsmålet. I stedet uttalte den at et søksmål om annullering kan avvises basert på sakens materielle innhold uten først å ta stilling til spørsmålet om saken kan tas til behandling, dersom dette er begrunnet ut fra hensynet til en forsvarlig rettspleie.

Hvordan retten valgte å behandle saken prosessuelt har vært gjenstand for debatt i etterkant av dommen. Flere kommentatorer, deriblant Max Schrems, har påpekt at domstolen gikk rett til en vurdering av de materielle spørsmålene uten å avklare om Latombe i det hele tatt hadde prosessuell partsevne. Det er i seg selv uvanlig, men domstolen begrunnet som sagt dette med hensynet til en forsvarlig rettspleie. Dette kan bli vurdert annerledes i ankesaken.

Det er også verdt å merke seg at EU-domstolen er bundet av det faktum partene legger frem. Retten foretar ingen selvstendig faktaundersøkelse, noe som innebærer at kvaliteten på de fremlagte faktiske opplysningene kan bli avgjørende for dommens konklusjoner. I Latombe-saken ble det ikke lagt frem like omfattende og systematiske bevis som man har sett i andre personvernprosesser – for eksempel i saker anlagt av NOYB. Dersom saksgrunnlaget hadde vært bedre dokumentert, kunne rettens vurderinger ha sett annerledes ut.

Dette illustrerer at selv om Latombe-dommen opprettholder EU-USA Data Privacy Framework, innebærer den ikke nødvendigvis en endelig avklaring. Hvor robust rammeverket faktisk er, vil kunne settes på en mer krevende prøve dersom mer fak-

tatunge og grundig prosederte saker bringes inn for domstolen i fremtiden.

5. Konsekvenser for norske og europeiske virksomheter

Underretten avviste dermed Latombes søksmål om annullering av EU-USA Data Privacy Framework og bekreftet rammeverkets gyldighet – for nå. Avgjørelsen gjør at europeiske virksomheter enn så lenge kan puste lettet ut og fortsette overføring av personopplysninger til USA under adekvansbeslutningen. Samtidig er debatten om transatlantiske overføringer langt fra over, og avgjørelsen gir kun midlertidig juridisk sikkerhet.

Latombe har nå anket til Domstolen (EU-domstolens høyere instans), og anken kan innebære at både prosess- og realitetsspørsmål blir behandlet på nytt.

Etter dommen har Datatilsynet også uttalt at deres anbefaling om å være forberedt og ha en strategi for alternative løsninger fortsatt står ved lag.

6. Praktiske råd for virksomheter

- Bruk DPF der mottaker i USA er sertifisert.
- For andre overføringer: benytt SCC-er eller BCR kombinert med en Transfer Impact Assessment (TIA).
- Oppretthold tekniske tiltak: pseudonymisering, ende-til-ende-kryptering, kunde-heldte nøkler, minimér data og loggtilgang.
- Etabler en «Plan B» for rask omlegging ved en eventuell rettslig utvikling som underkjenner rammeverket.

For norske virksomheter betyr dette at man bør se Latombe-dommen som en midlertidig stabilisering, men ikke et punktum for debatten. Strategisk planlegging og tekniske sikkerhetstiltak er fortsatt nødvendig.

Ole Martin Moe og Trine Smedbold er begge advokatfullmektiger i Advokatfirmaet Bull.

Datadelingsloven og veien mot et åpnere Norge

Av Hanne Pernille Gulbrandsen, Anniken Meuche Henriksen og Veronika Lundquist



Hanne Pernille Gulbrandsen



Anniken Meuche Henriksen



Veronika Lundquist

1. Innledning

Data har i lang tid blitt omtalt som den nye oljen – en ressurs med enormt potensial for verdiskaping, innovasjon og samfunnsutvikling. Men i motsetning til olje blir data mer verdifull når den deles, ikke når den holdes tilbake. Tilgang til offentlige data er en forutsetning for et åpent og demokratisk samfunn, og for at vi skal kunne utvikle nye tjenester og løsninger. Det er nettopp dette EUs «åpne data-direktiv»¹ skal sikre.

Digitaliserings- og forvaltningsdepartementet jobber nå med å gjennomføre åpne data-direktivet i norsk rett. I 2024 la et offentlig utvalg frem NOU 2024: 14 «Med lov skal data deles», med forslag til ny lov om datadeling (heretter datadelingsloven). Forslaget ble sendt på høring samme år. I september 2025 oppnevnte regjeringen Dataprioriteringsrådet for å kartlegge hvilke offentlige data som har størst samfunnsverdi og gi anbefalinger om prioriteringer.² Norge står med andre ord foran et nytt kapittel for deling av offentlige data.

Vi vil nedenfor gjennomgå noen av de viktigste endringene i forslaget til ny datadelingslov.

” Selv om det allerede finnes bestemmelser om deling av data i norsk rett, vil datadelingsloven medføre at offentlig sektor påføres nye lovkrav sammenlignet med tidligere.

2. Lovkrav om datadeling for offentlige virksomheter

Norge har allerede en relativt liberal tilnærming til offentlig datatilgang

sammenlignet med mange andre land, med en sterk tradisjon for åpenhet og innsyn i offentlig sektor. Det rettslige rammeverket følger i hovedsak av offentleglova (offl.) og digitaliseringsrundskrivet. Samlet inneholder de lovkrav og anbefalinger blant annet knyttet til å tilgjengeliggjøre data i standardiserte formater, publisere metadata i nasjonal datakatalog, og i mange tilfeller gjøre data gratis tilgjengelige.

Selv om det allerede finnes bestemmelser om deling av data i norsk rett, vil datadelingsloven medføre at offentlig sektor påføres nye lovkrav sammenlignet med tidligere. Delvis fordi loven innfører nye krav sammenliknet med gjeldende rett, men også fordi reglene vil gjelde for flere aktører. Offentleglovas viderebruksbestemmelser og digitaliseringsrundskrivet omfatter i hovedsak offentlige organer.³ Forslaget til datadelingsloven omfatter *alle* offentlige virksom-

1 Direktiv 2019/1024 («Open Data Directive»)

2 Se <https://www.regjeringen.no/no/aktuelt/regjeringen-legger-til-rette-for-a-dele-mer-data-raskere-oppnevner-dataprioriteringsradet/id3117929/>

3 Offl. § 2 og rundskriv D-2/25

heter, inkludert offentlige foretak som kontrolleres av stat, kommune eller fylkeskommune gjennom eierskap, stemmerett, styre eller lignende.⁴ Flere offentlige foretak enn tidligere vil dermed bli underlagt krav om deling av data.

3. Tekniske krav for økt standardisering

Blant de mest praktiske endringene i datadelingsloven, er innføringen av konkrete tekniske krav til hvordan data skal tilgjengeliggjøres. Mens offentleglova i stor grad har overlatt detaljer til rundskriv, lovfester datadelingsloven krav om maskinlesbare formater, standardiserte metadata og digital tilgjengeliggjøring.⁵

For dynamiske data – informasjon som endrer seg kontinuerlig, som trafikkstrømmer, værdata eller miljømålinger – innføres et krav om sanntidstilgjengeliggjøring.⁶ Når slike data skal gjøres tilgjengelige, skal det skje umiddelbart etter innsamling, fortløpende via API-er eller gjennom massenedlasting.⁷ Dette er en forutsetning for at dataene skal ha reell verdi. Eldre trafikkdata hjelper lite for den som skal planlegge dagens rute, og forrige ukes værdata er ubrukelige for landbruket som skal bestemme når de skal så.

Kravet om API-er og standardiserte formater driver også frem en nødvendig harmonisering. I dag varierer det hvordan ulike offentlige virksomheter tilgjengeliggjør data.⁸ Noen bruker moderne API-er, andre tilbyr kun PDF-filer eller papirkopier.⁹ Denne fragmenteringen gjør det kostbart og tidkrevende å bygge tjenester som kombinerer data fra flere kilder. Når alle må følge samme standard, blir det i økt grad mulig å skape helhetlige løs-

ninger som integrerer informasjon fra ulike offentlige virksomheter.

Alle offentlige virksomheter pålegges også å publisere data og metadata i nasjonal datakatalog.¹⁰ Dette er en lovfesting og utvidelse av dagens krav i digitaliseringsrundskrivet, som kun gjaldt for utvalgte statlige virksomheter. Konsekvensen er at Norges offisielle portal for deling av data på data.norge.no, vil bli mer utfyllende enn den er i dag.

4. Fra innsyn til aktiv deling

Offentleglova bygger på et grunnleggende prinsipp om innsyn på forespørsel. Borgere og bedrifter har rett til å be om tilgang til offentlige dokumenter, men ansvaret for å initiere denne prosessen ligger hos den som ønsker innsyn. Datadelingsloven snur denne logikken for visse typer data. Offentlige virksomheter pålegges nå en plikt til aktivt å gjøre datasett med høy verdi tilgjengelige, uten at noen har bedt om innsyn.¹¹

Datasett med høy verdi omfatter informasjon som anses å ha særlig stor samfunnsnytte, fordelt på seks tematiske områder: geografiske data, jordobservasjonsdata og miljødata, meteorologiske data, statistikk, selskapsregister og eierskapsregister, samt mobilitetsdata.¹² Disse datasettene skal ikke bare gjøres tilgjengelige, men aktivt publiseres i maskinlesbare formater via API-er og massenedlasting, og de skal være gratis.¹³ Når viktige data aktivt gjøres tilgjengelige i standardiserte, maskinlesbare formater, senkes terskelen for viderebruk og nytteverdien av dataene øker.

5. Gratis data som hovedregel

Prinsippet om at offentlig informasjon skal være gratis er en sentral forutsetning for viderebruk av data. Utgangspunktet er i dag at offent-

lige organer ikke skal ta betalt for informasjonsutlevering, med mindre det foreligger særskilt hjemmel.¹⁴ Datadelingsloven viderefører dette prinsippet, men med visse endringer som styrker prinsippet.

Én endring er at forskningsdata alltid skal være gratis.¹⁵ Videre er det et nytt krav etter åpne data-direktivet at datasett med høy verdi som hovedregel skal være gratis.¹⁶ Unntak fra dette gjelder for biblioteker, museer og arkiver, og for offentlige foretak dersom dette vil føre til konkurransevridning på de aktuelle markedene og offentlige organ generelt i en overgangsperiode på inntil to år dersom dette vil ha en vesentlig innvirkning på budsjettene til de aktuelle organene.¹⁷

Et eventuelt gebyr skal ikke overstige marginalkostnadene knyttet til tilgjengeliggjøringen, med mindre det er snakk om ABM-sektoren sektoren og offentlige virksomheter med inntjeningskrav.¹⁸ En endring fra tidligere er at marginalkostbegrepet etter åpne data-direktivet kun omfatter kostnader knyttet til selve tilgjengeliggjøringen – ikke innsamling og produksjon.

I praksis innebærer dette en endring for særlig geodata og eiendomsdata. I dag kan offentlige virksomheter kreve full kostnadsdekning for slike data basert på en særregel i offentlegforskrifta § 4 (5). Denne muligheten fjernes. Geodata og eiendomsdata vil i stor grad regnes som datasett med høy verdi, og må derfor tilbys gratis. For virksomheter som Kartverket og kommunale kartmyndigheter som har bygget opp inntekter fra salg av kartdata, representerer dette en endring av deres finansieringsmodell.

4 Forslagets § 2

5 Ibid. § 5 (1) og (2)

6 Ibid. § 7

7 Utvalget sier dette i praksis må skje via API-er

8 NOU 2024: 14 s. 33

9 Ibid. s. 129

10 Forslagets § 6

11 Ibid. § 13

12 Åpne data-direktivet ANNEX 1

13 Ibid. art. 14 (1)

14 Offl. § 8

15 Forslagets § 8

16 Utvalget foreslår dette lovfestet i forskrift

17 Åpne data-direktivet art. 14 (1)

18 Forslagets § 10 (3)



Illustrasjon: Colourbox.com

6. Åpenhet om betaling og forbud mot enerettsavtaler

Datadelingsloven innfører også nye krav til åpenhet om betaling. Virksomheter som krever betaling for informasjon, må offentliggjøre vilkår og betalingssum på forhånd.¹⁹ Dette er en videreføring av gjeldende rett, men med et nytt element: medlemsstatene skal publisere en liste på internett over alle offentlige virksomheter som krever betaling utover rene tilgjengeliggjøringskostnader.²⁰ Dette skaper transparens og gjør det enkelt å identifisere hvilke data som er gratis og ikke.

” Datadelingsloven handler derfor ikke bare om å oppfylle et EU-direktiv, men om å realisere potensialet og utnytte ressursene som ligger i informasjon.

Forbudet mot enerettsavtaler strammes også inn. Allerede i dag er det forbudt for offentlige organer å inngå avtaler som gir noen enerett til å bruke offentlig informasjon, med mindre visse vilkår er oppfylt.²¹ Datadelingsloven utvider dette forbudet til også å gjelde offentlige foretak.²² For enerettsavtaler omfattet av unntaket, oppstilles det et nytt krav om at disse må offentliggjøres på internett to måneder før ikrafttredelse.²³ Dette er et viktig vern mot at offentlige data låses inne i kommersielle avtaler som hindrer konkurranse og innovasjon.²⁴

7. Avslutning

Den nye datadelingsloven vil kreve en viss omstilling, særlig hos kommuner og offentlige foretak. Blant høringsinstansene ble det ytret bekymring for eventuelle økte kostnader knyttet til teknisk tilrettelegging og tap av inntekter fra data-salg.²⁵ Samtidig representerer loven

et viktig skritt mot et mer åpent og innovativt Norge. Ved å lovfeste krav om aktiv datadeling, standardiserte formater og gratis tilgang til verdifulle datasett, legges det er godt grunnlag for nye tjenester, bedre beslutningsgrunnlag og økt samfunnsnytte. Datadelingsloven handler derfor ikke bare om å oppfylle et EU-direktiv, men om å realisere potensialet og utnytte ressursene som ligger i informasjon.

Hanne Pernille Gulbrandsen, partner og advokat i Deloitte Advokatfirma AS.

Anniken er advokat og manager i Deloitte Advokatfirma. Hun tilhører teamet Intangibles, Data and Technology og jobber hovedsakelig med problemstillinger knyttet til personvern og teknologirett.

Veronika Lundqvist er advokatfullmektig i Deloitte Advokatfirma, tilhørende teamet Intangibles, Data and Technology. Har særskilt kunnskap om skjæringspunktet mellom opphavsrett og teknologi, og jobber nå hovedsakelig med problemstillinger knyttet til immaterialrett, teknologirett og personvern.

¹⁹ Se offl. § 8 (5) sml. forslaget § 11

²⁰ Åpne data-direktivet art. 6 (3)

²¹ Offl. § 6 (1) og (2)

²² Forslagets § 12 (1)

²³ Ibid. § 12 (2)

²⁴ NOU 2024: 14 s. 56

²⁵ Ibid. s. 250-251

Nye retningslinjer for melding til Datatilsynet ved brudd på personopplysningssikkerheten

Av Rune Opdahl og Håvard Sveier Ottemo

1. Innledning

Datatilsynet mottar stadig flere meldinger om brudd på personopplysningssikkerheten – fra 2225 i 2021 til 3191 i 2024. Økningen skyldes ikke nødvendigvis flere brudd, men like gjerne lavere terskel og større bevissthet. Om lag 80 % av meldingene avsluttes uten videre oppfølging, noe som kan indikere at flertallet av innmeldte brudd er forbundet med liten risiko.

Mengden av meldinger kan være en byrde for Datatilsynet. Dette kan være en av årsakene til at Datatilsynet nylig har revidert sin veileder om «Hvilke brudd skal meldes til Datatilsynet?». I denne artikkelen kommenterer vi den reviderte veilederen.

2. Meldeplikten

Etter GDPR artikkel 33 skal den behandlingsansvarlige melde brudd på personopplysningssikkerheten til Datatilsynet, med mindre det er usannsynlig at bruddet vil medføre risiko for fysiske personers rettigheter og friheter. Altså er vurderingen to-delt: Først må det tas stilling til om det foreligger et brudd på personopplysningssikkerheten; dernest må det tas stilling til risiko ved sikkerhetsbruddet.

Manglende oppfyllelse av bestemmelsen kan medføre overtredelsesgebyr. Eksempelvis ila Datatilsynet selskapet Argon Medical Devices overtredelsesgebyr på 2,5 millioner kroner for å ha meldt om et brudd for sent.

Det kan være utfordrende å bedømme hvilke hendelser som utløser meldeplikt, særlig tatt



Rune Opdahl

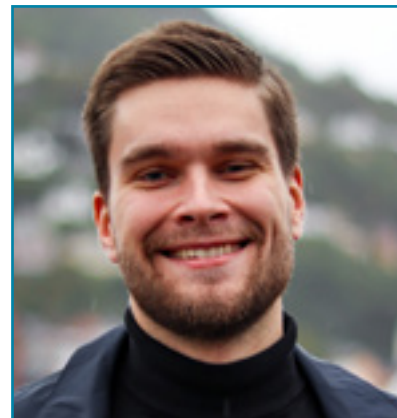
i betraktning tidsfristen på 72 timer. Derfor er en oppdatert veileder fra Datatilsynet kjærkomment – forutsatt at den gir god veiledning.

” Det kan være utfordrende å bedømme hvilke hendelser som utløser meldeplikt, [...]. Derfor er en oppdatert veileder fra Datatilsynet kjærkomment – forutsatt at den gir god veiledning.

3. Fjernet oppfordring om melding ved tvil

Datatilsynets tidligere veileder oppfordret til melding ved tvil:

«Hvis den behandlingsansvarlige er usikker på om unntaket er oppfylt,



Håvard Sveier Ottemo

er det bedre å melde til Datatilsynets for sikkerhets skyld»

Denne oppfordringen er nå fjernet. Datatilsynet har likevel beholdt bemerkningen om at den behandlingsansvarlige må være «tilnærmet helt sikker» på at bruddet ikke vil medføre noen risiko for de berørte før unntaket er oppfylt, som likevel kan resultere i at de behandlingsansvarlige fortsetter å melde selv om hendelsen etter loven ikke er meldepliktig.

4. Fra skal til kan

I den tidligere veilederen opererte Datatilsynet med en oversikt over eksempler på brudd som *skal* meldes. Dette var villedende, ikke veiledende. Eksempelvis sto det at «Brev eller e-post som inneholder personopplysninger er sendt til feil mottaker» skulle meldes, uten en nyansering om risiko ved feilen (som blant annet avhenger av opplysningenes karak-

ter, kryptering og hvem mottakeren er).

I den nye veilederen har Datatilsynet endret oversikten til brudd som *kan* meldes. Dessuten er listen supplert med bemerkninger om risiko, eksempelvis: «*Forsendelsesfeil som inneholder beskyttelsesverdige personopplysninger og hvor dette kan medføre en risiko for fysiske personers rettigheter og friheter*». Også dette blir mer villedende enn veiledende. Når Datatilsynet har lagt til presiseringen om hendelsen kan medføre risiko, er meldeplikten utløst. Altså burde overskriften være brudd som *skal* meldes, ikke brudd som *kan* meldes.

Vi merker oss for øvrig at rekkefølgen på eksemplene er omrokkert, hvor digitale angrep mot datasystemer er satt først og forsendelsesfeil er satt nederst på listen. Vi antar det skyldes at forsendelsesfeil har utgjort en stor andel av avviksmeldinger (37 % i 2025), mens risikoen ved slike hendelser ofte er beskjeden. Selv om listen ikke angir en rangordning, kan det være et signal

om hva Datatilsynet anser som mer og mindre alvorlig.

5. Behov for ytterligere veiledning

Endringene gjør den oppdaterte veilederen mer i tråd med loven. Bruken av *kan* istedenfor *skal* skaper imidlertid forvirring og burde korrigeres.

Det er dessuten enkelte sider ved meldeplikten som Datatilsynets veileder med fordel også kunne adressert:

Veilederen mangler en forklaring av hva som utgjør *brudd på personopplysningsikkerheten* (selv om Datatilsynets eksempler gir en indikasjon). Brudd på GDPR er ikke enstydig med brudd på personopplysningsikkerheten. For eksempel vil ikke manglende behandlingsgrunnlag eller manglende informasjon til de registrerte i seg selv utgjøre brudd på personopplysningsikkerheten. Det gjelder ikke en selvinkrimineringsplikt etter GDPR.

Videre sier veilederen ingenting om hva som utgjør *risiko for fysiske personers rettigheter og friheter* og hvordan slik risiko skal vurderes. GDPR fortalepunkt 75 nevner blant annet identitetstyveri, økonomisk tap og sosiale ulemper, men dette fortalepunktet er vanskelig å tolke og har ingen bindende virkning. Det ville vært til hjelp om Datatilsynet ga veiledning om dette.

Ved å motta et stort antall meldinger, har Datatilsynet opparbeidet seg inngående erfaring med brudd på personopplysningsikkerheten. I en fremtidig versjon av veilederen, kan vi håpe at Datatilsynet er enda tydeligere om hvilke hendelser som skal meldes.

Rune Opdahl: Partner, Advokatfirmaet Wiersholms avdeling for teknologi, media, telekom og immaterialrett.

Håvard Sveier Ottemo: Advokatfullmektig, Advokatfirmaet Wiersholms avdeling for teknologi, media, telekom og immaterialrett.



Illustrasjon: Colourbox.com

40 år med nordiske konferanser i rettsinformatikk

Av Olav Torvund

De årlige, nordiske konferansene i rettsinformatikk er en tradisjon som har vart i 40 år. Under konferansen i Oslo i november 2025, presenterte jeg en liten oversikt over historikken. Dette er en videreutvikling av det jeg presenterte.

Det er referater fra mange av disse konferansene i de nordiske årbøkene i rettsinformatikk. Men det er ikke referater fra alle, og noen er ganske ufullstendige. Noen konferanser er dokumentert på andre måter. Jeg har i stor grad basert meg på disse. Men jeg har også måttet supplere med min hukommelse, med de feilkilder det innebærer. Jeg har deltatt på de fleste, men ikke alle konferansene. Det gir meg en oversikt, men gjør samtidig at det kan være litt vanskeligere å holde dem fra hverandre, og å tidfeste dem. Jeg har fått noen korreksjoner etter det jeg presenterte, fra personer som kunne fortelle at «jeg deltok på min første konferanse mens jeg var vit.ass. i xxxx, og den ble holdt i xxxx.» Det er ganske sikkert flere tilfeller hvor mine minner er mer enn bare litt uklare.

Det startet i Mariefred utenfor Stockholm 5.–6. oktober 1984. Peter Seipel tok initiativet. Om det var et møte eller en konferanse, blir et definisjonsspørsmål. Det var en liten gruppe, spesielt inviterte deltakere, og jeg var ikke blant de som



Olav Torvund

deltok. I referatet i Nordisk årbok i rettsinformatikk 1985, står det:

«Konferensens syfte var bl a att informera ansvariga inom utbildningsorgan om ämnet rättsinformatik och utbildningsbehov. Konferensen behandlade bl a gränsdragningsproblemen kring rättsinformatiken som ämne.»

1984 var på så mange måter et viktig år. George Orwell hadde gjort året til et viktig år når det gjaldt spørsmål om overvåking osv. Men det var også året for den første nordiske konferansen om rettsinformatikk, den første nordiske årboken i rettsinformatikk ble utgitt dette året, og det var året da det første nummeret av *Lov & Data* ble utgitt.

Vi fulgte opp med en konferanse i Oslo i 1985, som, om min korrigerte hukommelse nå stemmer, ble holdt i IRI's lokaler i Niels Jules gt. Det var et vanlig konferanseformat med faglige presentasjoner, og i tillegg ble det holdt et møte om undervisning i faget.

Det var på denne tiden tatt initiativer til å arbeide med IT-rett ved

Universitetet i Århus, og det ble invitert til en konferanse i Århus i 1986. Temaene for denne konferansen var

- Rettslig regulering av telekommunikasjon
- Automatisering av offentlig forvaltning
- Opphavrett og informasjonsteknologi.

Innleggene fra konferansen er utgitt i Strange Beck and Ole Bruun Nielsen (red): *Ret og informasjonsteknologi*. Aarhus 1987.

I 1987 ble det invitert til en konferanse på Hanaholmen i Esbo i Finland.

I 1988 var vi tilbake i Sverige, da IRI Stockholm inviterte til en konferanse på Hässelby Slott utenfor Stockholm. Sirkelen var nå sluttet, og tradisjonen etablert. I 1989 var det igjen konferanse i Oslo, denne gangen på Det norske videnskapsakademi. Det ble da også holdt en egen studentkonferanse på jusstudentenes hytte, «Hoppeseter», utenfor Oslo.

” [1984] var også året for den første nordiske konferansen om rettsinformatikk, den første nordiske årboken i rettsinformatikk ble utgitt dette året, og det var året da det første nummeret av *Lov & Data* ble utgitt.

Danmark fulgte opp med en konferanse i Køge utenfor København i 1990, og i 1991 var vi igjen i Finland. Konferansene i Finland har noen ganger vært holdt i Helsinki og noen ganger i Rovaniemi. Og den har en gang vært holdt på Åland. I de senere årene har det vært Universitetet i Rovaniemi som har organisert disse konferansene. Jeg har ikke oversikt over når den ble arrangert hvor i Finland.

I 1992 ble konferansen arrangert i Stockholm, og temaet var Software procurement. Det var den første konferansen hvor jeg ikke deltok, bortsett fra den første i Mariefred. Det var den første konferansen som ble holdt på engelsk.

I 1993 var vi igjen i Norge. Konferansen ble arrangert av IRI i Oslo, men ble holdt på Lillehammer, året før OL. I tillegg til det som har blitt nevnt har konferansen i Norge en gang vært arrangert på Solstrand utenfor Bergen, det må ha vært i 1997. Den har vært arrangert i Lund i Sverige, og i Odense i Danmark.

Tradisjonen var nå godt etablert, og den ble organisert etter tur i fire av de nordiske landene. Island ble aldri med i dette. Det har vært deltakere fra Island, men konferansen har aldri vært arrangert i Island. Om min hukommelse stemmer, var det et år det ikke ble arrangert en nordisk konferanse, uten at jeg husker hvilket år.

Under covid-pandemien ble det arrangert to digitale konferanser. En var organisert av IRI Stockholm i 2020, og en av SERI i Oslo i 2021. Det var viktig å holde tradisjonen. Men noe av formålet med slike konferanser blir borte når man ikke lenger møtes fysisk. I 2022 var det igjen mulig å møtes, og konferansen ble holdt i København, organisert av Københavns universitet.

En workshop hvor doktorander presenterer sine prosjekter har nå blitt en del av konferansene, uten at jeg husker når dette begynte. Jeg har klare minner og bilder fra en slik

workshop i København i 2014, men jeg husker ikke om det var den første med en slik workshop. Det er viktig at doktorander får en slik mulighet til å presentere sine prosjekter, og det er verdifullt å få et innblikk i hvilke prosjekter man arbeider med andre steder. Kretsen har blitt utvidet ved at det nå arbeides med teknologirelaterte spørsmål ved mange læresteder. I de første tiårene var det for få doktorgradsprosjekter til at de kunne forsvare en egen workshop i tilknytning til konferansene. Til illustrasjon nevner jeg at Jon Bing var den første i Norge som tok doktorgrad innenfor denne fagkretsen i 1982, jeg var den andre i 1993. Det var ikke flere i de andre nordiske landene. Doktorgradsprosjekter ble presentert på konferansene, men da som konferansepresentasjoner med utgangspunkt i et pågående doktorgradsarbeid.

Det har ikke vært noen formell organisasjon bak disse konferansene. Det har blitt etablert en tradisjon hvor en representant for det landet som er det neste i rekken, under middagen på årets konferanse inviterer til en konferanse det følgende år.

I Sverige og Norge har universitetsinstitutter stått for arrangementene. IRI i Stockholm er verdens eldste eksisterende universitetsinstitusjon innen dette feltet. Det ble startet i 1968. Oslo er nummer to, og virksomheten her startet i 1970. Er det noe de fleste vet, så er det at vi nordmenn hater å bli slått av svenskene. Men vi er gode venner og har alltid hatt et godt samarbeid.

I Danmark og Finland har det ikke vært tilsvarende universitetsinstitutter. Det har vært arbeidet med teknologirelaterte rettsspørsmål ved flere universiteter, uten noen egen, formell overbygning. Der har foreningene for jus og EDB hatt en mer aktiv rolle i å organisere konferansene, sammen med ulike universitetsmiljøer.

Går vi tilbake til begynnelsen var vi få som arbeidet innenfor dette området, og vi var på utsiden av de etablerte juridiske fagmiljøene. Det var viktig å søke sammen med likesinnede i de andre nordiske landene.

Nå gjennomsyrrer informasjons-teknologien og digitaliseringen hele samfunnet, og det er få, om noen rettsområder hvor man ikke må forholde seg til informasjonsteknologi. Teknologien er ikke lenger det sammenbindende elementet som det en gang var. Personer som Peter Seipel og Jon Bing var så sentrale i fagets historie og utvikling, og for dem var det mulig i alle fall å ha en oversikt over hvordan faget utviklet seg i mange retninger. For oss som har kommet til siden, er det ikke mulig å ha den samme oversikten. Noen har forsøkt, uten egentlig å lykkes.

Mange teknologirelaterte problemstillinger knyttet til andre juridiske disipliner har først blitt tatt opp under paraplyen «rettsinformatikk». Bruk av informasjonsteknologi i juridisk virksomhet er noe man hele tiden har arbeidet med. Rettslige informasjonssystemer sto lenge sentralt. I dag videreføres dette av virksomheter som ikke er direkte knyttet til de akademiske miljøene, som Lovdata og Rettsdata. Men Lovdata er et barn av virksomheten ved IRI i Oslo. Kunstig intelligens er noe man i større eller mindre grad har arbeidet med i alle fall så lenge jeg har hatt noen kontakt med miljøet, og det har blusset opp igjen i de senere årene.

Personvern er et sektorovergripende problemkompleks som har hatt og har sitt ankerfeste i de rettsinformatiske miljøene. Innenfor mange områder ser vi at de teknologirelaterte rettsspørsmålene har blitt «business as usual». Elektronisk handel var i en periode et spørsmål som mange var opptatt av, særlig på 1990-tallet. I dag skjer det meste av handelen elektronisk. Men kan ikke arbeide med juridiske spørsmål knyttet til handel og annen kom-



Illustrasjon: Colourbox.com

mersiell virksomhet, uten å forholde seg til informasjonsteknologien. Men teknologien har ikke en like sentral plass som da det ble behandlet under overskriften «Elektronisk handel».

Opphavsrett og informasjonsteknologi er et tema som har gått igjen på flere av de nordiske konferansene. Opphavsretten er et barn av informasjonsteknologien. Den har gjennom hele fagets historie blitt utfordret av og har utviklet seg i møte med den informasjonsteknologiske utviklingen, fra Gutenberg til kunstig intelligens. Man kan ikke lenger arbeide med opphavsrett uten å forholde seg til dagens informasjonsteknologi.

Moderne masseforvaltning er gjennomdigitalisert. Man kan ikke lenger arbeide seriøst med forvaltningen og forvaltningsretten, uten å forholde seg til denne digitaliseringen. Listen kunne ha vært gjort mye lenger.

I løpet av årene har konferansene i praksis blitt mer nasjonale og mindre nordiske. Det er mange som nå

arbeider med rettslige spørsmål relatert til informasjonsteknologi, med ulike faglige utgangspunkt og avgrensninger. Det arrangeres mange nasjonale konferanser og kurs. I Norge har vi blant annet den årlige Personvernkonferansen, som arrangeres den første fredagen i desember. Og vi har Forum rettsinformasjon. Det er flere. Dette dekker langt på vei praktikernes behov for faglig påfyll og oppdatering. Det arrangeres også andre nordiske og internasjonale konferanser om det vi kan velge å kalle delområder, eller områder som overlapper med andre rettsområder.

” På en måte er vi på vei tilbake mot der det startet: Som en nordisk, akademisk nettverkskonferanse.

På en måte er vi på vei tilbake mot der det startet: Som en nordisk, akademisk nettverkskonferanse. Som nevnt arbeides det nå med

spørsmål innenfor dette emnet ved mange institusjoner, og det er mange interessante doktorgradsprosjekter. Så om den nordiske konferansene i mindre grad dekker et behov for praktiserende jurister, har det blitt et desto større behov for å ta vare på et nordisk, akademisk nettverk.

De første årene ble innleggene holdt på et slags skandinavisk, slik at i alle fall vi fra Danmark, Sverige og Norge kunne holde våre innlegg på våre egne språk. For deltakere fra Finland kunne språket være en utfordring. Stadig flere innlegg ble holdt på engelsk, og de senere konferansene har vært rent engelskspråklig.

Under middagen på den nordiske konferansen i Oslo 2025, ble det invitert til en ny nordisk konferanse i Odense i 2026, uten at det ble annonsert noen dato. De baltiske landene ønsker å bli inkludert i det nordiske nettverket, og det ble fra TalTech i Tallin (Estland) fremsatt et ønske om å arrangere konferansen i 2027.

United Nations Convention against Cybercrime and The Signing Ceremony

By Stein Schjøllberg

The adoption of the Convention against cybercrime

1.1. The background

The General Assembly adopted on 27 December 2019 a Resolution¹ on the report of the Third Committee of 25 November 2019 *Countering the use of information and communications technologies for criminal purposes*. The General Assembly adopted the Resolution with 79 countries voted in favour, and 60 countries voted against, with 30 countries abstained. The Resolution included to establish an open-ended Ad Hoc inter-governmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. It was decided in 2020 that the UNODC, shall serve as Secretariat for the Ad Hoc Committee. Because of the situation concerning the coronavirus disease (COVID-19), the Ad Hoc Committee began its work in 2021. Six sessions was held from January 2022 until august 2023, with the participation of member States and invited extern delegates. The *Concluding Session* was held from 29 January until 9 February 2024. The General Assembly decided on 24 April 2024 that a *Reconvened Concluding Session*, should be held from 29 July to 9 August 2024. A proposal was presented under the *Reconvened concluding session* on 7 August 2024. The proposal was agreed upon with acclamation on 8 August 2024.



Stein Schjøllberg

With the background on the discussions in more than two years in the Ad Hoc committee, the agreement was certainly a surprise.²

United States made the following statement to the proposal from the Ad Hoc Committee:³ Our committee has adopted a Convention against Cybercrime that reflects universal values and U.S. interests, including focused criminalization provisions, robust and flexible provisions on technical assistance, and strong provisions to safeguard human rights that are unprecedented in a UN criminal justice convention.

This compromise text, adopted by consensus, represents the hard work of many member states, informed by countless civil society, industry, and other stakeholder

views, and the United States hopes that it reflects a durable commitment to combatting cybercrime under a rights-respecting framework.

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

The draft convention was on 19 August 2024 sent to the United Nations General Assembly,⁴ and was discussed by the *United Nations Third Committee*. The Third Committee recommended to the General Assembly the adoption of a draft resolution without a vote on 11 November 2024. The Report from the Third Committee was sent to the General Assembly on 27 November 2024.⁵

” We welcome the Committee's adoption of the UN Convention Against Cybercrime as a rights-respecting criminal justice instrument for the 21st century and beyond

1.2. A Resolution was adopted by the General Assembly on 24 December 2024.

The Resolution *United Nations Convention against Cybercrime* was adopted

1 See <https://undocs.org/A/Res/74/247>

2 See <https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html>

3 See https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/abc_reconvened_concluding_session/main

4 See <https://documents.un.org/doc/undoc/gen/n24/056/82/pdf/n2405682.pdf>

5 See <https://documents.un.org/doc/undoc/gen/n24/372/04/pdf/n2437204.pdf>

without a vote,⁶ and opens it for signature in Hanoi in 2025 and thereafter at United Nations Headquarters in New York until 31 December 2026. The Resolution urges all States and competent regional economic integration organizations to sign and ratify the Convention as soon as possible to ensure its rapid entry into force.

The Convention consists of a Preamble and nine chapters:

- Chapter I General provisions
- Chapter II Criminalization
- Chapter III Jurisdiction
- Chapter IV Procedural measures and law enforcement
- Chapter V International cooperation
- Chapter VI Preventive measures
- Chapter VII Technical assistance and information exchange
- Chapter VIII Mechanism of implementation
- Chapter IX Final provisions

The Resolution includes that the Ad Hoc Committee shall continue its work for *Additional Protocols*, with a view to negotiating a draft protocol supplementary to the Convention, addressing inter alia, additional criminal offences as appropriate.

The Resolution also includes that the Ad Hoc Committee shall be holding *Sessions on Conference of the States Parties to the Convention*. The Sessions shall have a duration of up to five days in Vienna, one year after the adoption of the Convention, to prepare the draft text of the rules of procedure of the Conference of the States Parties to the Convention.

The General Assembly has decided that 24 December shall be designated *The International Anti-Cybercrime Day*, in order to raise awareness of cybercrime and of the

role of the Convention in combatting and preventing it.

The Convention includes in *Article 65* that it shall enter into force on the ninetieth day after the date of deposit of the fortieth instrument of ratification, acceptance, approval or accession. For the purpose of this paragraph, any instrument deposited by a regional economic integration organization shall not be counted as additional to those deposited by member States of that organization.

A press release was published, titled: *UN General Assembly adopts landmark convention on cybercrime*.⁷

1.3. International organizations statements on the convention against cybercrime

INTERPOL welcomes on 23 December 2024, the adoption of UN convention against cybercrime, including as follows:⁸

The convention recognizes the essential role of INTERPOL's law enforcement network in facilitating international cooperation through the rapid and secure exchange of information on "computer-related crime" and other related criminal offences.

Yale University Law School, USA, organized a panel discussion on 25 March 2025: *The U.N. Cybercrime Convention — Hearing from the Drafters*.⁹

A group of experts involved in drafting the United Nations treaty on cybercrime participated in the discussions.

Thomas Burrows, a former associate director at the U.S. De-

partment of Justice, and member of the U.S. delegation to the negotiations, gave an insider's view of the Convention's overarching goals. He retired in February 2025 after handling extradition and mutual legal assistance (MLA) matters including cybercrimes. He said he believes the 11 core offenses under the new treaty provide standards for countries to align their domestic legislation and avoid dual criminality challenges. This will enable stronger extradition and legal assistance cooperation. Burrows also outlined how preparation for the negotiations fostered a consensus among the majority of delegations. He cited the need to strengthen capacity in developing countries to ensure the treaty's eventual success.

Anthony V. Teelucksingh, also a member of the U.S. delegation to the negotiations, a former senior counsel at the U.S. Department of Justice, but retired in February 2025. He praised the process's speed but cautioned that governments must also think about strengthening their capacity to address cybercrime. He also commented on the Convention's recognition of the principle of passive personality jurisdiction, which allows states to assert jurisdiction when their nationals are victims of cybercrime abroad.

Alexander Seger, representing the Council of Europe, explained that the parties to the Budapest Convention decided to engage in the treaty process to ensure consistency of the U.N. treaty with the Budapest Convention and to address inclusion of the minimum human rights safeguards necessary for cooperation. Both objectives were achieved, and both treaties are broadly consistent and complement each other, he said.

John Brandolino, UNODC, highlighted issues confronted during the drafting process, including differences over surveillance authority, asset-sharing formulas, and

⁶ See <https://docs.un.org/en/A/RES/79/243>

⁷ See <https://www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html>

⁸ See <https://www.interpol.int/News-and-Events/News/2024/INTERPOL-welcomes-adoption-of-UN-convention-against-cybercrime>

⁹ See <https://law.yale.edu/yls-today/news/panel-shares-insights-drafting-new-un-cyber-crime-treaty>

the precise ambit of criminalized conduct. According to Brandolino, the finished product is a thoughtful compromise.

UNODC has presented the main chapters of the Convention.¹⁰

UNODC has also published *Five reasons why the new Cybercrime Convention matters*.¹¹

1. A new tool for a growing threat,
2. Around the clock cooperation,
3. Protecting children,
4. Responding to victims' needs,
- and 5. Improved prevention

The European Union Commission proposed on 16 July 2025, the Council to sign and conclude the United Nations Convention against Cybercrime, and included:¹²

First, as a UN instrument, the Convention has a wider reach in terms of membership than existing EU and international instruments. In this respect, it is similar to previous UN instruments on cooperation in criminal matters of almost universal adoption, such as UNTOC and UNCAC. It can thus enable enhanced cooperation against cybercrime at a global scale.

Second, the Convention is inspired by the Budapest Convention's criminalisation provisions, which can further enhance cooperation based on a long-standing and tested legal framework.

2. The Signing Ceremony in Hanoi on 25-26 October 2025

The Signing Ceremony was held in Hanoi, Vietnam, on 25-26 October 2025. More than 2.500 delegates

from 119 countries participated at the conference.

The Signing Ceremony was opened by the President of Vietnam State President Luong Cuong on 25 October 2025, and the opening remarks included:¹³

On behalf of the State and people of Vietnam, I warmly welcome you all to Hanoi – the City for Peace, to attend the Signing Ceremony of the United Nations Convention Against Cybercrime — a historic event marking the beginning of a new era of global cooperation in cyberspace.

For Vietnam, today's Signing Ceremony of the United Nations Convention against Cybercrime is not only a great honor, but also a responsibility to the international community. Guided by its foreign policy of independence, selfreliance, peace, cooperation, and development, diversification and multilateralisation of external relations, and as an active, reliable, and responsible member of the international community, Vietnam has, over the past five years, worked closely with other countries throughout the negotiation of this Convention.

The UN Secretary-General Antonio Guterres also made opening remarks. He described the UN Convention against Cybercrime, the Hanoi Convention, as a powerful, legally binding instrument to strengthen collective defences against cybercrime. His remarks included:

I am honoured to join you here in Hanoi on this historic occasion.

I would like to thank Vietnam for hosting this signing ceremony and for its leadership in bringing us together.

Until now, the world has lacked a common legal framework to unite our efforts.

But after five years of complex negotiations, Member States have delivered the first criminal justice treaty in more than two decades.

The UN Cybercrime Convention is a powerful, legally binding instrument to strengthen our collective defences against cybercrime.

It is a promise that fundamental human rights such as privacy, dignity, and safety must be protected both offline and online.

Executive Director of the United Nations Office on Drugs and Crime (UNODC) Ghada Waly also delivered opening remarks, including as follows:

The road has been long and challenging. Over 420 hours of formal negotiations and countless hours of informal negotiations involving more than 150 Member States and enriched by 160 stakeholders from international organisations, NGOs, academia, and the private sector.

The result is a resounding statement that multilateralism still works, and that the international community is serious about cybercrime.

The United Nations Convention against Cybercrime was signed at the formal Signing ceremony on 25 October 2025, by 64 States in the following order:

Vietnam, The Maldives, Algeria, Australia, Azerbaijan, Belarus, Belgium, Brazil, Burkina Faso, Cambodia, Chile, China, Costa Rica, Cuba, Czech Republic, Republic of Korea, Congo, Djibouti, Dominican Republic, Ecuador, Egypt, European Union, Ghana, Greece, Guinea-Bissau, Iran, Ireland, Jamaica, Laos, Libya, Luxembourg, Malaysia, Morocco, Mozambique, Nicaragua, Nigeria, Palau, Peru, Philippines, Poland, Portugal, Russian Federation, Slovakia, Republic of South Africa, Spain, Sri Lanka, State of Palestine, Sweden, Thailand, Togo, Turkey, Uganda, United Kingdom, Tanzania, Uruguay, Uzbekistan, Venezuela, Qatar, Brunei, Angola, Namibia, Austria, Nauru.

10 See <https://www.unodc.org/unodc/en/cybercrime/convention/convention-against-cybercrime-chapters.html>

11 See <https://www.unodc.org/unodc/front-page/2024/December/five-reasons-why-the-new-cybercrime-convention-matters.html>

12 See https://home-affairs.ec.europa.eu/news/commission-proposes-sign-and-conclude-un-convention-against-cybercrime-2025-07-16_en

13 See <https://hanoiconvention.org/vietnamese-state-presidents-welcome-remarks-at-signing-ceremony-of-un-convention-against-cybercrime/>

Additional 8 States signed later, and the Convention was then signed by 72 States at the end of the conference.¹⁴

Speakers from 71 countries delivered their statements during the conference.¹⁵ Many statements at the Signing Ceremony have been published.¹⁶

Australia made a statement, including as follows:

But global cooperation is vital.

That is why Australia is pleased to sign the UN Convention against Cybercrime here today in Hanoi.

This is the first-ever UN-endorsed instrument addressing cybercrime and the collection of electronic evidence.

It is a testament to the success of multilateralism and the UN's role as a forum for solving problems that transcend borders.

The Convention will harmonise cybercrime legislation, strengthen investigation and cooperation, and narrow the operating space for organised crime groups.

It will eliminate unintentional safe havens and ensure a global uplift in capability.

And it will do so using a human rights-based approach to its implementation – to ensure our efforts to combat cybercrime do not come at the expense of the rights we seek to protect.

South Africa made a statement, including as follows:

No country can confront cybercrime alone. The exploitation of children online demands our urgent and coordinated action. As international cooperation lies at the heart

of this convention, we must work collectively and exchange timeous information to prevent, detect and prosecute these crimes to ensure that victims receive the justice they deserve. As African countries accelerate digital transformation, they face increasing cyber threats that threaten developmental gains. It is therefore imperative that efforts to combat cybercrime be inclusive, responsive to diverse national contexts, and grounded in international cooperation. It is in recognition of these imperatives that South Africa took the decision to sign the United Nations Convention against Cybercrime.

United Kingdom made a statement, including as follows:

The agreement by consensus, of the text of the of the United Nations Convention against Cybercrime, just under a year ago, signalled a landmark moment for international cooperation on this critical and complex issue.

I am proud that the United Kingdom has signed the Convention here in Hà Nội, in line with our international efforts to combat cybercrime.

Cybercrime poses a serious and growing threat to every part of society, from private citizens to public institutions. It often targets our most vulnerable.

The UK stands ready to work with international partners to build resilience, share intelligence, and uphold a secure and open digital environment for all. We will support the effective establishment of the Conference of State Parties, working with Member States and expanding our close work with global stakeholders.

Cybercrime is a global challenge. We can only tackle these crimes if we work together. We look forward to making a start today.

Sweden made a statement, including as follows:

Sweden aligns itself to the statement delivered by the European Union on behalf of the European Union and its Member States and would like to deliver the following short statement in our national capacity.

Sweden is therefore proud and pleased to sign the United Nations Convention against Cybercrime and thereby showing our commitment in this joint fight. We were active in the negotiations of the Convention and will continue to be active in the next phases.

This Convention can complement already existing conventions and ways to cooperate in the fight against cybercrime. Inspiration can be taken from those previous experiences. We need to make sure that cybercriminals can have no safe haven globally.

The adoption of this Convention is a collective success for all UN members and shows the continued relevance and importance of multilateralism.

It incorporates important aspects of the rule of law and the respect for human rights. This is the basis for international cooperation that is one of the main purposes of the Convention. And also for the other tools provided by the Convention. We have all agreed that the Convention cannot be interpreted as permitting suppression of human rights or fundamental freedoms.

Luxembourg made a statement, including as follows:

First of all, I would like to highlight that as a member of the European Union, Luxembourg fully aligns itself with the statement that will be delivered by the European Union on behalf of the EU Member States.

Luxembourg welcomes the adoption and signature of the UN Convention against Cybercrime, a landmark achievement in the global fight against cybercrime.

Crimes perpetrated in cyberspace have far-reaching consequences on

14 See <https://www.unodc.org/unodc/front-page/2025/October/seventy-two-nations-sign-first-un-treaty-to-fight-cybercrime-in-milestone-for-digital-cooperation.html>

15 See <https://hanoiconvention.org/statement/provisional-list-of-speakers-in-the-plenary/>

16 See <https://hanoiconvention.org/statements/>

all actors of society, irrespective of their geographical location. Cybercrime impacts Governments, businesses and private individuals, inflicting lasting harm on its victims, especially on children. We therefore commend the efforts of our United Nations partners to reach consensus on a universal Convention to fight cybercrime.

The Convention thus sets a new standard for the fight against cybercrime on a worldwide level. It complements existing frameworks such as the UNTOC, UNCAC, and the Budapest Convention, and should fill a gap by reducing safe havens for cybercriminals.

United States made a statement, including as follows:

Recognizing our unique position as a major host of ISPs, the United States continues to review the UN Convention against Cybercrime. We note it is meant to provide law enforcement with critical tools, including expanded extradition mechanisms and enhanced opportunities to secure evidence from overseas jurisdictions.

We also note it is meant to strengthen International cooperation to combat the nonconsensual dissemination of imitate images and online child sexual exploitation, including grooming, child sexual abuse material, and sextortion.

As we engage in treaty-related discussions, we will not sit back and watch China, Russia, and others try to suppress freedom of expression or obtain data in a manner inconsistent with the obligations in the treaty. We will strongly condemn any efforts to misinterpret or seek to misuse the treaty as cover to unlawfully target U.S. citizens and businesses. We also strongly condemn the mischaracterization of lawfully adopted sanctions aimed at protecting our financial institutions.

The State Department confirmed on Monday 27 October 2025,¹⁷ that the U.S. did not sign the treaty. “The United States continues to review the treaty,” a State Department spokesperson said in a brief statement. On 10 June 2025 a similar statement was presented.¹⁸

Canada made a statement, including as follows:

On this milestone occasion, Canada reiterates its strong resolve to prevent and counter cybercrime. We welcome the Convention’s adoption by consensus in December 2024 and thank all those whose sustained efforts informed and produced this instrument: Member States, civil society, academia, independent experts, private sector entities, international organizations, and the United Nations Office on Drugs and Crime.

INTERPOL made a statement, including as follows:

INTERPOL is proud to have been part of the consultations and elaboration process that led to this achievement. The Convention holds profound significance for us and the global law enforcement community for two main reasons:

First, the Convention provides an enhanced legal and operational foundation for coordinated global action against cybercrime. It promotes harmonization in the criminalization of cyber offenses, sets procedural rules for sharing of electronic evidence and strengthens international cooperation, – prevention and technical assistance.

Second, the Convention anchors INTERPOL as a central platform

for international cooperation, through direct references under Chapter Five of the Convention, specifically in articles 37, 40, 41 and 47. These articles cover the provisions on extradition, mutual legal assistance, law enforcement cooperation and 24/7 networks for police cooperation on computer-related crime.

Together, these elements reinforce INTERPOL’s role in supporting the Convention’s effective implementation worldwide.

The Council of Europe made a statement, including as follows:

We welcome the adoption of the Hanoi Convention and its opening for signature as an important political achievement that aligns closely with our Budapest Convention on Cybercrime.

This convergence underlines the significance of the Budapest Convention, which for twenty-five years has served as the most relevant international framework against cybercrime. The shared concepts and measures of both Conventions have great potential to strengthen global responses to this phenomenon.

Governments were encouraged to sign and implement the new UN Treaty in a manner consistent with the Budapest Convention and with the conditions and safeguards contained in this new instrument.

The Hanoi Convention also provides a unique opportunity to expand co-operation with States which are not Parties to the Budapest Convention.

The Hanoi Convention offers an important opportunity to reinforce global co-operation against cybercrime, in a way that complements the Budapest Convention.

The Alliance of NGOs on Crime Prevention and Criminal Justice made a statement, including as follows:

But the implementation of this Convention cannot be a task that

17 See <https://therecord.media/us-declines-signing-cybercrime-treaty>

18 See https://www.unodc.org/documents/Cybercrime/AdHocCommittee/RoP_session/Comments_by_MS_06062025/US_RoP_of_the_UN_Convention_against_Cybercrime_11_June_2025.pdf



Illustrasjon: Colourbox.com

falls on governments and law enforcement alone. It will require a transnational, transsectoral approach.

The Ad Hoc Committee was recognised for its inclusive approach to multi-stakeholder voices, including NGOs, civil society, the private sector, and academic institutions.

This model can also ensure that the Conference adheres to the principles of effectiveness, inclusivity, transparency, and efficiency outlined in Article 57(b), and to ensuring adherence to the vital safeguards included in the Convention to uphold human rights and the rule of law.

Active engagement and a meaningful integration of civil society, the private sector and academia, in the Conference of Parties, and in national implementation, will undoubtedly contribute to effective implementation, in line with the model and spirit of the Ad Hoc Committee.

UNODC made a short summary in a Press release, including:¹⁹

The Convention against Cybercrime seeks to respond to the growing threat posed by cybercrime,

acknowledging that the misuse of information and communications technology is enabling crimes like terrorism, human trafficking, financial crimes and drug smuggling on an unprecedented scale. It aims to make the prevention and response to cybercrime more effective by strengthening international cooperation, technical assistance and capacity building, particularly for developing countries.

” It aims to make the prevention and response to cybercrime more effective by strengthening international cooperation, technical assistance and capacity building, particularly for developing countries.

Some highlights of the Convention:

- It is the first global framework for the collection, sharing and use of electronic evidence for all serious offences. Until now, there have been no broadly accepted international standards on electronic evidence;

- It is the first global treaty to criminalize cyber-dependent crimes and also offences related to online fraud, online child sexual abuse and exploitation material and online grooming of children;
- It is the first international treaty ever to recognize the non-consensual dissemination of intimate images as an offence;
- It creates the first global 24/7 Network where countries can quickly initiate cooperation; and
- It recognizes and promotes the need to build capacity in countries to pursue and cooperate on fast-moving cybercrimes.

All information on the The Signing Ceremony may be found on the official website.²⁰

I was in 2022 appointed by the United Nations as a Civil Society Delegate to the Ad Hoc committee and followed the Signing Ceremony very closely online. A book is published in Norwegian text in 2025.²¹

Stein Schjølberg, retired Chief Judge.

19 See <https://www.unodc.org/unodc/en/press/releases/2025/October/un-convention-against-cybercrime-opens-for-signature-in-hanoi-viet-nam.html>

20 See <https://hanoiconvention.org>

21 See <https://bokhandel.kolofon.no/b/fn-konvensjon-om-cyberkriminalitete-book>
<https://www.norli.no/boker/fn-konvensjon-om-cyberkriminalitet-9788230028667>

Exit-regulering av skytjenester

Av Ove A. Vanebo og Anne Buan

1. Innledning

Verden er et mer urolig sted. Ustabilitet, konflikter og skiftende politiske rammevilkår skaper forstyrrelser i den globale samhandlingen. Ikke minst merker vi dette når ulike skytjenester må forholde seg til endrete vilkår. Vi må forvente å kunne se tilfeller av at krav i nasjonal lovgivning kan føre til at en skytjeneste må endres eller avsluttes.

Mye av fokuset er på amerikanske skytjenester. Dette skyldes blant annet at USAs president har uttrykt at det kan være hensiktsmessig å hente data fra private skytleverandører.

Men problemet er større enn som så. Både Kina og Russland utfører ulike former for overvåking, og har grupperinger som finansieres for å hente inn informasjon. Fiendtlige hackere lammer tjenester og lekker privat informasjon, som regel for å få økonomisk gevinst.

Vår artikkel handler om hva slags vilkår og strategier parter som tilbyr eller bruker skytjenester bør reflektere over. Vårt hovedperspektiv er fra innkjøpersiden, men også tjenestetilbydere bør ha tanker om hvordan tjenesten de tilbyr skal håndtere endringer.

Exit fra tjenester kan håndteres på flere måter. I det følgende vil vi konsentrere oss om exit-strategier og avtaleklausuler.

2. Risikovurdering

Det er naturligvis enorme spenn i skytjenester. Noen vil være svært generiske og ha mange brukere, og det vil derfor være vanskeligere å overtale tilbyderne til å endre sin praksis eller justere standardvilkår. I andre tilfeller kan skytjenesten være svært tilpasningsdyktig og utviklet for oppdragsgiveren, og handlingsrommet kan derfor være enda større.



Ove A. Vanebo

Også exit-sitasjonene, dvs. omsendighetene som utløser «exit» kan være varierte. En relativt vanlig situasjon er at tjenesten ikke leverer hovedytelse eller sikkerhet som forspeilet på forhånd. Det kan desuten skje at staten skytjenesten er lokalisert i får en endret politisk situasjon; eksempelvis er det mye diskusjon om president Donald Trump vil endre overvåkingsreglene slik at amerikanske skytjenester ikke lenger kan brukes. Det kan også forekomme at tjenesteleverandøren sier opp avtalen, f.eks. hvis en bruker eller oppdragsgiver benytter tjenesten i strid med avtaler eller ikke gjør opp for seg økonomisk.



Det må m.a.o. utformes exit-klausuler i avtaleverket som gjør det mulig med en hensiktsmessig og effektiv exit og implementering bør, i den grad mulig, gjennomføres på en måte som legger til rette for en effektiv exit.



Anne Buan

Ofte blir hovedfokuset på exit-strategier. Slik strategier skal sørge for å planlegge og beskrive hvordan en virksomhet kan avslutte eller endre bruken av en skytjeneste ved behov. Av sentral betydning er det at det kan skje på en kontrollert, sikker og kostnadseffektiv måte.

Vi mener imidlertid at det viktigste arbeidet bør gjøres i forbindelse med kontraktsinngåelse og i forbindelse med implementering av skytjenesten. Det må m.a.o. utformes exit-klausuler i avtaleverket som gjør det mulig med en hensiktsmessig og effektiv exit og implementering bør, i den grad mulig, gjennomføres på en måte som legger til rette for en effektiv exit. Exit-strategien bør på sin side utarbeides parallelt med implementeringen og forholde seg de rammene som exit-klausulene og implementeringsarbeidet setter. Hvis leverandøren kan avslutte kundens kontrakt med 3 måneders varsel og exit krever 1000 timer må exit-planen nettopp ta utgangspunkt i dette med tanke på bemanning, migreringsplan med videre.

3. Hva er typiske problemer knyttet til en exit?

Flytting av applikasjoner og data fra en gitt skytjenesteleverandør til et

alternativt miljø er normalt mer kostbart og krevende enn å flytte inn, som følge av skytjenesteleverandøren incentiv for å beholde kundene og inntektene sine. Kundens tjenester er ofte bygget og integrert gjennom et økosystem av proprietære tjenester, filformater, API-er eller lignende slik at en exit kan innebære å etablere hele eller deler av tjenesten på nytt. Det kan også være kostbart å hente ut kundens data og å reformatere dataene slik at de kan brukes i et alternativt system.

Videre er det ofte en utfordring at kunden ikke har vært bevisst på avtalens reguleringer rundt oppsigelse, terminering og hvor raskt kundens data slettes som igjen kan gjøre en exit umulig innenfor de tidsrammer som gjelder. Leverandøren får gjerne en betydelig forhandlingsposisjon knyttet til exit-kostnadene dersom ikke exit-prosedyrer og priser er avtalt ved avtaleinngåelsen. De kan innebære å pålegge kunden høye kostnader for å flytte dataene/konvertere disse eller å få tilgang til nødvendig exit-bistand.

Mange vilkår bør ta hensyn til en exit, ved at det f.eks. er regulert hvordan nedetid, datatap, informasjonssikkerhet mv. bør håndteres. Utfordringen er likevel at avtaler ofte er laget for «solskinnsdager», og derfor i liten grad tar i betraktning at en exit situasjon – ofte i urolige tider – må ha en annen innretning enn mer ordinære vilkår.

4. Rettslig regulering av exit-situasjoner

4.1 Innledning

Vår hovedfokus er på den mer praktiske håndteringen av exit-situasjoner, men vi vil for ordens skyld kort angi hvilke sentrale regelverk som kan få betydning for exit-krav og -muligheter.

4.2 EUs personvernforordning – GDPR

GDPR har ingen egen exit-regulering. Partene må derfor se på de ge-

nerelle kravene i forordningen og forholde seg til mer fragmenterte bestemmelser.

Av størst betydning er GDPR artikkel 32: Sikkerhet ved behandlingen

- Skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen,
- Skal treffe tiltak for å sikre at enhver fysisk person som handler for virksomheten, behandler nevnte opplysninger bare etter instruks fra den behandlingsansvarlige

Også i GDPR artikkel 28, som gjelder avtale mellom behandlingsansvarlig og databehandler, vil man finne ulike krav som vil ha en side til exit-håndtering:

- Den behandlingsansvarlige må «bare bruke databehandlere som gir tilstrekkelige garantier» som «oppfyller kravene i denne forordning og vern av den registrertes rettigheter». Dette vil fort innebære en plikt til å bytte ut leverandør som ikke kan oppstille slike garantier.
- Databehandler må følge instruks «med hensyn til overføring av personopplysninger til en tredjestat». Dermed vil utleveringspålegg av en tredjestat fort kunne bryte med slike instruks.
- Databehandleren «bistår den behandlingsansvarlige med å sikre overholdelse av forpliktelsene i henhold til artikkel 32-36». Dette har en side til hvorvidt det er mulig å ivareta krav om informasjonssikkerhet, som igjen vil ha betydning for exit og valg av leverandør.
- Databehandleren «sletter eller tilbakeleverer alle personopplysninger til den behandlingsansvarlige etter at tjenestene knyttet til behandlingen er levert». I forbindelse med en exit, vil slik oppfølging av databruk ha betydning ved overgang til en ny tjenesteleverandør.
- Varslingsplikt

4.3 Forordningen om digital operasjonell motstandsdyktighet i finanssektoren – DORA

Lov om digital operasjonell motstandsdyktighet i finanssektoren gjennomfører DORA-forordningen i norsk rett. DORA inneholder eksplisitte krav til exit-strategi.

Det følger av DORA artikkel 28 nr. 8 at det er krav til exit-strategi for finansielle enheters bruk av tjenester som støtter kritiske eller viktige funksjoner. Slike funksjoner har avgjørende betydning for den finansielle enhetens økonomiske prestasjon, tjenestestabilitet eller evne til å oppfylle plikter i lov eller forskrift, se artikkel 3 nr. 22.

Exit-strategiene skal ta hensyn til risiko. Kundens adgang til oppsigelse i forbindelse med situasjoner nevnt i art. 28 nr. 7, må ivaretas. Dette vil gjelde bl.a. situasjoner med vesentlig overtredelse av lover eller forhold som endrer funksjonene som tilbys. De finansielle enhetene skal sikre at de kan si opp kontraktsregulerte ordninger *uten*

- at deres forretningsvirksomhet avbrytes,
- at overholdelsen av de forskriftsmessige kravene begrenses, og
- at kontinuiteten og kvaliteten på de tjenestene som leveres til kunder, lider skade.

Exit-planene skal være omfattende og dokumenterte, og være tilstrekkelig testet samt være gjennomgått regelmessig. de skal, i samsvar med forholdsmessighetskriteriene fastsatt i DORA artikkel 4 nr. 2.

Krav til *innholdet i kontraktene* med IKT-tjenesteleverandørene følger av DORA artikkel 30 nr. 2 f. Exit-strategier skal være på plass, og særlig sørge for innføring av en obligatorisk passende overgangsperiode. Tredjepartsleverandøren av IKT-tjenester skal fortsette å levere de respektive funksjonene eller IKT-tjenestene i den aktuelle perioden, slik at den finansielle enheten kan bytte til andre eller interne løsninger.

Ytterligere krav følger av nivå 2-regelverk, særlig delegert kommisjonsforordning (EU) 2024/1773. Ifølge den nevnte rettsakten artikkel 10, skal det foreligge retningslinjer som inneholder krav om en dokumentert exit-plan. Det skal gjennomføres en periodisk gjennomgåelse og prøving av den dokumenterte exit-planen. Ved fastsettelse av exit-planen skal det tas hensyn til følgende:

- Uforutsette og vedvarende tjenesteavbrudd
- Uhensiktsmessig eller mislykket levering av tjenester
- Uventet oppsigelse av den kontraktsregulerte ordningen.

Exit-planen skal ifølge forordningen være realistisk, gjennomførbar og basert på plausible scenarioer og rimelige forutsetninger. Gjennomføringsplanen skal være forenlig med uttredelses- og oppsigelsesvilkårene som fastsatt i kontraktsregulerte ordninger.

4.4 NIS2-direktivet

NIS2 (direktiv (EU) 2022/2555) skal sørge for tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i EØS. NIS2-direktivet er ennå ikke gjort til norsk rett, men er ventet å bli gjennomført i nasjonal rett gjennom en lov om grunnsikring om ikke altfor lenge.

Selv om heller ikke dette direktivet er nedfelt eksplisitte krav om exit-håndtering, er det basert på en «all-hazards»-tilnærming, som er en form for risikohåndtering som krever at organisasjoner beskytter seg mot alle typer trusler, inkludert bl.a. ondsinnede angrep, menneskelige feil, systemsvikt og naturkatastrofer. Det er vanskelig å tenke seg at en slik tilnærming ikke inneholder planer eller avtaler for exit-håndtering.

Tiltakene for å ivareta informasjonssikkerhet er nedfelt i artikkel 21 nr. 2, og flere aspekter er nevnt i bokstav d, ved at den aktuelle

virksomheten må ta hensyn til «sikkerhet i forsyningskjeden, herunder sikkerhetsrelaterte aspekter ved forholdet mellom hver enhet og dens direkte leverandører eller tjenesteleverandører».

Det europeiske byrå for nett- og informasjonssikkerhet, ENISA, har laget en Technical Implementation Guidance, som påpeker at det i forbindelse med implementering av NIS2 bør laget (71) «*exit strategies, in particular the establishment of a mandatory adequate transition period, provisions on intellectual property and responsibilities of the supplier during the exit period, for example to provide relevant documentation and historical logs.*»

4.5 Anskaffelsesretten

Er kunden i tillegg underlagt anskaffelsesregelverket vil en exit-situasjon også innebære at tjenesten må konkurranseutsettes på nytt i en ny kunngjort konkurranse. Dette innebærer en ytterligere aktivitet som Kunden må planlegge for i tilfelle av exit. Skjer exit-situasjonen mer akutt finnes det riktignok hjemmel i anskaffelsesregelverket for å gjennomføre såkalte hasteanskaffelser jf. forskrift om offentlige anskaffelser § 13-3 bokstav e og § 13-3 a (direkte tildeling). Merk imidlertid at valg av leverandør basert på disse prosedyrene gjerne ikke gir grunnlag for en varig løsning, kun en midlertidig løsning frem til en ordinær konkurranse er gjennomført.

5. Hva slags Exit-avtaleklausuler bør benyttes?

5.1 Innledning

Under vil vi gå gjennom ulike forhold vi anbefaler å regulere i en avtale mellom oppdragsgiver og skytjenesteleverandør for å sikre en hensiktsmessig exit-håndtering. Vi vil imidlertid ikke gå inn på den konkrete utformingen, ettersom det vil variere enormt og sprengte rammene for denne artikkelen.

5.2 Varsling ved krevende forhold og endringer i staten data befinner seg

Det følger allerede av blant annet GDPR at det skal varsles hvis f.eks. endrete politiske føringer kan skape større risiko for myndighetsinngrep og -overvåking.

Varslingen bør både skje innen en bestemt tidsfrist, f.eks. 48 timer fra tjenesteleverandøren fikk kunnskap om mulige endringer. Det bør også spesifiseres hva som skal være inntatt i varselet.

5.3 Dokumentasjon av alle prosesser rundt oppfølging av exit

Partene bør beskrive en tydelig, trinnsvis exit-prosess med roller, ansvar og milepæler. Dette kan omfatte at leverandøren utarbeider og vedlikeholder en oppdatert exit-plan som dekker aktiviteter før, under og etter avvikling, inkludert beredskaps- og kommunikasjonsplan. Begge parter bør utpeke en «exit-leder». Starttidspunkt for exit-triggere eller kriterier for dokumentasjonsutforming. Oppdragsgiver bør kreve logging, journalføring og revisjonsspor for alle exit-aktiviteter.

5.4 Sletting av data

Sletteprosedyrer kan nevnes, bl.a. sikker sletting i henhold til anerkjente standarder, inkludert overskriving, kryptografisk destruksjon for kryptert data og fysisk destruksjon der relevant. Omfang av sletteplikt kan tas med, bl.a. om leverandør skal slette data fra sikkerhetskopier, cache, logger, test- og utviklingsmiljøer, samt data hos underleverandører og i skytjenester mv.

Ansvar og roller bør også med: Hvem utfører, hvem verifiserer, og hvilke bevis skal leveres.

Det bør også være en mekanisme for å overholde lovpålagte oppbevaringskrav, med dokumentasjon av hva som ikke slettes og hvorfor.

Leverandøren kan levere en bekreftelse eller rapport som viser at sletting er utført i henhold til avtalen.

5.5 Migreringsperiode

Periodens lengde bør angis, ved at avtalen bør fastsette en minimumsperiode for migrering, tilpasset kompleksiteten i tjenesten. Avtalen bør regulere hvordan partene følger opp exit-prosessen, inkludert rapportering og kontrollmekanismer.

Leverandøren skal yte nødvendig bistand under migreringen, inkludert teknisk support og tilgang til systemer. Tilgjengelighet bør sikres også etter overføring, for eksempel ved å holde enkelte funksjoner operative i en overgangsperiode.

Tjenestekontinuitet er også sentralt å regulere, f.eks. fortsatt drift på uendret eller avtalt SLA-nivå i overgangsperioden, inkludert beredskap, overvåkning og feilretting.

Tilgjengelighet og ressurser bør også vies plass. Det kan bl.a. avklares om oppdragsgiver skal følges opp av et dedikert team, hva slags kompetansekrav som er viktige, ulike former for tilgjengelighet (inkl. utvidede tidsvinduer), og forpliktelser til kunnskapsoverføring, workshops og teknisk støtte mot ny leverandør.

5.6 Priser i overgangsperioden og for exit-aktiviteter

Det må avtales priser for overgangsbistand og exit-aktiviteter, slik at kostnader er forutsigbare. Ofte kan leverandøren forsøke å få høyere priser i en migrasjons-/overgangsperiode.

Det kan være hensiktsmessig å si noe om prisstruktur: Skal det for eksempel være timepriser per rolle, faste pakker for definerte leveranser, volumpriser (per GB/uttrekk), eller egne beredskapspriser? Kostnadskontroll kan sikres ved forhåndsgodkjenning av arbeid, ikke-overskridelsesklausul, tak pr. fase og krav om detaljerte timelister/leveranser. Mekanismer for å sikre konkurransedyktige vilkår ved forlengelse av overgang, er også relevante tiltak.

5.7 Håndtering av IP-rettigheter

Avtalen må avklare rettigheter vedrørende IP, herunder programvare, skript, malverk, integrasjonskomponenter, konfigurasjoner og dokumentasjon som utvikles eller tilpasses i kontraktperioden. Oppdragsgiver bør sikres en tilstrekkelig bred bruksrett til nødvendige elementer for å videreføre virksomhetskritiske prosesser etter exit, inkludert rett til å bruke, kopiere, modifisere og drifte slike elementer hos ny leverandør eller internt. Eventuelle begrensninger knyttet til tredjepartsprogramvare og åpne lisenser må kartlegges og reguleres uttrykkelig, med leverandørens plikt til å skaffe nødvendige viderelicensieringer eller alternativer. Leverandøren skal ikke kunne hindre kunden i å bruke nødvendige elementer etter exit.

5.8 Tilbakelevering/tilgjengiggjøring av data

En rekke aspekter knyttet til tilbakelevering av data kan reguleres. Det er avgjørende at leverandøren ikke kan slette kundens data kort tid etter en terminering av avtaleforholdet. Det er ikke uvanlig at standardvilkår inneholder bestemmelser om rask sletting etter opphør av avtalen.

Dersom dataene skal tilbakeleveres av leverandøren til kunden kan formatet som skal formidle data presiseres, og det kan være hensiktsmessig å benytte åpne og maskinlesbare formater. Er det i et uhensiktsmessig format, kan det koste mye å konvertere og overføre data.

Avtalen må presisere omfanget av data som skal tilbakeleveres, herunder forretningsdata, metadata, logger, dokumentasjon, konfigurasjoner, tilgangslister og historikk. Avtal også frister for tilbakelevering og kostnader for slik bistand.

5.9 Informasjonssikkerhet

Exit-prosessen må ivareta konfidensialitet, integritet og tilgjengelighet. Leverandøren bør dokumentere sikkerhetstiltak og bistå med nødvendige vurderinger (f.eks. DPIA/per-

sonvernkonsekvensvurdering) hvis det er relevant.

Ofte vil det være ulike personer og virksomheter som engasjeres for å sikre en smidig overgang. Det bør derfor være logger for all datauttrekk/sletting.

5.10 Oppsigelse

Avtal tydelige prosedyrer for oppsigelse, inkludert varslingsfrister og konsekvenser ved mislighold. Det bør etableres forutsigbare prosedyrer ved oppsigelse, herunder plikt for leverandøren til å yte overgangsbistand i en definert periode og til avtalte vilkår, slik at virksomhetskritiske tjenester kan videreføres uten avbrudd selv ved irregulær terminering. Konsekvenser ved mislighold bør omfatte rett til retting innen rimelig frist, dagbøter eller prisavslag ved vesentlige forsinkelser i exit, og adgang til å gjøre gjeldende tilbakeholdsrett på vederlag for ikke-leverte ytelser i tråd med gjeldende rett og kontrakt. Eventuelle begrensninger i leverandørens adgang til å terminere underleverandøravtaler som er kritiske for exit i oppsigelsesperioden bør beskrives, samt koordinering av termineringstidspunkter for å unngå utilsiktede tjenesteavbrudd.

5.11 Sluttoppgjør

For å unngå tvister om økonomi bør avtalen konkretisere hva som inngår i sluttoppgjøret, herunder utestående vederlag, lisensavgifter, kostnader til overgangsbistand, datatilbakelevering og eventuelle krediteringer eller refusjoner for forhåndsbetalte beløp.

Ofte kan det oppstå uenighet om hva som skal betales og når vederlaget skal betales. Av den grunn bør det blant annet presiseres hvordan sluttbetalingen skal beregnes og når den skal skje. Tidspunkt for slutfakturerings og betalingsforfall bør være klart, eksempelvis innen et definert antall dager etter endelig akseptert overlevering, med adskilt spesifisering av omtvistede og



Illustrasjon: Colourbox.com

uomtvistede beløp samt regler for tilbakehold av det førstnevnte.

6. Hva bør en exit-strategi inneholde?

6.1 Innledning

Det bør foreligge en dokumentert exit-plan som er realistisk og testet. Planen må beskrive alle steg fra beslutning om exit til full gjennomføring, inkludert roller, ansvar og tidsfrister.

Det er også hensiktsmessig med en periodisk gjennomgang og oppdatering av planen for å sikre at den er tilpasset gjeldende risiko og avtalvilkår.

6.2 Risikovurderinger/kritikalitet

For å vite hva som bør gjøres og hvilke tiltak som bør på plass, er det sentralt å ha på plass vurderinger av risikonivået.

Forut for planen bør det foreligge en systematisk ROS-analyse (risiko og sårbarhet) for å identifisere

sere trusler, sårbarheter og konsekvenser ved en exit. Vurder blant annet kritikaliteten til tjenestene: Hvilke funksjoner er forretningskritiske, og hvilke kan midlertidig settes på vent? Det enkleste er å bruke en metodikk som kombinerer sannsynlighet og konsekvens, og dokumentere akseptkriterier for risiko.

6.3 Identifisere alternative løsninger

Mulige alternative leverandører eller interne løsninger som kan overta tjenestene, bør kartlegges. Det kan også vurderes hvorvidt det er fornuftig med en multicloud-strategi eller bruk av åpne standarder for å redusere leverandørlås.

Kartlegg og dokumenter avhengigheter til proprietære moduler, tilpasninger, integrasjoner, lisensmekanismer og dataformater. For å redusere risiko bør det beskrives hvordan tilsvarende funksjonalitet sikres i ny løsning, og hvilke midler-

tidige tiltak som trengs for å unngå funksjonsavbrudd. Dersom det finnes uunngåelige proprietære avhengigheter, bør leverandøren forpliktes til konvertering eller tilgjengeliggjøring av nødvendig funksjonalitet i overgangsperioden på forutsigbare vilkår.

6.4 Informasjonssikkerhet

Informasjonen og tjeneste må sikres kontinuerlig beskyttelse, også i overgangsperioder. Det kan avtales om partene forholder seg til samme eller høyere/lavere sikkerhetsnivå i overgangsperioden

Tilgangsstyring bør på plass for å kontrollere tilgang for overgangsteam, prinsipp om minste privilegium, og raske avvikling av tilganger etter fullført migrasjon.

6.5 Migreringsplan

Migreringsplanen operasjonaliserer strategien til konkrete, tidfestede aktiviteter, kvalitetssikring og an-

svarslinjer, og bør minst omfatte følgende:

- **Overføringsløsninger**
Planen skal beskrive tekniske metoder for datauttrekk og overføring, herunder formater (fortrinnsvis åpne og dokumenterte), valideringsregler, datamodeller og metadata som gjør dataene anvendelige hos ny leverandør. Det bør fremgå hvordan integrasjoner håndteres, hvilke grensesnitt som benyttes, og hvordan konvertering, rensing og mapping utføres. Sikker overføring skal være kryptert og verifiserbar (for eksempel gjennom hash-summer og mottaksbekreftelser), med plan for inkrementelle uttrekk og endelig cutover.
- **Hva som gjøres i migreringsperioden**
Migreringsperioden bør dekke parallell drift der det er nødvendig, datakvalitetskontroller, funksjonelle og tekniske tester, ytelsestester, feilretting og verifikasjon hos mottaker. Tjenestekontinuitet og SLA-nivåer i overgangsperioden må presiseres, med tydelige kriterier for når produksjon flyttes og hvordan eventuell tilbakerulling gjennomføres. Planen skal også adressere koordinering med tredjepartsleverandører og håndtering av lisensflyt.
- **Bemanning**
Definer dedikerte roller og ansvar på tvers av partene, inkludert teknisk ledelse, sikkerhetsansvarlig, dataansvarlig, testleder og endringsleder. Kompetansekrav, tilgjengelighet og eskaleringspunkter bør beskrives, sammen med beslutningsmyndighet for å håndtere avvik og endringer uten forsinkende byråkrati. Kontinuitet i nøkkelressurser bør sikres, og det bør settes av kapasitet for kveld/helg ved kritiske milepæler.

- **Testing av strategien**
Gjennomfør planlagte tester og øvelser, fra simple gjennomganger av prosess til tekniske uttak og fullskala prøvemigrering der det er mulig. Testkriterier, aksepterskjer, suksessmål og læringspunkter skal dokumenteres, og planen oppdateres basert på resultatene. Det bør også testes for sikkerhet, herunder tilgangsstyring, data-integritet og hendelseshåndtering under migrering.

6.6 Håndtering av nedetid,

Nedetid må håndteres. Dette kan f. eks. innebære å inkludere maksimal tillatt nedetid under migrering eller avvikling i en Service Level Agreement (SLA) som regulerer slike spørsmål. Avtal kompensasjonsmekanismer ved brudd på SLA (f.eks. økonomisk kompensasjon eller ekstra support)

6.7 Håndtering av datatap

Datatap kan forebygges gjennom redundante uttak, validering og sikre gjenopprettingsmekanismer. Strategien bør omfatte krav til fullstendighet og integritet i uttrekk, kontrollsummer, referanse- og nøkkelkontroller, og verifikasjon av datalinjer. Backupløsninger og gjenopprettingstester må være dokumentert, med klar plan for når backuper tas, hvor de lagres, hvem som har tilgang og hvordan data gjenoprettes ved feil. Det bør også avtales dokumentasjonskrav og uavhengig bekreftelse for endelig sletting etter vellykket migrering.

6.8 Beredskapsplan

Beredskapsplanen skal sikre styring, transparens og rask håndtering av avvik under exit. Den bør beskrive styringsmodell med faste statusmøter, rapporteringsfrekvens, fremdriftsrapporter, risikologg med eiere og tiltak, endringskontroll, avvikshåndtering og eskalering. Videre bør den angi kommunikasjonslinjer internt og mot interessenter, klare roller i hendelseshåndtering, og krite-

rier for når ekstraordinære tiltak iverksettes.

Planen bør være koordinert med virksomhetens overordnede beredskaps- og kontinuitetsplaner, og inkludere tilgang til nødvendige ressurser og beslutningsmyndighet for å handle raskt.

Ove A. Vanebo er assosiert partner i CMS Kluge og er spesialist på personvern og cybersikkerhet

Anne Buan er partner i CMS Kluge og er spesialist på IT- og teknologianskaffelser

We Need to Talk About China. You Either Keep the Costs Low or Keep Control

By Jurgita Lapienytė

China holds a kill switch. But whose fault is that?

Resistance to Chinese tech in Europe began a long time ago, with Huawei being excluded from infrastructure projects, such as building the 5G network. While there was no evidence of a Chinese government backdoor into European systems, governments didn't want to risk it.

What was seen for a long time as moves in a trade war extended into Chinese devices being pushed out of governmental institutions, and there were attempts to overtake Chinese algorithms by forcing platforms like TikTok to change hands.

Much of what's happening around China is political. However, many of the security concerns are legitimate, as markets are drowning in cheap Chinese-made technologies that people choose simply because they are more affordable, hence, potentially less secure.

This week, Europe is fussing about Chinese-made buses that apparently can be controlled remotely.

Oslo's public transportation agency, Ruter, audited the city's electric buses and found that Yutong-made



Jurgita Lapienytė

vehicles can be disabled via remote-control capabilities in the bus software, diagnostics modules, and battery and power-control systems.

” Nurses, doctors, students, and workers use buses every day, and by purposely shutting them down, a foreign actor could wreak havoc on the country.

In reality, it means that the Chinese manufacturer could remotely stop or render those buses unusable. A Dutch company's buses were also probed, but no such backdoor control capabilities were discovered.

Denmark's audit came to the same conclusions, and now it's the UK's turn to investigate the buses.

Technically, the buses are still safe to use: they cannot be steered remotely, only stopped. So the

worst-case scenario is that your trip home will be cut short.

But you probably don't want Beijing having any influence over your travels, do you?

Just because Chinese manufacturers have control over your vehicles doesn't mean that control was built in for nefarious purposes. If anything, it's simply cheaper, as the devices can be serviced remotely.

But just because something is standard, we shouldn't dismiss it; instead, we should call for more rigorous standards.

Europe isn't panicking. It is auditing its fleet now to assess the dangers and possibly come up with new standards for its suppliers. And not only Chinese ones, as plenty of non Chinese manufacturers – especially those that prioritize cost over security by design – ship products with telemetry, remote update channels, and service backdoors.

Resilience is expensive. Nurses, doctors, students, and workers use buses every day, and by purposely shutting them down, a foreign actor could wreak havoc on the country.

The choice is simple, really: keep costs low or keep control.

Jurgita Lapienytė is the Editor-in-Chief at Cybernews, an award-winning cybersecurity journalist, and a leading voice in investigative reporting. With 15+ years of experience, she uncovers cyber threats, amplifies women in tech, and drives public awareness. Recognized as Cybersecurity Journalist of the Year and featured in Top Cyber News Magazine's 40 Under 40 in Cybersecurity, she is a sought-after speaker and thought leader in the field.



Illustration: Colourbox.com



AI på treningsrommet – Getty Images vs. Stability AI Limited

Den engelske High Court of Justice har nylig avsagt dom i en mye omtalt sak som gjaldt bruk av opphavsrettslig beskyttet materiale uten lisens til trening av AI-modellen Stable Diffusion. Saken sto mellom en gruppe saksøkere tilknyttet Getty Images på den ene siden og Stability AI Limited som saksøkt på den andre siden.

Getty Images (Getty) er et globalt bildebyrå som opererer under flere navn og tilbyr lisensierte bilder, fotografier, musikk og videoer. Bare i bildedatabasen som er tilgjengelig på nettsiden [gettyimages.com](https://www.gettyimages.com) kan brukeren i dag søke blant 11 461 132 ulike bilder. På den samme siden er det i dag gjort tilgjengelig 1 549 905 videoklipp som kan lisensieres og benyttes. Yahoo Finance opplyser i en artikkel fra oktober 2025 at Getty sitter på totalt 562 millioner visuelle objekter, med en omsetning på 946 millioner dollar i 2024. Materialet tilbys hovedsake-

lig gjennom den omtalte nettsiden, samt [gettyimages.co.uk](https://www.gettyimages.co.uk) og [istockphoto.com](https://www.istockphoto.com). Dette er altså en global aktør med et enormt rettighetsbibliotek og betydelig omsetning. Brukerne av tjenesten inkluderer ulike typer private virksomheter, privatpersoner, medier rundt om i verden og andre forbrukere av bildemateriale. Forretningsmodellen er tuftet på at de enkelte brukerne betaler et lisensvederlag for å bruke materialet. De enkelte selskapene i Getty-konsernet har ulike kommersielle modeller, men samtlige av disse er avhengige av at bruk av materialet skjer mot en betalt lisens.

Stability AI Limited (Stability) ble grunnlagt i 2019 og ble kjent for et bredere publikum i august 2022 gjennom lanseringen av AI-modellen Stable Diffusion. Denne AI-modellen er blant annet i stand til å generere bilder basert på beskrivelser som brukeren skriver inn i et tekstfelt. Tjenesten kan også brukes til annen bildebehandling, som for eksempel å redigere eksisterende bilder eller å oppskalere kvaliteten. Flere særtrekk ved Stable Diffusion skiller den fra andre AI-modeller. Stability har blant annet gjort den underliggende kildekoden tilgjengelig, noe som igjen åpner for videre utvikling og modifisering. Senere versjoner har noe strengere lisenskrav, men kjerneteknologien er fort-

satt tilgjengelig for forskning og utvikling utenfor Stabilitets kontroll. Et annet kjennetegn ved Stable Diffusion er at tjenesten er veldig effektiv og krever relativt lite datakraft for å behandle forespørslene fra brukeren. Dette har en stor praktisk betydning ved at tjenesten kan kjøres på alminnelige datamaskiner, såfremt disse har et sterkt nok grafikkort. Kombinasjonen av åpen kildekode og tilgang til å kjøre modellen på vanlige spill-PC-er gjør at mange benytter tjenesten for å eksperimentere og gjøre seg kjent med teknologien.

Stable Diffusion ble trent opp på et datasett bestående av om lag 2,3 milliarder bilder kjent som LAION-5B. Vi kommer tilbake til dette datasettet litt senere i denne artikkelen. Rent teknisk er Stable Diffusion en tekstbasert AI-modell innenfor det som kalles en generativ diffusjonsmodell. I dette ligger det at tjenesten er innrettet for å lage innhold som har likhetstrekk med datasettet den er trent på, kombinert med brukerens input. Benevnelsen «diffusjon» kjenner vi fra fysikken, altså spredningen av partikler fra et område med høy konsentrasjon til et område med lavere konsentrasjon. Overført til Stable Diffusion innebærer diffusjon av data at det som i utgangspunktet består av tilfeldige koblin-



Illustrasjon: Tegning av Fiona Holmboe Manshaus, november 2025 (ikke AI-generert)

ger eller støy, raffineres og forbedres gjennom en iterativ prosess som til slutt resulterer i sammenhengende bilder av høy kvalitet. Det dannes dermed etter hvert konsentrasjoner av data som opplæringen tilsier skal høre sammen. Den generative modelleringen innebærer at tjenesten trenes til å gjenkjenne mønstre og sammenhenger i dataene som har blitt koblet sammen. Etter gjennomført innlæringsperiode vil tjenesten kunne generere nye data eller bildemateriale basert på slutninger utledet fra det kjente stoffet fra opplæringen.

AI-modeller som Stable Diffusion har blitt tatt godt imot av publikum og brukes av millioner av mennesker daglig. En rekke bransjer har raskt innsett nytten som ligger i å kunne generere eller tilpasse bildemateriale på denne

måten. Reklamebyråer genererer bilder til bruk i markedsføring, reklamefilmer, brosjyrer, plakater og annonser. Innen kunst og design utvikles det en helt ny generasjon av kunst, og AI-produserte verk vinner kunstkonkurranser og står utstilt på en rekke museer og utstillinger. Innen spill- og underholdningsbransjen lages det visuelt innhold, teksturer og hele verdener basert på AI-generert innhold. Innen utdannings- og forskningsmiljøer lages det visuelt materiale som benyttes i læringsmidler, presentasjoner og modellering. Det finnes en rekke andre eksempler, for eksempel innen arkitektur, mote og produktutvikling. Dette er svært ulike bransjer, men alle disse kan bruke AI-generert innhold for å modellere, teste og fremvise nye tanker og konsepter.

Lanseringen av de ulike AI-modellene som nå vokser frem, reiser også en rekke problemstillinger. Et spørsmål som ofte trekkes frem, er hvor klokt det er å slippe løs disse modellene, tilsynelatende uten noen form for samordnet styring eller kontroll. Utviklingen går i et så rasende tempo at det er umulig å trekke noen sikre slutninger om hvordan dette området vil se ut om bare 10 til 15 år. En annen innvending gjelder selve opplæringsmetoden, som bygger på en massiv og intens utnyttelse av millioner av eksisterende åndsverk. Materialet som produseres av AI-modeller har dessuten en uklar immaterialrettslig status. Er dette åndsverk, og i så fall; hvem er det som besitter rettigheten til det enkelte verk? Er det brukeren som har instruert AI-modellen, eieren av modellen, programutvikleren, rettighetshaverne til treningsmaterialet eller noen andre? I en litt annen retning går diskusjonen om hvorvidt bilder og filmer produsert på denne måten fortjener betegnelsen kunst. Som nevnt ovenfor har AI-bilder vunnet kunstkonkurranser, noe som vekker sterke følelser hos menneskelige kunstnere som ikke bare ser en trussel mot sin egen virksomhet, men også en utvikling der kunstbegrepet endres i takt med AI-teknologiens fremvekst.

Saken som skal diskuteres her, gjaldt i utgangspunktet spørsmålet om ulisensiert bruk av eksisterende åndsverk i treningen av Stable Diffusion utgjorde en opphavsrettskrenkelse. Kjernepunktet i saksanlegget var nettopp bruk av materiale fra Getty under opplæringsperioden. Det ble opprinnelig tatt ut en omfattende stevning med en lang kravliste rettet mot Stability. Hovedkravene gjaldt krenkelser av opphavsrett, varemerkerett og etterligningsvern. Kort tid før fristen for de avsluttende innleggene trakk imidlertid Getty flere av disse kravgrunnlagene. Det ble blant annet erkjent av Getty at det ikke forelå

bevis for at treningen av Stable Diffusion hadde skjedd i Storbritannia. Dermed falt kanskje den mest interessante delen av denne saken bort. Getty fastholdt imidlertid fortsatt at det forelå en opphavsrettskrenkelse ved at Stable Diffusion i seg selv utgjorde en «infringing copy», og vi skal se nærmere på rettens drøftelse av dette spørsmålet. De øvrige spørsmål knyttet til varemerkebruk m.m. går jeg ikke nærmere inn på her.

Getty besitter som nevnt en stor database med billedmateriale. Databasen inneholder i tillegg det retten omtaler som sofistikerte, kuraterte metadata om det enkelte verk. Således vil hver enkelt datafil ikke bare inneholde selve verket, men også tilknyttet informasjon som produksjonsdato, type verk, filstørrelse, antall piksler, informasjon om skaperen av verket samt tittel og nøkkelord. Det ble anført fra Getty at disse metadataene var spesielt relevante og egnet for maskinlæring. Det ble blant annet vist til at billedmaterialet hadde meget høy kvalitet, samt at metadataene ga unik tilleggsinformasjon om det enkelte verk med stor betydning for selve læringsprosessen.

Møtepunktet mellom Getty og Stable Diffusion ligger i datasettet LAION-5B, som ble omtalt ovenfor. LAION står for Large-Scale Artificial Intelligence Open Network. Dette er en tysk organisasjon som arbeider med ulike AI-modeller og er kjent for å ha gjort tilgjengelig flere store datasett. Disse datasettene har blitt benyttet til å trene opp flere kjente AI-modeller, herunder alle publiserte versjoner av Stable Diffusion. Treningen har foregått på ulike underkategorier av LAION-5B, med metadata som inneholder om lag 5,85 milliarder CLIP-filtrerte bilde-tekst-par med URL-referanser. Kort oppsummert betyr dette at oppsettet fra LAION inneholder lenker til nesten 6 milliarder bilder. Uten å gå for dypt inn i teknologien står CLIP for Con-

trastive Language-Image Pre-training. CLIP kobler tekst og bilder i store datasett og bygger på det som kalles kontrastiv læring. Modellen skiller mellom parvise datapunkter ved å maksimere likhet innen en klasse som representerer et riktig svar, og minimere likheten i en annen klasse som representerer feil svar. Dersom *teksten* for eksempel viser til en sort hest, vil et *bilde* av en hest kunne bli fremhevet. Der teksten i stedet angir en rød postkasse, vil hesten nå ikke lenger være like relevant. Selve læringsmetoden har mye til felles med en bildebok for barn. En side i boken viser et bilde av en ball, og under står teksten «ball». De to elementene som består av bilde og tekst låses sammen til en språklig enhet. Dette lagres for fremtidig bruk.

På denne måten læres mønstre og relasjoner, og modellen vil fortløpende justere sine interne parametere for hele tiden å lage mer presise koblinger mellom treningsdataene og forespørsler som skal behandles. En viktig form for slike parametere er vekter. Vekter fungerer litt på samme måte som nevroner i den menneskelige hjernen. Hver forbindelse har en assosiert vekt eller verdi som angir både styrken og hvor viktig den enkelte forbindelsen er. Når en AI-modell for eksempel skal vurdere om en e-post er reklame, vil den kunne gå gjennom eposten og vurdere innholdet basert på definerte faktorer. For eksempel vil AI-modellen vurdere nøkkelord, språklige sammenhenger, virkemidler, lengde på setninger, tegnsetting og lignende. Hvert element knyttes opp mot en definert vekt, som til sammen gir en konklusjon på om innholdet er reklame eller ikke. Disse vektene er faktorer som kan justeres under trening, slik at utfallet av vurderingen blir mer presise eller bedre tilpasset utviklerens ønsker.

Som en del av opplæringsprosessen vil det være nødvendig å laste ned selve bildene som URL-listene i LAION datasettet viser til. Denne

prosessen omtales som materialisering. Det er gjennom materialiseringen at AI-modellen får tilgang til selve bildet, som i dette tilfellet ble mellomlagret på en Amazon-server. I tillegg ble det fremstilt midlertidige eksemplarer av bildet i minnebrikken på grafikkortene som kjørte selve treningsøkten i AI-modellen. Stabilitys egen beskrivelse av denne prosessen gjorde det klart at det først skjedde en eksemplarframstilling og lagring på selve serveren, og deretter en ytterligere og midlertidig eksemplarframstilling i det bildet ble håndtert gjennom RAM-brikken på grafikkortet. Vi kan lese ut av dommen at Getty erkjente at datasettene fra LAION faktisk inneholdt referanser til Gettys bilder og at disse mest sannsynlig ville ha blitt brukt i opplæringen. Partene avklarte dette i saksforberedelsen ved at Getty presenterte 11 bilder som eksempler. Den underliggende anførselen var likevel at det i praksis var blitt benyttet millioner av bilder. Stability på sin side erkjente at enkelte av disse 11 eksemplene var blitt benyttet av Stable Diffusion.

Som omtalt ovenfor forelå det ikke bevis på at noen av disse handlingene hadde skjedd i Storbritannia, og Getty hadde altså forut for de muntlige forhandlingene frafalt de deler av kravet som gjaldt denne formen for eksemplarframstilling. I saken var det erkjent fra Stability at treningen innebar bruk av bilder som ble hentet fra Gettys database via URL-lenken i LAION. Stability anførte samtidig at antallet bilder som konkret ble benyttet, ville variere ut fra oppsettet for den enkelte treningsrunden. For tilfeller hvor Stable Diffusion produserte bilder med Gettys varemerke integrert, anførte Stability at dette skyldtes bruk av en tredjepart (brukeren av tjenesten), og at bruken ikke var varemerkerettslig relevant. Bakgrunnen for denne diskusjonen var at Stable Diffusion kunne frembringe bilder som inneholdt et såkalt vann-

merke fra Getty. Getty har selv lagt inn vannmerker på bildene i sin egen database. Når brukeren søker opp bilder hos Getty, vil disse fremvises med vannmerket integrert i bildet. Først når brukeren betaler lisens for bildet, fjernes vannmerket slik at bildet kan lastes ned og brukes uten vannmerket. Vi går ikke her dypere inn på spørsmålet om inngrep i varemerkeretten.

Engelsk rett skiller mellom primær og sekundær krenkelse av opphavsrett. Eksemplarframstilling og fremføring er typiske direkte og primære krenkelser. Salg av eksemplarer av åndsverk, samt utleie, import og besittelse, er handlinger som under engelsk rett vil kategoriseres som sekundære krenkelser. Den gjenstående anførselen om krenkelse av opphavsrett gikk på at selve Stable Diffusion innebar en sekundær krenkelse av opphavsretten. Gettys anførsel var ikke at Stable Diffusion i seg selv utgjorde en eksemplarframstilling av de aktuelle verkene, eller at slike eksemplarer var lagret i Stable Diffusion. Ifølge Getty skjedde krenkelsen ved at utviklingen av vektene (som ble utviklet gjennom opplæringen, ref ovenfor) benyttet i Stable Diffusion ville ha utgjort en sekundær krenkelse av opphavsretten dersom handlingen hadde funnet sted i Storbritannia. Copyright, Designs and Patents Act av 1988 § 27 definerer hva som utgjør en krenkende kopi av et åndsverk:

“27. Meaning of “infringing copy”.

(1) In this Part “infringing copy” in relation to a copyright work, shall be construed in accordance with this section.

(2) An article is an infringing copy if its making constituted an infringement of the copyright in the work in question.

(3) An article is also an infringing copy if—

(a) it has been or is proposed to be imported into the United Kingdom, and

(b) its making in the United Kingdom would have constituted an infringement of the copyright in the work in question, or a breach of an exclusive licence agreement relating to that work.”

Det springende punkt i rettens vurdering ble dermed om det forelå en «article» etter § 27, med henvisning til paragrafene 22 og 23, og om denne var en «infringing copy». Getty anførte at vilkårene i § 27 nr 3 a og b var innfridd ved at det hadde skjedd en slik import som beskrevet i bokstav a, og at det å fremstille «artikkelen» ville ha vært ulovlig i Storbritannia. Getty viste her til at opplæringen som fant sted innebar ulisensiert eksemplarframstilling både på server og i RAM-brikken. «Artikkelen» det i denne sammenhengen siktes til, er ikke selve Stable Diffusion, men de underliggende vektene som ble utledet og optimalisert gjennom opplæringsprosessen. Vektene ble direkte påvirket av gjennomgangen av de ulike eksemplarene, og denne eksponeringen endret samtidig fundamentale forhold ved vektene karakter.

Stability anførte på sin side at begrepet «article» i lovens forstand var begrenset til å gjelde håndfaste objekter. Bestemmelsen i § 27 kunne dermed ikke anvendes på abstrakt informasjon som vekter i en AI-modell. Videre anførte Stability at begrepet «infringing copy», slik definert i § 27, ikke kunne få anvendelse utfra flere hensyn, blant annet fordi vektene i seg selv ikke lagrer eller fremstiller eksemplarer av de aktuelle verkene.

Retten viser i premiss 553 til at vurderingen må ta utgangspunkt i hvordan en AI-modell som Stable Diffusion er lært opp, og hvordan den senere produserer sine egne bilder. For å avklare om Stable Diffusion i det hele tatt kan utgjøre en krenkelse av opphavsretten, må ret-

ten først ha en klar formening om hva Stable Diffusion faktisk er. Dette spørsmålet hadde vært gjenstand for flere ekspertvurderinger, og retten viser til Professor Brox, som hadde uttalt følgende, gjengitt i dommens premiss 554:

“8.36...in order for a diffusion model to successfully generate new images, that model must learn patterns in the existing training data so that it can generate entirely new content without reference to that training data.

8.37 Rather than storing their training data, diffusion models learn the statistics of patterns which are associated with certain concepts found in the text labels applied to their training data, i.e. they learn a probability distribution associated with certain concepts. This process of learning the statistics of the data is a desired characteristic of the model and allows the model to generate new images by sampling from the distribution.

[...]

8.40 ...For models such as Stable Diffusion, trained on very large datasets, it is simply not possible for the models to encode and store their training data as a formula.... It is impossible to store all training images in the weights. This can be seen by way of a simple (example) calculation. As I explained in paragraph 6.28 above, the LAION-5B dataset is around 220TB when downloaded. In contrast, the model weights for Stable Diffusion 1.1-1.4 can be downloaded as a 3.44GB binary file. The model weights are therefore around five orders of magnitude smaller than a dataset which was used in training those weights.”

Eksperten påpeker altså at AI-modellen ikke lagrer selve bildene i vektene. Dette fremgår blant annet av at modellvektene for Stable Diffusion kan lastes ned som en relativt liten binærfil. Filstørrelsen på binærfilen er på under 4 gigabyte, mens datasettet LAION-5B, som ble brukt til opplæringen, utgjør om lag

220 terabyte. Under opplæringen lagrer ikke modellvektene pikselverdier knyttet til alle de millioner eller milliarder av bilder som gjennomgås. I stedet konverteres bildeinformasjonen fra pikselenheter til et såkalt latent område ved hjelp av en autoenkoder. Et slik latent område inneholder en komprimert representasjon av bildet, i et format som altså er langt mer effektivt både for lagring og senere beregninger eller bruk av informasjonen. Alt dette tilsier at bildematerialet ikke kan være lastet inn i selve vektene som ligger i Stable Diffusion.

Samtidig har ekspertene vært enige om at Stable Diffusion kan generere bilder som er distinkte og ulike treningsbildene, men at det også kan produseres bilder som er tilnærmet identiske med læringsmaterialet. Det kommer ikke klart frem fra avgjørelsen hvorfor Getty ikke hadde forfulgt dette sporet nærmere. Så lenge Stable Diffusion er i stand til å gjengi bilder fra opplæringen, vil det kunne være nærliggende å argumentere for at dette i seg selv utgjør en ulovlig eksemplarframstilling. Avhengig av det nærmere faktum rundt akkurat denne prosessen, vil det kunne anføres at både lagringen og den nye framstillingen utgjør inngrep i opphavsretten. Argumentet må da være at det ikke er avgjørende hvorvidt bildene er lagret i samme pikselformat som originalene. Så lenge bildene kan gjenskapes, er det en sterk indikasjon på at disse er lagret, om enn i et annet format, i vektene som ligger i AI-modellen. En relevant parallell kan være bruken av et komprimeringsprogram for å komprimere en fil. Selv om den nye filen er mindre målt i ren filstørrelse, vil det fortsatt kunne sies å foreligge en kopi av det originale verket så lenge dette kan gjenopprettes fra den nye filen. Dette argumentet ble imidlertid ikke fremholdt i denne saken.

Rettens vurdering av begrepet «article» og hvorvidt dette også omfatter mer flyktig digital informa-

sjon er for omfattende til å gjengis fullstendig her. I en tidligere artikkel (*Nasjonalstater og hacking*, Lov & Data nr. 160 4/2024) har jeg diskutert det engelske tolkningsprinsippet «always speaking», som taler for en dynamisk lovtolkning. Dommeren er inne på dette også i den foreliggende saken, og viser i premiss 580 til at prinsippet taler for at elektronisk lagrede data kan omfattes av begrepet «article»:

«I agree with Getty Images that the “always speaking principle” is of assistance in these circumstances. Stability does not suggest that the statute was intended to be “frozen” in time and I consider that modern storage methods in intangible media amount to a fresh set of facts which fall within the same genus of facts as those to which the original expressed policy has been formulated. The fresh set of facts arises by reason of the prevalence in the modern world of intangible electronic storage which has been brought about by enormous strides in technology since the date of commencement of the CDPA. The purpose of the Act – the protection of copyright owners – would, in my judgment, be fulfilled by an interpretation which encompassed modern technology.»

Selv om retten konkluderer med at loven også i prinsippet vil kunne omfatte digital informasjon lagret på ulike medier, gjenstår spørsmålet om det foreligger en «infringing copy». Stability presenterte en passende spissformulering av denne problemstillingen. «...[a]n infringing copy must be a copy» (ref premiss 592, understreket i dommen). Det Stability vil få frem er at det må foreligge en kopi – et eksemplar som rent fysisk og praktisk lar seg gjenfinne et sted. Ettersom modellvektene i Stable Diffusion ikke lagrer den visuelle informasjonen som ligger i originalverkene, kan det heller ikke foreligge en kopi eller eksemplar i lovens forstand.

Retten formulerer etter dette problemstillingen slik i premiss 599:

“...[w]hether an article whose making involves the use of infringing copies, but which never contains or stores those copies, is itself an infringing copy such that its making in the UK would have constituted an infringement. Taking the specific facts with which I am concerned, is an AI model which derives or results from a training process involving the exposure of model weights to infringing copies itself an infringing copy?”

Dette diskuteres videre i det sentrale premiss 600 i dommen, hvor retten konkluderer med at det ikke foreligger en eksemplarframstilling i lovens forstand:

“In my judgment, it is not. It is not enough, as it seems to me, that (in Getty Images’ words) “the time of making of the copies of the Copyright Works coincides with the making of the Model” (emphasis added). While it is true that the model weights are altered during training by exposure to Copyright Works, by the end of that process the Model itself does not store any of those Copyright Works; the model weights are not themselves an infringing copy and they do not store an infringing copy. They are purely the product of the patterns and features which they have learnt over time during the training process. Getty Images’ central submission that “as soon as it is made, the AI model is an infringing copy” is, accordingly, in my judgment, entirely misconceived. Unlike the RAM chip in Sony v Ball which became an infringing copy for a short time, in its final iteration Stable Diffusion does not store or reproduce any Copyright Works and nor has it ever done so. The fact that its development involved the reproduction of Copyright Works (through storing the images locally and in cloud computing resources and then exposing the model weights to those images) is of no relevance. Furthermore, that there is no requirement that an article which is an infringing copy must continue to retain a copy does not assist Getty Images, because it is implicit in the word “continue” that at some point the article has in fact contained an infringing copy. The model weights for each

version of Stable Diffusion in their final iteration have never contained or stored an infringing copy.”

” Det sentrale ved dommen er etter min mening rettens utlegninger og vurderinger knyttet til hva en AI-modell er i ulike rettslige betydninger.

Getty vant altså ikke frem med sine anførsler knyttet til dette kravet. Retten landet på at modellvektene er et resultat av læringsprosessen, men at de ikke gjengir eller lagrer bildeverkene som sådan. Dette mener retten må gjelde selv om modellvektene påvirkes og endres fortløpende gjennom opplæringen

og kontakten med bildeverkene. Retten bygger på at modellvektene aldri kan sies å ha inneholdt, lagret eller kopiert de aktuelle verkene. Kravet om sekundær krenkelse av opphavsrett førte dermed ikke frem, men retten sa seg altså enig i det prinsipielle spørsmålet og konstaterte at en «article» i lovens forstand kan omfatte mer flyktig digital informasjon.

Dommen omfatter flere andre spørsmål, og retten har noen ytterligere drøftelser også rundt spørsmålet knyttet til brudd på opphavsretten. Getty vant delvis frem med mindre krav knyttet til krenkelse av varemerkeretten. Det sentrale ved dommen er etter min mening rettens utlegninger og vurderinger knyttet til hva en AI-modell er i ulike rettslige betydninger. Rettens drøftelser rundt modellvekter og hvordan disse inn-

går i opplæringen av denne typen AI-modeller er svært interessant og svært grundig. Dette betyr også at dommen er et utmerket springbrett for videre diskusjoner og avklaringer fremover innenfor dette området, uavhengig av om man er enig eller uenig i rettens konklusjoner. Samtidig er akkurat denne saken preget av flere uklarheter knyttet til Gettys krav og anførsler, som altså ble endret vesentlig helt mot slutten av saksforberedelsen. Det kan virke som at faktum rundt hvor selve opplæringen hadde funnet sted ikke var tilstrekkelig klarlagt ved saksanlegget. Det helt sentrale spørsmålet om hvorvidt selve opplæringen og bruken av rettighetsbelagte verk til dette formålet, ble derfor ikke vurdert. Det er imidlertid helt klart at vi kan forvente flere saker på dette området fremover.

FN-konvensjon om cyberkriminalitet

Nasjonal og internasjonal regulering av cyberkriminalitet:

Europarådets konvensjon om artificial intelligence (AI)

Forfatter: Stein Schjølberg

Tittel: FN-konvensjon om cyberkriminalitet. Nasjonal og internasjonal regulering av cyberkriminalitet : Europarådets konvensjon om artificial intelligence (AI)

Oslo: Kolofon, 2025

ISBN: 9788230028674



Stein Schjølberg er tidligere en politibetsmann ved Oslo Politikammer, og senere sorenskriver. Han var grunnleggeren av den internasjonale harmonisering av lovtiltak, og grunnleggeren av kunnskapen om datakriminalitet i Norge, og har i mange år vært en av Norges ledende eksperter på datakriminalitet og cyberkriminalitet. Han har vært en av verdens ledende eksperter på cyberkriminalitet, og ble 20. januar 2022 oppnevnt av FN som en *Civil Society Delegate in the United Nations Ad Hoc Committee*, som den eneste *Civil Society*-representant fra de nordiske land. AD Hoc- komiteen utarbeidet i 2022-24 en FN-konvensjon om cyberkriminalitet.

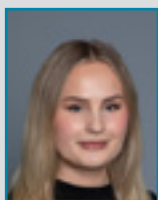
Boken inneholder omtale av FN-konvensjonen om cyberkriminalitet, *United Nations convention against cybercrime*, som ble vedtatt av Hovedforsamlingen i FN den 24. desember 2024. Konvensjonen bygger hovedsakelig på Budapest-konvensjonen av 2001, som de norske straffebestemmelser også er et resultat av.

Andre viktige forebyggende tiltak som også ble vedtatt i 2024 blir

også behandlet i boken. Det er Europarådets konvensjon om Artificial Intelligence (AI) av 17. mai 2024, og FN-Resolusjonen om Artificial Intelligence (AI) av 11. mars 2024.

Schjølberg redegjør i boken for de straffebestemmelsene i straffeloven som omhandler cyberkriminalitet, og gir en oversikt over de tiltakene politi og påtalemyndighet kan gjennomføre i etterforskningen av slik kriminalitet. Boken inneholder omtale av 70 høyesterettsavgjørelser, blant annet en avgjørelse om at publisering av en ytring i en lukket gruppe på Facebook kan straffes som hensynsløs atferd, og en avgjørelse om at data fremskaffet ved dataavlesing utført av utenlandske myndigheter kan føres som bevis i norske straffesaker. Boken gjennomgår også den nasjonale og internasjonale historiske utviklingen av tiltak mot cyberkriminalitet.

Omtalen er hentet fra Kolofon bokhandel:
<https://bokhandel.kolofon.no/b/fn-konvensjon-om-cyberkriminalitet>



Delphi

Klara Thyren og Alexander Persson

Grundaren av Flashback frias i tingsrätten från hets mot folkgrupp och IMY inleder tillsyn av Miljödata

Flashbacks grundare frias från ansvar enligt BBS-lagen *Bakgrund*

Den 1 oktober 2025 meddelande Stockholms tingsrätt sin dom i målet B 3823–24 där grundaren och VD:n för webbforumet Flashback åtalades för brott mot 7 § lagen (1998:112) om ansvar för elektroniska anslagstavlor och för att han, som tillhandahållare av tjänsten, av grov oaksamhet underlåtit att ta bort meddelanden som uppenbart innehöll hets mot folkgrupp enligt 16 kap. 8 § BrB. I domen tydliggörs flera viktiga principer och tolkningar av lagen (1998:112) om ansvar för elektroniska anslagstavlor (den så kallade ”BBS-lagen”).

Utredningen

Tingsrätten prövade tolv inlägg på Flashback som åklagaren menade utgjorde hets mot folkgrupp. Domstolen betonade vikten av att värna om yttrandefriheten men konstaterade att den inte skyddar uttalanden som uttrycker missaktning mot grupper utifrån till exempel nationalitet eller hudfärg. Elva av inläggen ansågs ha passerat gränsen för saklig kritik och bedömdes som hets mot folkgrupp.

Domstolen prövade också Flashbacks uppsiktsplikt och konstaterade att tillhandahållaren inte behöver läsa varje inlägg, men måste bedriva regelbunden tillsyn. Elektroniska anslagstavlor får inte stå utan övervakning under längre perioder, och vad som anses rimligt beror på hur omfattande verksamheten är och hur många som använder den. Om det inte är möjligt att läsa alla meddelanden i tjänsten kan uppsiktsplikten uppfyllas genom att med hjälp av en ”klagomur” ge användare möjlighet att nå tillhandahållarna för att påtala förekomsten av straffbara meddelanden. Trots att forumet hade moderatorer och rapporteringsfunktioner bedömdes tillsynen vara otillräcklig eftersom de olagliga inläggen fanns kvar på forumet i över ett år. VD:n ansågs därför ha brustit i sin uppsiktsplikt, men eftersom bristen inte bedömdes nå upp till nivån för grov oaksamhet friades VD:n från ansvar.

Hur långt sträcker sig uppsiktsplikten?

Fallet belyser flera viktiga frågor för den som driver elektroniska anslagstavlor, särskilt när det gäller hur långt uppsiktsplikten sträcker sig. Tingsrätten klargör att tillhandahållare har ett ansvar att faktiskt och

regelbundet granska innehållet på sina elektroniska anslagstavlor. Det är inte tillräckligt att bara förlita sig på rapporteringsfunktioner eller att användarna själva rensar bort olämpliga inlägg. Det krävs en aktiv och tydligt organiserad struktur för tillsynen. Domstolen framhåller också att kraven på kontroll ökar i takt med forumets storlek och aktivitet. Ju fler inlägg som publiceras, desto större är behovet av tydliga rutiner.

Avvägningen mellan yttrandefrihet och straffansvar

Tingsrätten betonade att yttrandefriheten är grundlagsskyddad och därför måste begränsas med stor försiktighet. Reglerna om hets mot folkgrupp innebär en sådan begränsning och ska tolkas restriktivt, där straffansvar bara kan bli aktuellt när det tydligt framgår att ett yttrande har passerat gränsen för saklig och vederhäftig kritik. Även obekväma eller kontroversiella åsikter omfattas fortfarande av yttrandefrihetens skydd. Fallet tydliggör att bestämmelsen om hets mot folkgrupp ska tillämpas snävt för att inte inskränka yttrandefriheten mer än nödvändigt. Hänsyn tas bland annat till innehållets ton och attityd samt till om texten utgör en saklig

diskussion eller enbart är ett uttryck för förakt.

Konsekvenser för plattformsoperatörer – ett proportionellt ansvar

Rättsfallet visar även att ansvaret för elektroniska anslagstavlor bedöms utifrån en proportionalitetsprincip. Det betyder att tillhandahållaren inte behöver granska varje inlägg i förväg, men ska organisera verksamheten så att olagligt material kan upptäckas och tas bort inom rimlig tid. Kontroll och tillsyn måste ske regelbundet och anpassas efter forumets storlek och aktivitet. Ju fler användare och inlägg som finns, desto större krav ställs på rutiner och fungerande rapporteringssystem. Domstolen framhåller däremot att ansvaret ska vara rimligt och balanserat. Tillhandahållaren kan inte undgå ansvar genom att hänvisa till att uppgiften är för omfattande, men kraven får inte heller vara så stränga att de försvårar möjligheten att driva ett större forum.

I praktiken innebär detta att modereringsresurser, tekniska verktyg och rutiner måste anpassas efter plattformens omfattning och aktivitet. Det är också viktigt att dokumentera de tillsynsåtgärder som vidtas för att kunna visa att olagligt innehåll hanteras i enlighet med tillsynskravet.

IMY inleder tillsyn av Miljödata efter dataintrång

Den 3 november 2025 meddelade Integritetsskyddsmyndigheten ("IMY") att myndigheten inleder tillsyn med anledning av IT-attacken mot Miljödata i Karlskrona AB ("Miljödata") som inträffade den 23 augusti 2025. Tillsynen syftar till att utreda om lämpliga tekniska och organisatoriska åtgärder har vidtagits för att säkerställa en lämplig



Illustrasjon: Colourbox.com

säkerhetsnivå i förhållande till de risker som behandlingen medför, i enlighet med artikel 32 GDPR.

Miljödata är en systemleverantör inom området för arbetsmiljöhantering, HR och rehabilitering. Bland annat kommuner, regioner, universitet och större privata verksamheter har Miljödata som systemleverantör och har påverkats av angreppet. Incidenten medförde att hotaktören fick tillgång till Miljödatas IT-miljö, vilket resulterade i att mycket stora mängder personuppgifter röjdes och publicerades på darknet. Enligt Åklagarmyndighetens uppskattning, som IMY hänvisat till, handlar det om uppgifter tillhörande cirka 1,5 miljoner privatpersoner. Bland de röjda uppgifterna fanns känsliga personuppgifter, uppgifter om personer med skyddad identitet och personuppgifter som rör barn.

IMY har tagit emot över 500 anmälningar från aktörer som angett att Miljödata är deras personuppgiftsbiträde, samt omkring 70 klagomål från drabbade registrerade. Granskningen fokuserar på om Miljödata har vidtagit erforderliga

tekniska och organisatoriska åtgärder enligt GDPR och huruvida någon part har brustit i dess skyldigheter enligt GDPR. Eftersom många aktörer har berörts av IT-angreppet har IMY valt att granska ett urval baserat på den verksamhet som bedrivs och de risker det finns indikationer på. Granskningen omfattar därför även en region och två kommuner, med syftet att undersöka hur dessa har behandlat personuppgifter i system som tillhandahålls av Miljödata.

IMY har tillskrivit Miljödata, en region och två kommuner tillsynsskrivelser med frågor som parterna ska besvara. Det återstår därefter att se hur IMY beslutar i ärendet och huruvida någon part har brustit i sina GDPR-skyldigheter. Incidenten understryker hur viktigt det är med att implementera säkerhetsåtgärder och konsekvent se över att de upprätthålls.

Av Klara Thyren, Associate, Advokatfirman Delfhi, Alexander Persson, Thesis Trainee, Advokatfirman Delfhi.



Gorrissen Federspiel

Tue Goldschmieding

Nyt om persondataret

Vestre Landsret 15-dobler GDPR-bøde til ILVA A/S for ulovlig opbevaring af personoplysninger

Vestre Landsret afsagde den 2. september 2025 dom i en ankesag mod det danske møbel- og boligtilbehørsfirma ILVA A/S (»ILVA«) for overtrædelse af princippet om opbevaringsbegrænsning i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«). Sagen blev behandlet under sagsnummer SS-364/2021-VLR.

Sagen vedrørte personoplysninger om ca. 350.000 tidligere kunder, som blev opbevaret i et ældre IT-system (et AX 2.5-system). Opbevaringen fandt sted uden slette- og anonymiseringsprocedurer. Sagen blev afgjort ved Retten i Aarhus i første instans, hvor ILVA blev fundet skyldig og idømt en bøde på 100.000 kr. under hensyntagen til virksomhedens nettoomsætning.

Ankesagen for Vestre Landsret angik navnlig spørgsmål om tilregnelse og bødeudmåling. Landsretten fandt det bevist, at flere personer i ILVA's interne styringsgruppe kendte til systemets fortsatte brug på trods af, at systemet ikke var underlagt en slettepolitik. Retten fandt derfor, at overtrædelsen skulle tilregnes virksomheden som forsætlig.

Landsretten forelagde præjudicielle spørgsmål for EU-Domstolen om forståelsen af »virksomhed« i relation til bødeudmålingen efter artikel 83 i GDPR, herunder om bøde-

deloftet skulle baseres på datterselskabets omsætning eller koncernens omsætning. Med henvisning til EU-Domstolens besvarelse af landsrettens præjudicielle spørgsmål i sag C-383/23, fik landsretten bekræftet, at begrebet »virksomhed« i GDPR artikel 83 skal forstås i overensstemmelse med konkurrenceretten, og at bødeloftet skal beregnes ud fra koncernens samlede globale omsætning.

Landsretten stadfæstede byrettens dom men forhøjede bøden til 1.500.000 kr. Ved bødefastsættelsen lagde landsretten vægt på den udviste forsætlighed under forløbet samt på koncernens samlede omsætning.

Dommen er af principiel betydning, fordi den fastlægger, at bødeloftet efter GDPR artikel 83 i danske straffesager skal beregnes med udgangspunkt i den samlede globale årlige omsætning i koncernen. Derudover fastslår dommen, at ledelsens kendskab til faktiske forhold i strid med GDPR's princip om opbevaringsbegrænsning kan kvalificeres som en forsætlig overtrædelse, hvilket anses som en skærpende omstændighed ved bødefastsættelsen.

Læs Vestre Landsrets dom her: <https://domsdatabasen.dk/#/sag/9975/11672/>

Datatilsynet har udtalt kritik af kriminalforsorgen for mangelfuld håndtering af indsigtssager

Det danske Datatilsyn (»Datatilsynet«) traf den 10. juli 2025 afgørelse i en

sag om Den Danske Kriminalforsorgs (»Kriminalforsorgens«) håndtering af indsattes indsigtsanmodninger. Sagen blev behandlet under journalnummer 2024-432-0030.

Datatilsynet fandt flere kritisable forhold ved et tilsyn af Kriminalforsorgens behandling af indsigtsager fra indsatte. På baggrund af tilsynet har Datatilsynet udtalt kritik af Kriminalforsorgen.

Datatilsynets udtalte kritik af Kriminalforsorgens manglende overholdelse af indsigtsretten efter GDPR artikel 15 samt af udøvelsen af den registreredes rettigheder herunder overholdelse af tidsfrister efter GDPR artikel 12. Kriminalforsorgens behandling af indsigtssagerne var mangelfuld bl.a. på grund af utilstrækkeligt kendskab til reglerne herunder anvendelse af forkert lovgrundlag, idet der ikke blev skelnet mellem aktindsigt efter lovbekendtgørelse nr. 433 af 22. april 2014 (»den danske lov om forvaltning«) og lovbekendtgørelse nr. 145 af 24. februar 2020 (»den danske lov om offentlighed«) og indsigtsretten efter GDPR.

Datatilsynet fremhævede, at fejlene i behandlingen af indsigtssagerne resulterede i, at indsatte ikke fik udleveret de oplysninger, som de havde ret til, og grundet lange svar-tider ikke fik oplysninger udleveret inden for de gældende tidsfrister. På den baggrund udtalte Datatilsynet kritik af Kriminalforsorgen for manglende overholdelse af indsigtsreglerne i GDPR.

Kriminalforsorgen har efterfølgende oplyst, at der er iværksat afhjælpende tiltag herunder målrettet onboarding af medarbejdere. Datatilsynet har tilkendegivet, at de i 2026 vil følge op og anmode Kriminalforsorgen om en redegørelse for de implementerede tiltag på området samt for behandlingstiderne for indsigtsager.

Læs Datatilsynets afgørelse her:
<https://www.datatilsynet.dk/afgoerelser/afgoerelser/2025/jul/datatilsynet-udtaler-kritik-af-kriminalforsorgen>

Datatilsynet giver Superligaen tilladelse til automatisk ansigtsgenkendelse men ikke klubberne i 1. division

Det danske Datatilsyn (»Datatilsynet«) traf den 16. juli 2025 afgørelse om tilladelse til automatisk ansigtsgenkendelse for fodboldklubberne i henholdsvis Superligaen og 1. division efter § 7, stk. 4 i lovbekendtgørelse nr. 289 af 8. marts 2024 (»den danske lov om databeskyttelse«). Sagen blev afgjort under journalnummer 2024-51-0014.

Sagen omhandlede anmodning om tilladelse til at anvende automatisk ansigtsgenkendelse for alle 12 klubber i Superligaen og alle 12 klubber i 1. division. Datatilsynet meddelte Superligaklubberne tilladelse til automatisk ansigtsgenkendelse i sæsonen 2025/2026. Klubberne i 1. division fik afslag på anmodningen.

Datatilsynet begrundede afslaget til 1. divisionsklubberne med, at der ikke forelå de samme udfordringer med uroligheder ved afviklingen af kampe i 1. division som i Superligaen. Datatilsynet lagde derudover vægt på, at antallet af karantænesager og antallet af tilskuere var markant lavere ved fodboldkampe i 1. division sammenlignet med i Superligaen. I den forbindelse fremhævede Datatilsynet, at behovet for at sikre ro og orden gennem anvendelsen af automatisk ansigtsgenkendelse var større i Superligaen

end i 1. division. Således ville anvendelsen af ansigtsgenkendelsesteknologi ikke stå i rimeligt forhold til formålet. Ifølge Datatilsynet ville behandlingen ikke være nødvendig af hensyn til væsentlige samfundsinteresser, og derfor fik klubberne i 1. division meddelt afslag på anvendelse af automatisk ansigtsgenkendelse.

Læs Datatilsynets afgørelse her:
<https://www.datatilsynet.dk/afgoerelser/afgoerelser/2025/jul/-fodboldklubberne-i-superligaen-faar-til-ladelse-til-brug-af-ansigtsgenkendelse>

Datatilsynet har udtalt alvorlig kritik af tandlægevirksomheds skjulte optagelser

Det danske Datatilsyn (»Datatilsynet«) traf 26. august 2025 afgørelse i en sag vedrørende skjulte lydoptagelser hos en tandlægevirksomhed. Sagen blev afgjort under journalnummer 2024-31-1076.

Klager var ansat hos tandlægevirksomheden, og i ansættelsesperioden foretog tandlægevirksomheden lydoptagelser af samtaler med klager. Klager var ikke informeret om at samtalerne blev optaget. Tandlægevirksomheden oplyste, at der under ansættelsesperioden var kontroverser med klager, og at optagelserne skulle anvendes som dokumentation herfor. Klager lagde efter sin fratrædelse sag an mod tandlægevirksomheden i en ansættelsesretlig retssag.

Datatilsynet vurderede, at tandlægevirksomheden ikke havde et retligt grundlag for optagelserne af klager, da hensynet til at sikre sig mod eventuelle krav i en retssag ikke kunne påberåbes af tandlægevirksomheden som legitim interesse efter GDPR artikel 6, stk. 1, litra f, idet optagelserne af klager var påbegyndt allerede tre år inden, at klager lagde sag an mod tandlægevirksomheden.

Datatilsynet vurderede yderligere, at en arbejdsgivers optagelse af en samtale med en arbejdstager har karakter af en uventet behandling,

og at der på den baggrund skulle have været givet information om lydoptagelsen inden den blev igangsat, hvilket Datatilsynet udledte af princippet om gennemsigtighed i GDPR artikel 5, stk. 1, litra a.

I afgørelsen udtalte Datatilsynet alvorlig kritik af tandlægevirksomhedens behandling af personoplysninger, da de skjulte lydoptagelser af samtalerne ikke havde overholdt GDPR artikel 5, stk. 1, litra a om gennemsigtighed og artikel 6, stk. 1 om retligt grundlag.

Læs Datatilsynets afgørelse her:
<https://www.datatilsynet.dk/afgoerelser/afgoerelser/2025/aug/tandlaegevirksomhed-faar-alvorlig-kritik-for-skjulte-lydoptagelser>

Datatilsynet indleder undersøgelse af Region Hovedstaden i forbindelse med forskningsprojekt

Det danske Datatilsyn (»Datatilsynet«) indledte den 5. september 2025 af egen drift en sag vedrørende et forskningsprojekt i Region Hovedstaden. Sagen opstod i kølvandet på medieomtale af regionens behandling af personoplysninger i forbindelse med et konkret forskningsprojekt, hvor en forsker fra Region Hovedstadens psykiatri fik tilladelse til at anvende personoplysninger fra 3,65 millioner danskers sygehusjournaler til projektet.

Datatilsynet har derfor i en høringskrivelse af 5. september 2025 bedt Region Hovedstaden redegøre for de databeskyttelsesretlige vurderinger, der gik forud for regionens igangsættelse af behandlingen af personoplysninger, herunder hvorvidt der blev foretaget en konsekvensanalyse.

I høringskrivelsen fremgik også Datatilsynets generelle bemærkninger vedrørende konsekvensanalyser. Datatilsynet bemærkede, at konsekvensanalyser er væsentlige retssikkerhedsgarantier for de registrerede og at konsekvensanalyser skal foreligge inden behandlingen af person-

oplysninger påbegyndes. Hvis behandling af personoplysninger påbegyndes, og risikoen for de registreredes rettigheder er høj, vil behandlingen være ulovlig, hvis der ikke er foretaget en konsekvensanalyse inden.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/sep/datatilsynet-indleder-undersogelse-af-regi-on-hovedstaden>

EDPB og EDPS har vedtaget fælles udtalelse vedrørende EU-Kommissionens forslag

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 9. juli 2025, at Det Europæiske Databeskyttelsesråd (»EDPB«) og Den Europæiske Tilsynsførende (»EDPS«) har vedtaget en fælles udtalelse til EU-Kommissionens forslag om at forenkle foranstaltninger for små og mellemstore virksomheder samt for small-cap og mid-cap selskaber.

I udtalelsen fremstår EDPB og EDPS overordnet positive overfor EU-Kommissionens (»Kommissionens«) forslag. Dog fremsætter EDPB og EDPS også en række opfordringer til Kommissionen om tilføjelser og præciseringer af forslaget præampelbetragtninger samt præciseringer af Kommissionens valg af minimumstærskel i forslaget.

Kommissionens forslag indebærer bl.a. indskrænkninger af kravet i GDPR, om at dataansvarlige og databehandlere skal føre en fortegnelse over deres behandlingsaktiviteter. I den forbindelse opfordrer EDPB og EDPS i deres udtalelsen til, at Kommissionen skal præcisere, at grænsen for ikke at skulle føre fortegnelse fastsættes til 750 medarbejdere fremfor for den oprindeligt overvejede grænse på 500 medarbejdere. EDPB og EDPS opfordrer ligeledes til at præcisere, at en fortegnelse kun vil være påkrævet for behandlingsaktiviteter, som sandsynligvis vil resultere i en høj risiko for de registreredes rettig-

heder. Formålet med den opfordrede præcisering er at undgå misforståelsen om, at en fortegnelse vil være påkrævet for alle behandlingsaktiviteter, hvis bare én af behandlingsaktiviteterne sandsynligvis vil resultere i høj risiko for de registreredes rettigheder.

Slutteligt opfordrer EDPB og EDPS i udtalelsen til, at Kommissionen skal indføre begreberne små og mellemstore virksomheder samt small-cap og mid-cap selskaber i GDPR.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/internationalt/internationalt-nyt/2025/jul/edpb-og-edps-vedtager-faelles-udtalelse-om-eu-kommissionens-forslag>

Datatilsynet vil åbne kontor i Grønland

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 19. august 2025, at Datatilsynet vil åbne et kontor i Grønland. Beslutningen om åbningen af et kontor i Grønland kom på baggrund af et stærkt grønlandsk ønske om at styrke vejledningen om databeskyttelse samt på baggrund af den danske regerings beslutning om at justitsområdet i Grønland skal styrkes med 850 mio. kr. Kontoret i Grønland tilføres tre årsværk.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/sep/datatilsynet-vil-aabne-kontor-i-gronland>

Datatilsynet udpeget som tilsynsmyndighed for udvalgte bestemmelser i AI-forordningen

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 22. august 2025, at Datatilsynet er blevet udpeget som tilsynsmyndighed for to bestemmelser i Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13. juni 2024 (»AI-forordningen«). Det drejer sig om AI-forordningens artikel 5, stk. 1, litra d og g, hvor Datatilsynet skal føre tilsyn med reglerne om forbudte former for AI.

Artikel 5, stk. 1, litra d omhandler forbud mod AI-systemer, som anvendes til at vurdere eller forudse risikoen for, at en fysisk person begår en strafbar handling og som alene er baseret på profilering af den fysiske person eller på deres personlighedstræk og personlige egenskaber.

Artikel 5, stk. 1, litra g omhandler forbud mod AI-systemer, som anvendes til biometrisk kategorisering for at udlede race, politisk anskuelse, fagforeningsmedlemskab, religiøs eller filosofisk overbevisning, seksuelle forhold eller seksuel orientering.

Klageadgang og indberetningspligt ved alvorlige hændelser indtræder den 2. august 2026. Indtil da kan Datatilsynet dog indlede sager af egen drift.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/sep/datatilsynet-udpeget-som-tilsynsmyndighed-for-udvalgte-bestemmelser-i-ai-forordningen>

Datatilsynets statistik over brud på persondatasikkerheden er blevet udvidet

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 1. september 2025, at Datatilsynet har udvidet statistikken over anmeldelser af brud på persondatasikkerheden med en mere specificeret opdeling og med et større indblik i utilsigtede hændelser.

Opdateringen indebærer bl.a., at statistikken over brud på persondatasikkerheden i den offentlige sektor nu er inddelt i statslige, regionale og kommunale myndigheder. Derudover er statistikken over utilsigtede hændelser udbygget med flere hændelsestyper.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/sep/datatilsynet-udvider-statistikken-over-brud-paa-persondatasikkerheden>



Illustrasjon: Colourbox.com

Datatilsynet har publiceret råd til borgerne om beskyttelse efter sikkerhedsbrud

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 10. september 2025, at Datatilsynets hjemmeside er blevet opdateret med nye råd til, hvordan borgere kan beskytte sig efter et sikkerhedsbrud.

Datatilsynet har publiceret en række råd om hvad borgere, hvis personoplysninger er blevet ramt af et sikkerhedsbrud, kan gøre for at begrænse risikoen for misbrug, herunder risikoen for phishing, misbrug af kodeord og identitetstyveri. Rådene på Datatilsynets hjemmeside omhandler både kontakt til den relevante virksomhed eller myndighed samt råd til, hvordan borgere selv kan begrænse misbrug.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/sep/saadan-kan-du-beskytte-dig-efter-et-sikkerhedsbrud>

Datatilsynet redegør for retningslinjer for politiske sms'er i forbindelse med valgkampe

Det danske Datatilsyn (»Datatilsynet«) redegjorde den 12. september 2025 for reglerne om politiske partiers brug af personoplysninger under valgkampe i lyset af det forstående kommunalvalg i Danmark den 18. november 2025. Her fremhævede Datatilsynet Europa-Parlamentets og Rådets forordning (EU) 2024/900 af 13. marts 2024 om gennemsigtighed og målretning i forbindelse med politisk reklame (»forordningen om gennemsigtighed og målretning af politisk reklame«), som skal gøre det lettere for borgere at genkende politiske reklamer og identificere afsenderen.

Partierne skal generelt behandle borgernes personoplysninger inden for rammerne af databeskyttelsesreglerne og i den forbindelse sikre, at vælgerne tydeligt informeres om, hvilke personoplysninger der behandles, hvor personoplysningerne stammer fra, og til hvilke formål personoplysningerne anvendes.

Fra den 10. oktober 2025 gælder det yderligere for målrettet politisk onlinereklame, at målretning, f.eks. baseret på alder eller bopæl, kun må ske med vælgerens samtykke efter forordningen om gennemsigtighed og målretning af politisk reklame. Der gælder desuden et forbud mod at målrette onlinereklamer på baggrund af særligt følsomme personoplysninger som politisk eller religiøs overbevisning, fagforeningsmedlemskab, seksualitet eller helbred.

For andre former for politisk reklame, såsom telefonopkald eller husstandsomdeling, gælder databeskyttelsesreglerne fortsat, hvilket betyder, at partierne skal kunne begrunde, hvorfor indsamlingen og anvendelsen af personoplysningerne er nødvendig og vurdere, om deres interesse i at nå vælgerne vejer tungere end hensynet til den enkeltes privatliv.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/sep/politiske-sms%20%80%99er-i-valgkampen-hvad-gælder-for-brugen-af-dine-oplysninger>

Datatilsynets analyse af Østre Landsrets dom om erstatning efter GDPR artikel 82

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 19. september 2025 en analyse af Østre Landsrets dom af 20. august 2025 vedrørende erstatning efter GDPR artikel 82.

Sagen omhandlede en borgers krav om erstatning for immateriel skade efter et databrud. Østre Landsret tilkendte borgeren ret til erstatning på 2.500 kr., efter at borgerens helbredsoplysninger af kommunen ved en fejl blev delt med en tredjepart. Sagen er blevet anket til Højesteret.

Østre Landsret dom er den første dom i Danmark, hvor der er tilkendt erstatning for immateriel skade efter GDPR. Den danske dom skal ses i lyset af EU-domstolens afgørelse i sag C-300/21 fra 4. maj 2023, hvor EU-domstolen fastslog, at erstatning efter GDPR ikke begrænser sig til materiel skade men også omfatter immateriel skade. Herudover fastslog EU-domstolen, at erstatning efter GDPR artikel 82 ikke må være betinget af, at den skade, som den registrerede har lidt, skal have en vis alvorsgrad. Der er således intet minimumskrav for skadens alvorlighed.

Datatilsynet har vurderet, at landsretssagen udgør en væsentlig praksisændring, idet erstatning uden

økonomisk tab ikke hidtil har været tilkendt efter GDPR af en dansk domstol. I hidtidige sager vedrørende erstatning uden økonomisk tab efter GDPR artikel 82 er erstatning blevet afvist med henvisning til krav om kvalificeret skadevirkning, således at skaderne fra databrudet ikke har været af sådan karakter, at der kunne kræves erstatning.

Datatilsynet har vurderet, at afgørelsen, såfremt den stadfæstes af Højesteret, kan medføre omfattende konsekvenser for virksomheder og myndigheder, eksempelvis hvis der anlægges gruppesøgsmål af borgere ramt af samme databrud.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/sep/ny-danske-dom-kan-aendre-praksis-for-erstatning-efter-gdpr>

Datatilsynet advarer om risici ved brug af AI-værktøjer til udformning af henvendelser og klager

Det danske Datatilsyn (»Datatilsynet«) udgav den 22. september 2025 en række anbefalinger om brugen af AI-værktøjer i lyset af at have konstateret en markant stigning i antallet af klager og henvendelser, som helt eller delvist er udarbejdet ved hjælp af kunstig intelligens.

Datatilsynet tilråder, at klager som udgangspunkt udformes med egne ord, således at det tydeligt

fremgår, hvad der klages over. Datatilsynet bemærker endvidere, at klager udarbejdet med hjælp fra AI-værktøjer ofte risikerer at forvride eller forenkle klagens egentlige indhold, hvilket betyder, at anvendelsen af sådanne værktøjer ikke nødvendigvis er en fordel.

Ønsker man trods denne anbefaling at benytte AI-værktøj til at udarbejde en henvendelse, fremhæver Datatilsynet vigtigheden af at undgå, at indtaste fortrolige eller følsomme personoplysninger eller andre oplysninger, som man ikke ønsker videregivet til udbyderen af værktøjet eller tredjemand. Selvom mange udbydere tilbyder en mulighed for at fravælge indsamling af oplysninger til videre træning af systemet, bør brugeren være opmærksom på, at oplysninger alligevel kan blive behandlet og videregivet. Dette skyldes bl.a., at AI-værktøjer ofte er konstrueret på en måde, hvor selv udbyderen eller udvikleren ikke har fuldstændig indsigt i, hvordan systemet internt behandler data.

Læs Datatilsynets anbefalinger her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/sep/flere-klager-til-datatilsynet-udarbejdes-med-ai-vaerktoej>

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



Gorrissen Federspiel

Tue Goldschmieding

Varemærkeret til markedsført vingummibamse »GULDBAMSEN« blev stiftet ved brug

Østre Landsret afsagde den 2. juli 2025 dom i appelsagen BS-5730/2025-OLR vedrørende nægtelse af varemærkeret til vingummibamser.

Appellanten Rigo Trading S.A (»Rigo«) havde indstævnet Ankenævnet for Patenter og Varemærker (»Nævnet«). Nævnet havde under henvisning til manglende særpræg nægtet registrering af Rigos varemærkansøgning til vingummibamse »GULDBAMSEN« for konfekturevarer i klasse 30.

Sagen havde tidligere været behandlet af Sø- og Handelsretten i første instans. Her havde retten vurderet, at der i lyset af væsentlige nyfremkomne oplysninger skulle ske hjemvisning til fornyet behandling. Østre Landsret fandt dog modsat Sø- og Handelsretten, at varemærkeretten til GULDBAMSEN var stiftet ved brug, hvorfor der ikke skulle ske hjemvisning men derimod omgørelse af Nævnets afgørelse, jf. § 3, stk. 1, nr. 3, lov-bekendtgørelse nr. 88 af 29. januar 2019 (»den danske lov om varemærker«).

Landsretten bemærkede i det lys, at Nævnet burde have foretaget en vurdering af, hvorvidt GULDBAMSEN havde fornødent særpræg på tidspunktet, hvor det blev taget

i brug. Landsretten lagde vægt på, at der ikke fandtes tilsvarende produkter da GULDBAMSEN kom på det danske marked, samt at Rigo siden 1978 havde anvendt varemærket i samme form som sin nuværende. Herefter fandt Østre Landsret, at der var stiftet fornødent særpræg ved brug, og at dette særpræg derfor forelå på ansøgningstidspunktet. Herefter ændrede landsretten Sø- og Handelsrettens dom, således at varemærket skulle føres til endelig registrering.

Læs Østre Landsrets dom her: <https://www.domstol.dk/oestrelandsret/aktuelt/2025/7/varemaerkeret-stiftet-ved-brug/>

Østre Landsret ophævede midlertidige forbud og påbud vedrørende sklerose-lægemidler tildelt af Sø- og Handelsretten

Østre Landsret afsagde den 18. juli 2025 kendelse i de sambehandlede kæresager vedrørende ophævelse af midlertidige forbud og påbud rettet mod lægemidler til multipel sklerose. De midlertidige forbud og påbud var blevet pålagt af Sø- og Handelsretten på baggrund af et patent, som retten havde fundet gyldigt. Kæresagerne blev i Østre Landsret behandlet under sagsnumrene BS-13527/2025-OLR, BS-

13836/2025-OLR, BS-16518/2025-OLR og BS-16523/2025-OLR.

Sagsøger var generikaproducenterne Sandoz A/S og Glenmark Pharmaceuticals Nordic AB (»Sagsøger«) mod Biogen International GmbH og Biogen (Denmark) A/S (»Sagsøgte«). Tvisten i sagen drejede sig særligt om gyldigheds-vurderingen af Sagsøgtes patent, og hvorvidt dette kunne danne grundlag for det midlertidige forbud og påbud nedlagt over for Sagsøger. Den Europæiske Patentmyndigheds (»EPO«) indsigelsesafdeling (»Opposition Division«) havde den 11. december 2024 truffet afgørelse vedrørende patentets gyldighed. Patentet blev vurderet ugyldigt i sin oprindelige form, men som følge af Sagsøgtes ændrede dosismængde i aktivstoffet i deres post-publicerede forsøg, fastslog EPO's Opposition Division, at patentet kunne anvendes i begrænset form. Den begrænsede form indebar at patentet kun kunne anvendes til behandling af RRMS fremfor oprindeligt både MS og RRMS.

Østre Landsret fandt, modsat Sø- og Handelsretten, at der var en formodning for at patentet ikke var gyldigt hverken i oprindelig eller i begrænset form. Retten lagde vægt på, at ændringen i dosismængden

skulle fortolkes som en svækket formodning for patentets gyldighed, og at afgørelsen fra EPO's Opposition Division talte i retning af, at patentet også i begrænset form havde en svækket formodning for gyldighed.

I samme ombæring antog landsretten på baggrund af præmisserne i en lignende sag G 2/21 fra EPO's appelinstans (»Technical Boards of Appeal«), at patentet ville være fundet ugyldigt af Technical Boards of Appeal grundet manglende opfindelseshøjde eller utilstrækkelig beskrivelse i tilfælde af en sag ved denne instans. Landsretten vurderede, at de post-publicerede forsøg ikke af Technical Boards of Appeal ville blive fundet tilstrækkelige som bevis for opfindelseshøjde. Det var derfor en retlig fejl, da EPO's Opposition Division havde taget Sagsøgtets post-publicerede forsøg i betragtning i vurderingen af opfindelseshøjde.

Herefter fandt Østre Landsret det ikke sandsynliggjort, at Sagsøgtets patent var gyldigt. Landsretten op hævede følgelig de af Sø- og Handelsretten meddelte midlertidige forbud og påbud, da der ikke længere kunne støttes ret på patentet.

Læs Østre Landsrets kendelse her: <https://www.domstol.dk/oestrelandsret/aktuelt/2025/7/ikke-formodning-for-gyldighed-af-biogens-patent/>

Sø- og Handelsretten frifandt EPC Alternative Source og Forza Fighting Gear i sag om varemærket »FORZA«

Sø- og Handelsretten afsagde den 6. august 2025 dom i sag BS-38012/2021-SHR anlagt af Sports Group Denmark A/S og Victor Rackets Ind. Corp (»Sagsøger«) mod EPC Alternative Source og Forza Fighting Gear BV (»Sagsøgte«) om påstået varemærkekrænkelser.

Retten lagde til grund, at Sagsøger var rettighedsindehavere til det registrerede danske varemærke »FZ FORZA« samt de registrerede

EU-varemærker »FORZA« og »FZ«. Følgelig fremstod Sagsøgtets figurmærker »FORZA«, »FORZA FIGHTING GEAR« og »FORZA SPORTSWEAR« som visuelt identiske og forvekslelige med Sagsøgers varemærker, navnlig da »FORZA« udgjorde den primære bestanddel.

Herefter tog retten stilling til, om Sagsøgtets brug af de nævnte figurmærker ved salg og markedsføring i og til Danmark udgjorde en varemærkekrænkelser og/eller en overtrædelse af lovbekendtgørelse nr. 1420 af 2. december 2024 (»den danske lov om markedsføring«). Retten bemærkede, at selvom Danmark fremstod som leveringsdestination på Sagsøgtets hjemmeside, havde Sagsøgte iværksat foranstaltninger med henblik på at hindre levering, samt at der ikke konkret forelå dokumenterede leverancer til Danmark.

Retten fandt herefter, at valgmuligheden »Danmark« som leveringsdestination ikke alene var tilstrækkelig til at anse markedsføringen som rettet mod Danmark og konstaterede ligeledes, at der i 2018 var indgået en sameksistensaftale vedrørende »FORZA SPORTSWEAR« mellem Sagsøgte og den tidligere ejer af varemærket.

Retten udtalte på den baggrund, at der ikke forelå en krænkelser af Sagsøgers rettigheder efter den danske lov om markedsføring, hvorefter Sagsøgte blev frifundet.

Læs Sø- og Handelsrettens afgørelse her: <https://www.domstol.dk/soeghandelsretten/aktuelt/2025/8/ikke-krænkelser-af-varemærker/>

Kodesproget FLOW tilhørte ikke sagsøger

Sø- og Handelsretten afsagde den 20. august 2025 dom i sag BS-64793/2023-SHR vedrørende en digital fodboldtræningsplatform. Tvisten i sagen omhandlede overdragelse af kodesproget FLOW. Sagens parter var henholdsvis sagsøger SoccerZoom ApS (»Soccer-

Zoom«) og sagsøgte AREA9 INVEST ApS, privatpersonerne A og B, samt Area9 Lyceam ApS (»Area9«).

Den digitale fodboldtræningsplatform var en ophavsretligt beskyttet dataplatform med særskilt web- og appløsning med en licensstruktur udformet som en SaaS-løsning. SoccerZoom var udvikler af platformen, og Area9 var ophavsperson til idéen bag platformen. Platformen var udarbejdet gennem kodesproget FLOW, som var udviklet af Area9.

Retten afviste indledningsvis, at størstedelen af SoccerZooms påstande kunne danne grundlag for en domskonklusion, eftersom de var for brede og uklare. Derudover fulgte det af bevisførelsen, at ikke alle påstandene var tilstrækkeligt aktuelle, eftersom Area9 på loyal vis havde udvist de fornødne bestræbelser på at aflevere det relevante materiale fra platformen, som tilhørte SoccerZoom.

Derudover havde SoccerZoom gjort gældende, at de var blevet ejer af kodesproget FLOW, og at Area9 skulle tilpligtes, at anerkende SoccerZooms ikkeeksklusive, uopsigelige og vederlagsfrie brugsret til kodesproget FLOW. Retten fastslog dog, at eftersom FLOW ikke kunne anses for apportindskudt i SoccerZoom, ligesom der af ejeraftalen til platformen ikke var en oprettelse af licensaftaler mellem parterne, måtte Area9 frifindes for denne påstand. Kodesproget FLOW skulle således ikke overdrages til SoccerZoom, da det ikke tilhørte SoccerZoom.

Dommen er den 2. september 2025 anket til Østre Landsret.

Læs Sø- og Handelsrettens dom her: <https://www.domstol.dk/soeghandelsretten/aktuelt/2025/8/ikke-grundlag-for-erstatning/>

Panelbeslag til lamelvægspanel krænkede patentrettigheder

Sø- og Handelsretten traf den 26. august 2025 afgørelse i sag

BS-15935/2025-SHR vedrørende en mulig krænkelse af patentrettighederne til panelbeslag. Sagen var anlagt af PVH Production A/S (»PVH«) over for Viwa Wood ApS (»Viwa Wood«). Begge parter driver virksomhed med lamelvægspaneler, hvorpå der kan opsættes forskellige typer af beslag til diverse formål.

PVH nedlagde over for retten påstand om forbud og påbud mod at fremstille, udbyde, anvende eller omsætte fire af Viwa Woods panelbeslag. Viwa Wood gjorde de indsigelse imod, at der skulle foreligge krænkelse særligt ved henvisning til sammensætningen af panelbeslagene og monteringsmetoden af panelbeslagene.

Retten fandt dog, at Viva Woods indsigelser ikke var tilstrækkelige til at sandsynliggøre, at der ikke forelå krænkelse. Retten fremhævede bl.a., at det ikke udelukkede krænkelse, at panelbeslaget var sammensat af flere dele end én, da patentet ikke indeholdt krav om én samlet del. Retten lagde ligeledes vægt på, at det ikke udelukkede krænkelse, at Viva Woods monteringsmetode adskilte sig fra PVH. Retten bemærkede i den forbindelse, at eventuel forskellig metode til montering ikke i sig selv kunne føre til, at de herved omstridte træk i patentet ikke var til stede.

Samlet set var det af retten sandsynliggjort, at Viva Woods panelbeslag krænkede PVHs patentrettigheder, og på den baggrund blev Viva Wood af retten meddelt et midlertidigt forbud og påbud.

Kendelsen er kærret til Østre Landsret.

Læs *Sø- og Handelsrettens kendelse* her: <https://www.domstol.dk/soeoghandelsretten/aktuelt/2025/8/forbud-panelbeslag/>

Aevens brug af navnet og varemærket Aeven krænkende ikke Aivens EU-varemærker

Sø- og Handelsretten afsagde den 27. august 2025 dom i sag BS-32501/2024-SHR mellem Aiven Oy

(»Aiven«) og Aeven A/S (»Aeven«) om en påstået krænkelse af Aivens varemærker efter artikel 9 i Europa-Parlamentets og Rådets Forordning (EU) 2017/1001 af 14. juni 2017 (»varemærkeforordningen«).

Aiven havde sagsøgt Aeven med påstand om, at Aeven skulle forbydes at benytte Aeven som navn, varemærke eller forretningskendetegn. Aiven havde siden den 24. august 2018 været indehaver af det registrerede ordmærke AIVEN. Ordmærket var selvopfundet med ingen indholdsmæssig betydning. Aiven udbød cloudbaserede softwareløsninger til virksomhedskunder som Adeo, Wolt og Decathlon.

Aeven offentliggjorde sit navn og varemærke AEVEN den 28. april 2023. Navnet var resultat af en navngivningsproces ledet af et reklamebureau, og ordet havde ingen indholdsmæssig betydning. Aeven udbød hybride cloud-tjenester, digitale arbejdspladser og netværk til kunder som Arla, Forsvaret og Banedanmark.

Retten skulle tage stilling til, om Aeven ved at bruge navnet og varemærket AEVEN havde krænket Aivens varemærkeret til ordmærket AIVEN. Retten fandt på den ene side, at varemærkerne lignede hinanden. Den visuelle forskel i ordenes anden vokal ændrede ikke på vurderingen. Retten lagde dog på den anden side vægt på, at både kunder og tjenesteydelser udbudt af virksomhederne var forskellige. Efter en helhedsvurdering kom retten frem til, at der ikke var risiko for forveksling, jf. varemærkeforordningens artikel 9, stk. 2, litra b, og frifandt derfor Aeven.

Læs *Sø- og Handelsrettens dom* her: <https://www.domstol.dk/soeoghandelsretten/aktuelt/2025/8/ikke-varemaerkekraenkelse/>

Virksomhed politianmeldt for skjult reklame og vildledning om produkttest

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«)

offentliggjorde den 2. juli 2025 at have politianmeldt virksomheden Obsidian Media ApS (»Obsidian Media«) for skjult reklame og for at vildlede om at have testet produkter.

Obsidian Medias hjemmesider gav indtryk af at indeholde uvildige anmeldelser og test af produkter, hvilket ikke var tilfældet, da produkterne aldrig var blevet testet af virksomheden selv. På den baggrund vurderede Forbrugerombudsmanden, at Obsidian Media havde handlet i strid med vildledningsforbuddet i § 5 i lovbekendtgørelse nr. 1420 af 2. december 2024 (»den danske lov om markedsføring«).

I tillæg indeholdt Obsidian Medias hjemmesider *affiliate*-links til andre virksomheders hjemmesider, hvorigennem Obsidian Media fik en indtægt. Der var således tale om reklamelinks. Forbrugerombudsmanden vurderede, at det ikke fremgik klart, at Obsidian Medias hjemmesider byggede på annonceaftaler, og at de dermed fremstod objektive ved at sløre deres kommercielle hensigt. Forbrugerombudsmanden anså derfor hjemmesiderne for skjult reklame i strid med § 6, stk. 4 i den danske lov om markedsføring.

Læs *Forbrugerombudsmandens pressemeddelelse* her: <https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20250702-forbrugerombudsmanden-politianmelder-obsidian-media-aps-for-skjult-reklame-og-vildledning-om-produkttest>

Profil Optik kunne ikke dokumentere, at briller blev fremstillet af plastaffald fra havet

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) indskærpede den 4. juli 2025 vildledningsforbuddet i § 5 og § 6 i lovbekendtgørelse nr. 1420 af 2.

december 2024 (»den danske lov om markedsføring«) overfor den danske optikerkæde Profil Optik.

Profil Optik havde markedsført en brilleserie med udsagn om, at

brillerne var fremstillet af genanvendt plast opsamlet fra havet. Derudover var brillerne blevet markedsført som klimavenlige og bæredygtige. Forbrugerombudsmanden bad Profil Optik om at dokumentere, at det også var tilfældet, jf. dokumentationskravet i den danske lov om markedsføring § 13.

Forbrugerombudsmanden fandt, at det ikke med sikkerhed kunne konstateres, at den plast, som brillerne blev fremstillet af, var blevet opsamlet fra havet. Det fremgik af den fremsendte dokumentation, at plasten kom fra gamle fiskenet, som Profil Optik fik fra en leverandør. Det fremgik dog ikke, hvordan leverandøren havde erhvervet fiskenettene.

Forbrugerombudsmanden vurderede på den baggrund, at markedsføringen kunne vildlede forbrugerne, og at det var vildledende at brillerne blev markedsført som klimavenlige og bæredygtige.

Læs Forbrugerombudsmandens afgørelse her: <https://forbrugerombudsmanden.dk/find-sager/sager/markedsfoeringsloven/2406796-optikerkaede-kunne-ikke-dokumentere-at-briller-blev-fremstillet-af-plastaffald-fra-havet>

Virksomhed kunne ikke lovligt sende markedsføring af skønhedsprodukter til en tidligere kunde baseret på undtagelsen til spamforbuddet

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) traf den 6. august 2025 afgørelse i en sag vedrørende skønhedsprodukter som samlet kategori. Sagen blev behandlet med sagsnummer 25/06966.

Virksomheden ønskede at benytte sig af undtagelsen til spamforbuddet, som findes i § 10, stk. 2, i lovebekendtgørelse nr. 1420 af 2. december 2024 (»den danske lov om markedsføring«), hvorefter en virksomhed kan sende markedsføring til en tidligere kunde uden forudgående samtykke. Spørgsmålet i sagen var om markedsføring af skønhedsprodukter kunne anses for

at være tilsvarende produkter, da dette er en betingelse for at kunne omfattes af undtagelsen til spamforbuddet.

Forbrugerombudsmanden vurderede, at markedsføringen af skønhedsprodukter bredt set ikke kunne anses som tilsvarende produkter, da virksomhedens produktortiment bestod af flere forskellige kategorier af skønhedsprodukter. Forbrugerombudsmanden udtalte, at kategorierne af skønhedsprodukter, såsom hårprodukter, parfume eller makeup, adskilte sig for meget fra hinanden til at kunne anses som tilsvarende produkter.

Virksomheden kunne derfor ikke anvende undtagelsen til spamforbuddet med henblik på markedsføring til tidligere kunder uden fornyet samtykke.

Læs Forbrugerombudsmandens afgørelse her: <https://forbrugerombudsmanden.dk/find-sager/sager/markedsfoeringsloven/2506966-en-virksomhed-kunne-ikke-lovligt-ende-markedsfoering-af-skoenhedsprodukter-til-en-tidligere-kunde-baseret-paa-undtagelsen-til-spamforbuddet>

NPV A/S lovede for mange kvadratmeter i projektbyggeri og skulle betale bøde på en kvart million kroner

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 5. september 2025, at ejendomsudvikleren NPV A/S (»NPV«) havde givet vildledende oplysninger om antal kvadratmeter i forbindelse med markedsføring af projektbyggeriet Strandgården på Amager.

Forbrugerombudsmanden politianmeldte sagen mod NPV i 2018 under sagsnummeret 18/05421. Der er herefter blevet afsagt dom af Østre Landsret.

NPV havde angivet arealerne for de enkelte rum på plantegningen men også medregnet arealet af vægge og mure i arealangivelsen. Det angivne areal svarede derfor til det samlede tinglyste areal men ikke til

det reelle areal af de færdige lejligheder. Landsretten bemærkede, at arealangivelserne resulterede i væsentlige arealforskelle fra salgsbrochuren til den færdige lejlighed. På den baggrund vurderede retten, at det var vildledende at benytte disse arealangivelser i plantegningen, jf. § 5 i lovebekendtgørelse nr. 1420 af 2. december 2024 (»den danske lov om markedsføring«).

Landsretten fandt det dog ikke tilstrækkeligt bevist, at potentielle købere blev vildledt om lejlighedernes størrelse på Strandgårdens hjemmeside ved brug af ordet »nettoareal« om det tinglyste areal.

Bøden blev fastsat til 500.000 kr. under hensyn til overtrædelsens grovhed, omfang og de tilsigtede økonomiske konsekvens, men bøden blev på grund af lang sagsbehandlingstid nedsat til 250.000 kr.

Læs Forbrugerombudsmandens pressemeddelelse her: <https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/resmeddelelser/2025/20250905-dom-ejendomsudvikler-lovede-for-mange-kvadratmeter-i-projektbyggeri-og-skal-betale-boede-paa-en-kvart-million-kroner>

Både annoncør og annonceplatform var ansvarlige for vildledende udsagn om kræft

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) vurderede den 10. september 2024 et markedsføringsudsagn om koblingen mellem indeklimatjek og kræft som ulovlig efter § 3 og § 5 i lovebekendtgørelse nr. 1420 af 2. december 2024 (»den danske lov om markedsføring«) om god markedsføringsskik og forbud mod vildledning.

Forbrugerombudsmanden fandt, at annonceteksten »TJEK DIT INDEKLIMA OG UNDGA KRÆFT« fra virksomheden Radon-Danmark (Kjær Hansen ApS) (»RadonDanmark«), publiceret på Bownty ApS' annonceplatform bownty.dk (»Bownty«), var i strid med både vildledningsforbuddet og

god markedsføringsskik. Annonceplatformen Bownty havde et medansvar for markedsføringen, særligt fordi de havde udarbejdet den i samarbejde med annoncøren.

Virksomhederne kunne ikke dokumentere, at man ved et tjek af indeklimaet kunne undgå kræft, hvorfor det var Forbrugerombudsmandens vurdering, at udsagnet var vildledende. Forbrugerombudsmanden bemærkede, at radonpåvirkning ifølge den danske Sundhedsstyrelse udgjorde én af flere faktorer i at udvikle kræft, hvorfor man ikke kunne slutte, at man ved et indeklimatjek kunne undgå kræft. Derudover spillede udsagnet på frygt hos forbrugeren om udviklingen af kræft, hvis der ikke blev foretaget et indeklimatjek. Udsagnet var derfor også i strid med god markedsføringsskik.

Læs Forbrugerombudsmandens pressemeddelelse her: <https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20250910-annoncoer-og-annonceplatform-overtraadte-markedsfoeringsloven-med-udsagn-om-kræft>

Forbrugerombudsmanden anker dom om Jyske Banks opkrævning af negative renter

Den danske forbrugerombudsmand (»Forbrugerombudsmanden») offentliggjorde den 12. september 2025, at den har anket Sø- og Handelsrettens dom i sagen mod Jyske Bank om negative renter til Højesteret. Sø- og Handelsretten frifandt Jyske Bank for at have opkrævet negative renter på privatkunders konti.

Forbrugerombudsmanden er uenige i rettens fortolkning af den danske forbrugeraftalelovgivning. Forbrugerombudsmanden anser sagen for principiel for så vidt angår spørgsmålet om, hvor præcist en bank skal beskrive mulighederne for at ændre i dets aftaler med kunderne uden sidstnævntes accept, herunder at kunne indføre og opkræve negative renter.

Forbrugerombudsmanden vil derudover anmode Højesteret om at få en præjudiciel forelæggelse for EU-domstolen. Forbrugerombudsmanden har i sin pressemeddelelse henvist til fire domme afsagt af den tyske højesteret, som omhandlede lignende spørgsmål om bankaftaler, og hvor bankernes opkrævning af negative renter blev fundet ugyldige. Forbrugerombudsmanden finder de tyske domme relevante for anken, da de tyske domme er afsagt ud fra den tyske implementeringslov af samme EU-direktiv, som er implementeret i den danske forbrugeraftalelovgivning.

Læs Forbrugerombudsmandens pressemeddelelse her: <https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20250912-forbrugerombudsmanden-anker-dom-om-negative-renter>

Væsensforskel mellem forbrugeropfattelse og den faktiske bæredygtighed førte til politianmeldelse over brug af bæredygtighedsudsagn

Den danske forbrugerombudsmand (»Forbrugerombudsmanden») politianmeldte den 16. september 2025 Salling Group A/S (»Salling Group»), der står bag detailhandelskæden Netto, for vildledende markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»den danske lov om markedsføring») § 5 og § 6.

Politianmeldelsen skete som følge af Sallings bæredygtighedsudsagn i forbindelse med markedsføring af Nettos økologiske produktlinje »ØGO«. Konkret havde Salling Group fremhævet Nettos »ØGO« som det fjerde mest bæredygtige mærke i Danmark. Forbrugerombudsmanden bemærkede, at dette udsagn imidlertid var baseret på en privat spørgeundersøgelse af forbrugernes opfattelse af det nævnte mærke, og at det ikke var et udtryk for den reelle klima- og miljøbelastning af ØGO-produkter.

Sagen er Forbrugerombudsmandens tredje sag på tre år om Salling Groups brug af vildledende bæredygtighedsudsagn i deres markedsføring.

Læs Forbrugerombudsmandens pressemeddelelse her: <https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20250916-forbrugerombudsmanden-politianmelder-salling-group-for-vildledende-baeredygtighedsudsagn-om-nettos-oego-mærke>

Mærker uden kriterier for anvendelse vildledte forbrugerne

Den danske forbrugerombudsmand (»Forbrugerombudsmanden») offentliggjorde den 18. september 2025, at virksomheden Makeitmedia havde overtrådt vildledningsforbudet i § 5 og § 6 i lovbekendtgørelse nr. 1420 af 2. december 2024 (»den danske lov om markedsføring») ved at markedsføre mærker uden indhold.

Virksomheden Makeitmedia havde markedsført og solgt mærker til at indsætte på hjemmesider uden kriterier eller kontrol med anvendelsen af mærket. Således havde hjemmesidernes købte mærker reelt ikke noget indhold. Makeitmedia tilbød blandet andet et CSR-mærke, et Sundt Arbejdsmiljø-mærke, et Stop Papirspild-mærke og et Sikkerhedsmærke.

Forbrugerombudsmanden vurderede, at Makeitmedias mærker blev markedsført på en måde, som var egnet til at give forbrugeren indtryk af, at virksomheden adskilte sig positivt fra andre virksomheder, men da dette ikke var tilfældet, var mærkerne vildledende for forbrugeren.

Forbrugerombudsmanden fremhævede derudover, at Sikkerhedsmærket dog havde et kriterie for anvendelse, hvilket var et SSL-certifikat, men da et SSL-certifikat er en sædvanlig standard for branchen, må det ikke markedsføres som noget særligt. Gennem brugen af sikkerhedsmærket, blev SSL-certifika-

ter fremhævet som noget særligt, og sikkerhedsmærket var derfor vildledende.

Forbrugerombudsmanden har indskærpet reglerne om vildledende markedsføring overfor virksomheden, og Makeitmedia har lukket deres syv hjemmesider, som solgte mærkerne.

Læs Forbrugerombudsmandens pressemeddelelse her: <https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20250917-maerker-uden-indhold-vildleder-forbrugerne>

Forbrugerombudsmandens årsberetning for 2024

Den 15. september 2025 har den danske forbrugerombudsmand (»Forbrugerombudsmanden«) udgivet årsberetningen for 2024. Årsberetningerne er et indblik i, hvad Forbrugerombudsmanden har beskæftiget sig med i det forgangne år. I 2024 har særlige indsatsområder været; uretmæssig markedsføring i form af vildledende bæredygtighedsudsagn (»greenwashing«), internationalt samarbejde samt influenceres markedsføring over for børn og unge.

Læs Forbrugerombudsmandens pressemeddelelse her: <https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20250915-forbrugerombudsmandens-aarsberetning-2024-stor-arbejdsindsats-paa-det-groenne-omraade>

Læs Forbrugerombudsmandens årsberetning for 2024 her: <https://forbrugerombudsmanden.dk/media/bltmetpg/forbrugerombudsmandens-aarsberetning-2024-wa.pdf>

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



Illustrasjon: Colourbox.com



Bird & Bird

Beatrice Rälg

SOU 2025:100 – Åtgärder mot illegal IP-TV

Sammanfattning

SOU 2025:100 föreslår en modernisering av regelverket mot illegal ip-tv-verksamhet och anpassar lagstiftningen till dagens tekniska och marknadsmässiga verklighet. Genom att kombinera förtydligande lagändringar med strategiska åtgärder och myndighetsuppdrag adresseras både legalitet och hanterbarhet. Nyckelfrågor framåt blir genomförandet, myndigheter och aktörers samverkan samt balanseringen mellan effektivitet och rättssäkerhet med beaktande av grundläggande fri- och rättigheter.

Bakgrund

Regeringen beslutade den 25 januari 2024 att tillsätta Filmutredningen för att se över den nationella filmpolitiken och föreslå åtgärder mot illegal internetprotokoll-tv ("ip-tv"). Betänkandet "Åtgärder mot illegal ip-tv" (SOU 2025:100) överlämnades i september 2025. Utredningen har haft i uppdrag att beskriva hur innehållet i ip-tv som tillhandahålls utan tillstånd från berörda rättighetshavare görs åtkomligt och distribueras samt analysera hur sådan ip-tv påverkar den svenska film- och tv-branschen, analysera behovet av och förutsättningarna för ett förbud för privatpersoner att ta emot sådan ip-tv och föreslå hur ett förbud bör utformas, samt vid behov föreslå andra åtgärder för att motverka distributionen.

Utredningens bedömning och författningsförslag

Utredningen konstaterar att olovlig ip-tv utgör ett betydande problem genom omfattande intäkter till organiserad brottslighet, negativ påverkan på rättighetshavare, hot mot finansiering av film, tv och idrott samt minskade skatteeffekter. Utredningen föreslår därför ändring i lagen (2000:171) om förbud beträffande viss avkodningsutrustning, vars namn föreslås ändras till «Lag om förbud beträffande viss utrustning för obehörig tillgång till skyddade medietjänster».

Bland annat föreslås införandet av en ny bestämmelse som innebär att mål och ärenden enligt lagen ska handläggas av Patent- och marknadsdomstolen. Därutöver föreslås att straffskalan skärps och brott mot § 5 första stycket ska medföra böter eller fängelse upp till två år. Om brottet är grovt ska fängelse i lägst sex månader och högst sex år dömas ut. Parallellt föreslås ändring i lagen (2016:188) om patent- och marknadsdomstolar för att klargöra att PMD är behörig domstol för mål enligt den ändrade lagen.

Utredningen föreslår vidare att det införs ett förbud för privatpersoner att använda illegala ip-tv-tjänster. Myndigheter såsom Skatteverket, Polismyndigheten och Post- och telestyrelsen ska få särskilda uppdrag för arbetet mot illegal ip-tv. Reger-

ingen bör enligt utredningen initiera branschsamverkan för frivilliga åtgärder, exempelvis att hindra betalningar till återförsäljare och att sökmotorer tar bort eller nedprioriterar länkar till olagliga tjänster. Vidare bör en särskild utredning av möjligheterna till live-blockering, det vill säga snabb blockering under pågående evenemang, genomföras.

Förslaget innebär att användningen av utrustning eller tjänster för obehörig tillgång till skyddade medietjänster görs tydligare straffbar. Lagen bekräftar att det inte behöver ske traditionell avkodning, utan definitionen blir teknikneutral. Detta utgör en harmonisering mot faktisk teknik och brottsutveckling.

Utredningen pekar på att den exakta förlusten för rättighetshavare är svår att kvantifiera, men att det finns en tydlig påverkan på marknaden för hur film, tv och sport finansieras. Den föreslagna lagstiftningen och myndighetsåtgärderna syftar därför till att stärka den legala marknadens villkor. Lagändringarna föreslås träda i kraft den 1 juli 2026.

Se betänkandet i dess helhet här: Åtgärder mot illegal ip-tv, SOU 2025:100

Beatrice Rälg är biträdande jurist på Bird & Bird Advokatbyrå i Stockholm. Jag har en bakgrund inom immaterialrätt och kommersiell tvistlösning och arbetar idag huvudsakligen med IP-rättsliga frågor.



Gorrissen Federspiel

Tue Goldschmieding

Regeringen vil fremsætte lovforslag om forbud mod deepfakes

Den danske regering og en bred del af partierne i det danske Folketing har indgået en aftale om stærkere beskyttelse mod virkelighedsnære digitalt genererede efterligninger (»Deepfakes«). På den baggrund har det danske Kulturministerium (»Kulturministeriet«) udarbejdet et udkast til lovforslag med henblik på at kunne fremsætte lovforslaget for det danske Folketing i vinteren 2025/2026.

I udkastet til lovforslag bliver det foreslået at indsætte to nye bestemmelser i lovebekendtgørelse nr. 1144 af 23. oktober 2014 (»den danske

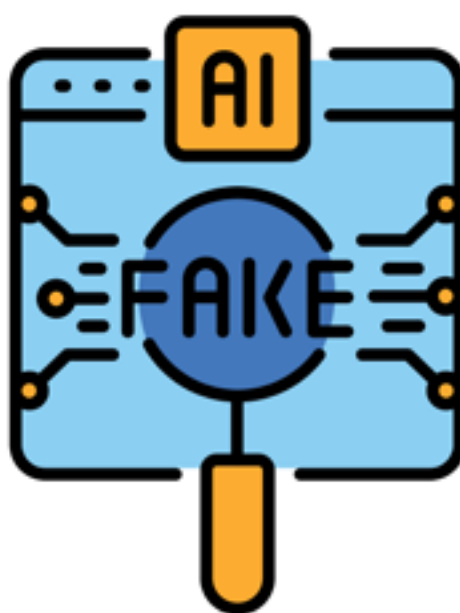
lov om ophavsret«). Den ene bestemmelse skal udgøre en generel beskyttelse mod deepfakes af personlige kendetegn. Denne bestemmelse vil omfatte den brede befolkning og beskytte mod deling af personers udseende, stemme og lignende uden den efterlignede persons samtykke.

Den anden bestemmelse skal indeholde en efterligningsbeskyttelse af udøvende kunstnere og artister. Denne bestemmelse omhandler et forbud mod deepfakes som efterligner kunstneriske præstationer uden kunstnerens samtykke.

Kulturministeriet har sendt udkastet til lovforslag i høring. Høringsfristen var 21. august 2025. I udkastet til lovforslag er ikrafttrædelsesdatoen for loven, hvis den vedtages, sat til den 31. marts 2026.

Læs Kulturministeriets høringsbrev samt udkast til lovforslag på høringsportalen: <https://boeringsportalen.dk/Hearing/Details/70269>

Tue Goldschmieding, partner i Gorrissen Federspiel og dansk redaktør for Lov & Data.



Illustrasjon: Colourbox.com

