Lov & Data

Mars 2025
Nr. 161 1/2025

Innhold













Lov & Data er et nordisk tidsskrift for rettsinformatikk og utgis av

Lovdata
Postboks 6688 St. Olavs plass
NO-0129 Oslo, Norge
Tlf.: +47 23 11 83 00
E-post: lovogdata@lovdata.no
Nettside: www.lod.lovdata.no
Alias: www.lovogdata.no
www.lawanddata.no

Elektronisk: ISSN 1503-8289
Utkommer med 4 nummer pr. år.

Lov & Data er medlemsblad for foreningene Norsk forening for Jus og EDB, Dansk forening for Persondataret, Danske IT-advokater, Svenska föreningen för IT och juridik (SIJU) og Finnish IT Law Association.

Fra 2024 er Lov & Data kun tilgjengelig på nett, lod.lovdata.no.

Lov & Data

Trykk og layout: Aksell AS

Miljøfyrtårn SERTIFISERT VIRKSOMHET

Leder

Tue Goldschmieding

Pseudonymisering af personoplysninger har altid været en væsentlig foranstaltning i beskyttelsen af behandlingssikkerheden. Betydningen af effektiv pseudonymisering af personoplysninger er gennem de seneste år kun vokset i takt med introduktionen af AI og big data analyse, hvor behandling af store mængder data er afgørende, og som konsekvens af behovet for supplerende foranstaltninger i forbindelse med tredjelandsoverførsler.

Som det også gør sig gældende med anonymisering, har pseudonymisering for mange virksomheder og organisationer været set som vejen til at realisere den brug af data, der ellers forekom umulig inden for rammerne af GDPR.

SRB-afgørelsen

Derfor var der også mange, der med glæde noterede sig Rettens afgørelse den 26. april 2023 i sagen T-557/20, som omhandlede omstruktureringen af Banco Popular under tilsyn af Den Fælles Afviklingsinstans (SRB). I denne sag blev Deloitte udpeget af SRB til at bistå i en høringsproces med berørte kreditorer og aktionærer. SRB tildelte en unik kode til hver kommentar modtaget i processen, og delte et begrænset datasæt med Deloitte, som kun SRB kunne forbinde til de berørte kreditorer.

Nogle kreditorer og aktionærer klagede til Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) over, at SRB ikke havde informeret dem om, at deres personoplysninger kunne blive delt med tredjeparter som Deloitte. EDPS var enig i klagen, men SRB appellerede afgørelsen til Domstolen. Domstolen fastslog, at for at vurdere, om dataene var effektivt anonymiserede, skulle man overveje de identificeringsmidler, der med rimelighed kunne anvendes af både dataansvarlige og andre parter, i tråd med CJEU's afgørelse i Patrick Breyer-sagen (C-582/14). Retten bemærkede også, at man skulle vurdere, om Deloitte havde de juridiske midler til rådighed, der i praksis ville gøre det muligt at få adgang til de nødvendige oplysninger for at reidentificere forfatterne af kommentarerne.

Selv om afgørelsen er blevet appelleret af EDPS til Den Europæiske Unions Domstol (CJEU), var der mange, der så en mulighed i pseudonymisering som vejen til at opnå en mere fleksibel brug og deling af data.

EDPB's nye retningslinjer

Det Europæiske Databeskyttelsesråd (EDPB) vedtog den 16. januar 2025 nye retningslinjer for pseudonymisering. Retningslinjerne præciserer, at pseudonymisering indebærer behandling af personoplysninger, så de ikke kan henføres til en specifik person uden supplerende oplysninger, som skal opbevares separat og sikkert. Retningslinjerne opdeler dette i tre komponenter: muligheden for at henføre oplysninger, brugen af supplerende oplysninger og adskillelsen af supplerende oplysninger ved tekniske og organisatoriske foranstaltninger.

EDPB cementerer endvidere, at pseudonymiserede personoplysninger, som kan henføres til en person ved brug af supplerende oplysninger, forbliver oplysninger om en identificerbar fysisk person og er derfor stadig personoplysninger, herunder hvis oplysningerne kan henføres til en person af den dataansvarlige.

Det er således svært ikke at læse retningslinjerne som et indspark i den verserende SRB-sag og et opgør med Rettens betragtninger om, at henførbarheden af personoplysninger skal vurderes subjektivt ud fra modtagerens mulighed for at reidentificere datasubjektet.

Retningslinjerne understreger dog væsentligheden af pseudonymisering som foranstaltning, og hvordan dataansvarlige kan benytte pseudonymisering som en teknisk og organisatorisk foranstaltning til at opfylde kravene om dataminimering og sikre balancen mellem datasubjekternes rettigheder og den dataansvarliges legitime interesser.

Retningslinjerne er dog ikke uden udfordringer, især for små og mellemstore virksomheder. For mange virksomheder kan det være en udfordring at forstå de tekniske aspekter af de anbefalede pseudonymiseringsteknikker og implementere disse teknikker.

Illustrasjon: Colourbox.com

Retningslinjerne kræver, at virksomhederne foretager en grundig risikovurdering og vælger passende tekniske og organisatoriske foranstaltninger for at sikre, at pseudonymiserede data ikke kan henføres til enkeltpersoner. Dette betyder, at virksomhederne skal have en detaljeret forståelse af alle aktører inden for pseudonymiseringsdomænet og forstå de retslige og tekniske midler, som aktørerne har til rådighed og vil kunne anvende til at reidentificere datasubjekter.

Retningslinjerne indeholder også en række eksempler, der illustrerer anvendelsen af pseudonymisering i forskellige sektorer, såsom medicinsk forskning og markedsføring.

Kompleksiteten i retningslinjerne rejser dog spørgsmål om, hvorvidt små og mellemstore virksomheder har de nødvendige kapaciteter til at implementere de anbefalede teknikker og foretage de risikovurderinger, der er nødvendige i brugen af pseudonymiseringsteknikker.

Det kan dog konkluderes, at EDPB med retningslinjerne understreger betydningen af pseudonymisering som en væsentlig foranstaltning der kan hjælpe dataansvarlige til at opfylde flere krav under Databeskyttelsesforordningen. For databeskyttelsesjuristen er pseudonymisering derfor også et vigtigt værktøj i værktøjskassen og en teknisk disciplin, der er nødvendig at mestre.

Tue Goldschmieding

Supplerende rettsgrunnlag for behandling av særlige kategorier av personopplysninger – En analyse av KI-forordningens artikkel 10 (5)

Av Håvard Sveier Ottemo

1. Innledning

Denne artikkelen belyser spørsmålet om kravene KI-forordningen setter til supplerende rettsgrunnlag for behandling av særlige kategorier av personopplysninger, er hensiktsmessig utformet med tanke på det eksisterende personvernregelverket.[1] Temaet er særlig relevant i lys av den voldsomme utviklingen som har funnet sted på både personvern- og KI-rettsfeltet de siste årene. Krysningspunktet, reguleringen og den medfølgende samhandlingen mellom disse forordningene er derfor av interesse.

Faren for uheldige regulatoriske overlapp i EU-retten, herunder mellom GDPR og KI-forordningen, er påpekt som et underliggende systematisk problem i Mario Draghis rapport om europeisk konkuranseevne. Han har i lys av dette tatt til orde for å finne og fjerne disse overlappene.[2]

Håvard Sveier Ottemo

Slike regulatoriske overlapp skaper utfordringer for europeiske virksomheter, uten at de nødvendigvis er formålstjenlige for å styrke borgernes fundamentale rettigheter i nevneverdig grad.

> Slike regulatoriske overlapp skaper utfordringer for europeiske virksomheter, uten at de nødvendigvis er formålstjenlige for å styrke borgernes fundamentale rettigheter i nevneverdig grad.

Det kan dermed være nyttig å sette enkelte lovbestemmelser under lupen for å se om KI-forordningen er utformet uten disse unødvendige overlappene. For å utforske dette vil artikkelen systematisk gjennomgå KI-forordningen artikkel 10 (5) i lys av kravene som stilles til supplerende rettsgrunnlag i GDPR artikkel 9 (2) bokstav g. Hva et supplerende rettsgrunnlag er, og hvilke krav som stilles til det, vil gjennomgås først.

2. GDPR artikkel 9 (2) bokstav g – Supplerende rettsgrunnlag

Utgangspunktet etter GDPR er at dersom man ønsker å behandle særlige kategorier av personopplysninger, trenger man et rettsgrunnlag i tillegg til et behandlingsgrunnlag etter GDPR artikkel 6.[3] Et slikt rettsgrunnlag må hjemles i et unntak etter GDPR artikkel 9 (2), ettersom særlige kategorier etter første ledd er forbudt å behandle.

Et av disse rettsgrunnlagene er GDPR artikkel 9 (2) bokstav g, som kan benyttes når:

> *«Behandlingen er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern*

1 Denne artikkelen er en komprimert utgave av min masteroppgave om tilsvarende tema. Det supplerende rettsgrunnlaget i KI-forordningen artikkel 59 vil ikke bli problematisert i denne artikkelen, men kan leses om i Ottemo (2024).

2 Europakommisjonen, «The future of European competitiveness Part B | In-depth analysis and recommendations», *Europakommisjonen*, 9. september 2024, s. 79 [Tilgjengelig: *https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf*] (lest 27.11.2024).

3 Skullerud mfl. (2023), Artikkel 9. Behandling av særlige kategorier av personopplysninger, Juridika [Tilgjengelig: https://juridika.no/no/lov/2016-04-27-679/%C2%A79/kommentar/] (lest 22.10.2024).

av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser»

Behandlingen må skje «på grunnlag av unionsretten eller [nasjonal] rett». En slik ytterligere behandlingshjemmel omtales som et *supplerende rettsgrunnlag*. At det supplerende rettsgrunnlaget må «sikre egnede og særlige tiltak» for å «verne den registrertes grunnleggende rettigheter og interesser», stiller krav til rettsgrunnlagets kvalitative innhold. At hjemmelen skal sikre «særlige tiltak» (EN: «specific measures») innebærer at den må gi mer informasjon om og konkretisere hvilke tiltak som skal til for å «verne den registrertes grunnleggende rettigheter og interesser».

Kravet om «særlige tiltak» innebærer derfor at rettsgrunnlaget må være mer tilpasset typesituasjonen enn de generelle tiltakene GDPR pålegger. De generelle kravene til behandlingen etter GDPR gjelder nemlig uansett,[4] og det supplerende rettsgrunnlaget hadde vært overflødig hvis det ikke tilføyde noe nytt. Har ikke det supplerende rettsgrunnlaget tiltak som er «egnede og særlige», så kan det dermed ikke gi grunnlag for behandling etter GDPR artikkel 9 (2) bokstav g.

3. KI-forordningen artikkel 10 (5)

KI-forordningen artikkel 10 tar for seg hvordan høyrisiko KI-systemer skal trenes på data. For at treningen av et høyrisiko KI-system skal anses lovlig etter KI-forordningen artikkel 10 (1), er det nødvendig å etterleve en rekke kvalitetskrav som oppstilles i resten av bestemmelsen. Et av disse er å luke ut «bias» – skjevheter – gjennom skjevhetsoppdagelse og -korreksjon etter KI-forordningen artikkel 10 (2) bokstav f og g.

KI-forordningen definerer ikke begrepet «bias», men ordlyden kan tilsi at det er tale om en underliggende forutinntatt mening, fordel eller ulempe som negativt eller positivt kan påvirke enkeltindivider eller grupper på urettferdig vis.[5] Slike skjevheter oppstår typisk på grunn av mangler og svakheter med datasettene brukt ved trening av et KI-system.[6]

KI-forordningen artikkel 10 (5) fastsetter at dersom det er «strictly necessary» for å sikre «bias detection and correction» i høyrisiko KI-systemer etter KI-forordningen artikkel 10 (2) bokstav f og g, kan leverandører[7] av slike systemer «exceptionally» behandle særlige kategorier av personopplysninger, såfremt dette skjer med nødvendige garantier for fysiske personers grunnleggende rettigheter og friheter.[8] Dette er da et supplerende rettsgrunnlag myntet på GDPR artikkel 9 (2) bokstav g.[9] Formålet med å gi KI-forordningen artikkel 10 (5) et slikt supplerende rettsgrunnlag er å gjøre det enklere å motkjempe diskriminering som følger av slike skjevheter i høyrisiko KI-systemer.[10]

For å benytte seg av dette supplerende rettsgrunnlaget må leverandøren oppfylle en rekke særskilte vilkår, *i tillegg til* å etterleve kravene i GDPR.[11] I det følgende vil disse særskilte vilkårene gjennomgås og analyseres for å se om de oppfyller kravene som stilles til supplerende rettsgrunnlag som nevnt i punkt 2 – altså, om de utgjør «egnede og særlige tiltak».

4. Gjennomgang av tiltakene etter artikkel 10 (5)

4.1. Nødvendighetsvilkåret

Det første tiltaket fastsettes i artikkel 10 (5) bokstav a, hvor det stilles krav om at:

> *«[T]he bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymised data»*

Tiltaket fremstår som overflødig. Det følger allerede av dataminimeringsprinsippet nedfelt i GDPR artikkel 5 (1) bokstav c at behandlingen skal være «begrenset til det som er nødvendig for formålene de behandles for».[12] Dette legges til grunn i GDPR fortalepunkt 39, hvor det fremgår at «[p]ersonopplysninger bør [bare] behandles […] dersom formålet med behandlingen ikke med rimelighet kan oppfylles på annen måte».

Den behandlingsansvarlige må da begrense seg til å behandle de personopplysningene som er nødvendige for å oppnå formålene med behandlingen. Alternativt – dersom det ikke er nødvendig – ikke behandle *noen* personopplysninger.[13] Å skille ut dette som et eget selvstendig tilleggsvilkår[14], som skal hensyntas utover det som følger av GDPR, utgjør dermed ikke et særlig tiltak.

4.2. Sikkerhets- og privatlivsbeskyttende tiltak

Det andre tiltaket fastsettes i artikkel 10 (5) bokstav b:

> *«[T]he special categories of personal data are subject to technical limitations on the re-use of the personal data, and state-of-the-art security and privacy-*

4 Foruten GDPRs lovsystematikk, følger dette også av KI-forordningen fortalepunkt 140.

5 Tolkningen er inspirert av Bekkum (2024), s. 8–9.

6 Ibid. s. 9.

7 KI-forordningen artikkel 3 (3) i betydningen «deployer».

8 KI-forordningen artikkel 10 (5).

9 Lagt eksplisitt til grunn i KI-forordningen fortalepunkt 70.

10 KI-forordningen fortalepunkt 70.

11 Betydningen av at disse utskilles som egne selvstendige tilleggsvilkår problematiseres i Ottemo (2024).

12 Se også GDPR fortalepunkt 39.

13 EDPB – Retningslinje 04/2019, avsnitt 76.

14 Se Ottemo (2024) punkt 4.2.1 og 4.2.8 for mer om bakgrunnen og konsekvensen av utskillingen av disse vilkårene som tilleggsvilkår.

preserving measures, including pseudonymisation»[15]

Lignende, etter GDPR artikkel 32 (1), skal den behandlingsansvarlige og databehandleren «gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen», idet det hensyntas «den tekniske utviklingen».

Den vide ordlyden «egnede tekniske og organisatoriske tiltak» hensyntatt «den tekniske utviklingen» (EN: «state of the art») i GDPR artikkel 32 (1) fanger opp KI-forordningens artikkel 10 (5) bokstav b «state-of-the-art security and privacy-preserving measures». Mens vilkårene i KI-forordningen er absolutte, har GDPR en risikobasert tilnærming, hvor hva som er «egnet» relativiseres ut ifra risikoen. Etter GDPR er det klart at det er den behandlingsansvarlige og databehandleren som selv må finne de tiltakene som er egnet for å avbøte risikoen.[16]

EU-domstolen har påpekt at vurderingen av om et tiltak er egnet er todelt. Det er først nødvendig å «[…] identify the risks of a personal data breach caused by the processing concerned and their possible consequences for the rights and freedoms of natural persons», for så å «[…] ascertain whether the measures implemented by the controller are appropriate to those risks, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of that processing».[17]

Særlige kategorier av personopplysninger vil av sin sensitive art kreve en høyere grad av beskyttelse,[18] og da særlig i konteksten trening av høyrisiko KI-systemer. Slike KI-systemer utgjør i utgangspunktet og per definisjon nettopp en stor risiko for individers fundamentale rettigheter.[19] Det vil dermed stilles strenge krav etter GDPR før et sikkerhets- og privatlivsbeskyttende tiltak etter GDPR artikkel 32 (1) i en KI-forordning-artikkel 10 (5)-situasjon kan anses som «egnet».

Mens KI-forordningen ikke sier *hva* standarden er, henviser den likevel til hva som er «state-of-the-art» innenfor sikkerhets- og privatlivsbeskyttende tiltak. Dette fremstår intetsigende og gir lite veiledning. Hva som til enhver tid er det absolutte «state-of-the-art» av tiltak, vil variere og være vanskelig å stadfeste. Ordlyden oppsetter dermed et absolutt, men et innholdsmessig ukjent krav.

Etter GDPR artikkel 32 (1) skal hva som er «state of the art» tilsvarende hensyntas ved iverksetting av tiltak. Her spesifiseres det imidlertid at sikkerhetsnivået som oppnås ved dette skal være «egnet». Dette gir den behandlingsansvarlige og databehandlere et spillerom for hvilke tiltak som skal iverksettes.[20] Som EDPB har påpekt, er «state of the art»-begrepet etter GDPR «[…] a dynamic concept that cannot be statically defined at a fixed point in time, but should be assessed *continuously* in the context of technological progress».[21] Artikkel 32 (1) setter videre krav til tiltak som må iverksettes, ikke et resultat som må oppnås.[22] EU-domstolen har stadfestet at «[…] the controller is obliged to mitigate the risks of personal data breaches and not prevent all breaches of those data».[23] «[S]tate of the art»-kravet etter GDPR skal altså kun hensyntas som ett av flere moment i en større dynamisk og sammensatt egnethetsvurdering.

KI-forordningen oppstiller på sin side dette som et absolutt vilkår. Det foreligger ingen vurdering av egnethet. Dette vilkåret vil da på grunn av dets innholdsmessige flytende – men absolutte – natur bli tilnærmet umulig for leverandøren å etterleve. Det overnevnte utsagnet fra EDPB illustrerer hvor høye krav det isolert sett stilles for å etterleve hva som er «state-of-the-art» etter KI-forordningen. Kravet i KI-forordningen står i motsetning til det tilsvarende, men relative og dermed mer etterlevbare kravet etter GDPR artikkel 32 (1).

KI-forordningen artikkel 10 (5) bokstav b fremstår ikke som særlig tilpasset eller tydelig på hvilke tiltak som skal iverksettes.[24] De risikorelative kravene etter GDPR vil langt på vei stille tilsvarende strenge krav, men vil i motsetning være enklere å etterleve. Videre er pseudonymisering allerede særskilt nevnt som et tiltak som – dersom egnet – skal tas for å sikre «egnede tekniske og organisatoriske tiltak», jfr. GDPR artikkel 32 (1) bokstav a. Det er vanskelig å se hvordan hvordan KI-forordningen artikkel 10 (5) bokstav b bidrar ytterligere til å sikre behandlingen av personopplysningene utover det som allerede følger av GDPR. Tvert imot kan bestemmelsen bidra til å skape større usikkerhet knyttet til hvilke tiltak som er tilstrekkelige.

4.3. Konfidensialitetsvilkåret

Det tredje tiltaket fastsettes i artikkel 10 (5) bokstav c:

15 Se GDPR artikkel 4 (5) for definisjonen av pseudonymisering.

16 Kuner mfl. (2020), s. 635.

17 EU-domstolen, VB [C5] C 340/21, avsnitt 42.

18 Skullerud mfl. (2023), Artikkel 32. Sikkerhet ved behandlingen, Juridika [Tilgjengelig: *https://juridika.no/no/lov/2016-04-27-679/%C2%A732/kommentar/*] (lest 06.09.2024).

19 Se KI-forordningen fortalepunkt 48.

20 Voigt og von dem Bussche (2024), s. 40–41.

21 EDPB – Retningslinje 04/2019, avsnitt 20, riktig da som en kommentar angående GDPR artikkel 25 (1), men ordlyden er tilsvarende.

22 Kuner mfl. (2020), s. 637.

23 EU-domstolen, *MediaMarktSaturn [C5]* C-687/21, avsnitt 39.

24 Som GDPR artikkel 9 (2) bokstav g krever av det supplerende rettsgrunnlaget, se punkt 2.

> *«[T]he special categories of personal data are subject to measures to ensure that the personal data processed are secured, protected, subject to suitable safeguards, including strict controls and documentation of the access, to avoid misuse and ensure that only authorised persons have access to those personal data with appropriate confidentiality obligations»*

«[M]easures» som skal sikre at personopplysningene er «secured», «protected» og «subject to suitable safeguards», er allerede omfattet av ordlyden «egnede tekniske og organisatoriske tiltak» etter GDPR artikkel 32 (1). Tekniske og organisoriske tiltak som ikke tilfredsstiller disse vilkårene, kan etter den brede ordlyden vanskelig anses som «egnet».

Adgang til personopplysningene og konfidensialitet er allerede regulert eksplisitt i henholdsvis GDPR artikkel 32 (1) bokstav b og GDPR artikkel 32 (2). Tilsvarende kommer til uttrykk i GDPR artikkel 32 (4), ved at den behandlingsansvarlige og databehandleren skal forsikre seg om at fysiske personer med tilgang til personopplysningene «behandler […] [person]opplysninger bare etter instruks fra den behandlingsansvarlige».

Tiltakene som pålegges etter artikkel 10 (5) bokstav c kan da vanskelig anses som hverken egnet eller særlig etter GDPR artikkel 9 (2) bokstav g.

4.4. Overføringsforbudet

Det fjerde tiltaket fastsettes i artikkel 10 (5) bokstav d:

> *«[T]he special categories of personal data are not to be transmitted, transferred or otherwise accessed by other parties»*

Reguleringen av overføring av personopplysninger til andre parter utrykkes «relativt» i flere av bestemmelsene i GDPR, særlig gjennom reguleringer tilknyttet konfidensialitet og utilsiktet tilgang. GDPR oppsetter imidlertid ikke noen harde forbud mot å dele særlige kategorier av personopplysninger til tredjeparter.

Mens kravene til konfidensialitet *kan* – for å være «egnet» –[25] kreve at informasjonen ikke under noen omstendigheter skal oversendes til andre parter, er imidlertid dette sjeldent aktuelt. Et slikt forbud kan ikke oppstilles som et absolutt krav ved all bruk av KI etter GDPR. GDPR har ikke noe utgangspunkt om at særlige kategorier aldri kan deles til tredjeparter. GDPR vil imidlertid kreve flere og bedre tekniske og organisatoriske tiltak for å ivareta sikkerheten og bøte på risikoen assosiert med å oversende særlige kategorier av personopplysninger, kontra alminnelige personopplysninger. Dersom dette, samt et rettsgrunnlag etter GDPR artikkel 9 (2) foreligger, er oversending, overføring og annen tilgjengeliggjøring i utgangspunktet tillatt og i samsvar med GDPR.

Videre, og betydelig mer problematisk, er det usikkert om KI-forordningen med delingsforbudet har ment å forby bruken av databehandlere. Disse vil etter ordlyden omfattes av «other parties». I GDPR er «tredjepart[er]» (EN: «third party») legaldefinert som enhver annen *enn* databehandlere, m.m.[26] Dersom KI-forordningens ordlyd *ikke* er ment å ekskludere databehandlere, er det uforståelig at EU-lovgiver velger en annen terminologi enn den som allerede er legaldefinert på personvernrettsfeltet. Å benytte seg av andre etablerte legaldefinisjoner i andre EU-rettsakter er en lovgivningsteknikk som hyppig brukes av EU for å sikre uniform forståelse på tvers av rettsaktene. Se f.eks. legaldefinisjonen av særlige kategorier av personopplysninger og personopplysninger i henholdsvis KI-forordningen artikkel 3 (37) og (50).

Et slikt forbud vil da utelukke at noen behandler særlige kategorier av personopplysninger på leverandørens vegne for å bidra med å motkjempe og korrigere skjevheter i KI-systemene. Databehandlere som over tid bygger opp inngående kompetanse i å effektivt motkjempe skjevheter i KI-systemer, kan da ikke tilby sine tjenester til utviklere av KI-systemer. Leverandørene vil da bli tvunget til å løse dette uten databehandlere. Databehandlertjenester utgjør på generelt grunnlag ofte sentrale funksjoner i behandlingen av personopplysninger, for eksempel lagringstjenester. Den behandlingsansvarlige vil da bryte med KI-forordningen dersom den benytter seg av disse tredjemannstjenestene. Å kategorisk utelukke databehandlere ved skjevhetskorrigering og -oppdagelse av KI-systemer er lite hensiktsmessig, og vil gjøre det uforholdsmessig vanskelig for leverandører å luke ut skjevheter fra sine systemer.

Det er påfallende at KI-forordningen skal stenge for en såpass sentral del av databehandlingssfæren som databehandlere utgjør uten å drøfte problemstillingen i fortalen eller under lovgivningsprosessen. Både bestemmelsens ordlyd, valget av ordlyden «in addition» i KI-forordningen artikkel 10 (5),[27] samt ordlyden «without prejudice» i KI-forordningen artikkel 2 (7),[28] åpner derimot for at KI-forordningen nettopp kan avvike løsningen etter GDPR og særregulere disse tilfellene. KI-forordningen artikkel 10 (5) bokstav d fremstår som lite gjennomtenkt, og som en dårligere løsning enn det som allerede følger av GDPR.

25 Se GDPR artikkel 32 (1) bokstav b.
26 Se GDPR artikkel 4 (10).
27 Betydningen av denne ordlyden blir ytterligere problematisert i Ottemo (2024).
28 Ibid.

4.5. Sletting av personopplysninger

Det femte tiltaket fastsettes i artikkel 10 (5) bokstav e:

> *«[T]he special categories of personal data are deleted once the bias has been corrected or the personal data has reached the end of its retention period, whichever comes first»*

At personopplysningene skal slettes «once the bias has been corrected» kan utledes allerede fra grunnprinsippene i GDPR: Personopplysninger skal ikke lagres «i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for», jfr. GDPR artikkel 5 (1) bokstav e. Det samme følger av GDPR artikkel 17 (1) bokstav a: den registrerte har rett til å få sine personopplysninger slettet dersom personopplysninger ikke lenger er «nødvendige for formålet som de ble samlet inn eller behandlet for». Er skjevheten korrigert, er formålet for behandlingen av personopplysningene oppnådd. At personopplysningene etter KI-forordningen slettes når de har nådd «the end of its retention period», følger og defineres allerede av lagringsbegrensningsprinsippet etter overnevnte GDPR artikkel 5 (1) bokstav e.

Det er imidlertid interessant at artikkel 10 (5) bokstav e ikke tar stilling til slettingsplikten og dens betydning for *oppdagelse* av skjevheter. Det er vanskelig for en leverandør å vite om alle skjevheter i et KI-system faktisk *er* oppdaget og korrigert. Dette gjør at det kan være uheldig for leverandører å korrigere skjevheter løpende, og at leverandøren heller venter til at eventuelle skjevheter har samlet seg opp. De særlige kategoriene av personopplysninger må nemlig etter ordlyden slettes «*once* the bias has been corrected».[29] De må slettes allerede ved første skjevhetskorrigering. De kan som en konsekvens ikke benyttes til å finne andre potensielle uoppdagede skjevheter – eksisterende eller fremtidige. Mens dette trolig ikke har vært lovgivers intensjon,[30] så gir den uklare ordlyden et uheldig tolkningsrom.

4.6. Begrunnelse i behandlingsprotokollene

Det sjette og siste tiltaket fastsettes i artikkel 10 (5) bokstav f:

> *"[T]he records of processing activities pursuant to Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680 include the reasons why the processing of special categories of personal data was strictly necessary to detect and correct biases, and why that objective could not be achieved by processing other data."*

Dette er nytt ved KI-forordningen og har ikke en direkte tilsvarende regulering etter GDPR. Et krav om å rettferdiggjøre behandlingen i behandlingsprotokolen foreligger ikke etter GDPR artikkel 30 eller GDPR for øvrig.

GDPR krever imidlertid at en behandlingsansvarlig som planlegger å foreta behandlingsaktiviteter som «medføre[r] en høy risiko for fysiske personers rettigheter og friheter», skal foreta en vurdering av personvernkonsekvensene, jfr. GDPR artikkel 35 (1). En slik personvernkonsekvensvurdering (DPIA[31]) skal minst inneholde «en vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene», jfr. GDPR artikkel 35 (7) bokstav b. Det ligger i høyrisiko KIs natur at de utgjør en «høy risiko for fysiske personers rettigheter og friheter».[32] At det behandles sensitive personopplysninger, herunder særlige kategorier av personopplysninger, er i seg selv et moment i vurderingen av hvorvidt det skal utføres en DPIA.[33] I en slik personvernkonsekvensvurdering er det naturlig å vurdere både hvorvidt en *trenger* å behandle særlige kategorier av personopplysninger, og for hvor lang tid.[34] At en ikke skal behandle flere – eller mer sensitive –[35] personopplysninger enn hva som er nødvendig, følger som tidligere nevnt av dataminimeringsprinsippet, jfr. GDPR artikkel 5 (1) bokstav c.

Selv om det altså ikke stilles krav om at den behandlingsansvarlige fører nødvendighetsvurderingen inn i behandlingsprotokollene etter GDPR, vil GDPR uansett pålegge den behandlingsansvarlige å foreta en tilsvarende vurdering om behandlingsaktivitetens nødvendighet gjennom DPIA-en. Vurderingene vil da ha store overlapp. KI-forordningen kunne dermed ha unngått unødvendig dobbeltarbeid ved å minimum stadfeste at personvernkonsekvensvurderingen alltid skal foretas, eller ved å bestemme at denne skal inkluderes i behandlingsprotokollene. Å oppstille dette som et nytt selvstendig krav – med tilhørende selvstendig vurdering – fremstår unødvendig.

5. Avsluttende refleksjoner

Mens KI-forordningen ikke er ment å medføre forandringer til det eksisterende personvernregelverket,[36] foreligger det uheldige formuleringer og krav som negativt påvirker reguleringen av behandlingen av særlige kategorier av personopplysninger. Mens KI-forordningen na-

29 Min kursivering.

30 Rettskildene er tause angående problemstillingen.

31 «Data Protection Impact Assessment» på engelsk.

32 Se KI-forordningen fortalepunkt 48.

33 Artikkel 29-gruppen – Retningslinje (2017), s. 9.

34 Skullerud mfl. (2023), Artikkel 35. Vurdering av personvernkonsekvenser, Juridika [Tilgjengelig: *https://juridika.no/no/lov/2016-04-27-679/%C2%A735/kommentar/*] (lest 09.09.2024).

35 Se Kuner mfl. (2020), s. 317, dataminimeringsprinsippet omfatter ikke bare personopplysnings*kvantitet*, men også *kvalitet*.

36 Men med unntak, se Ottemo (2024).

turlig nok har hatt sitt regulatoriske fokus på kunstig intelligens, er det likevel ugunstig at EU-lovgiver ikke i større grad har hensyntatt de personvernmessige aspektene på en bedre og mer systematisk måte. Særlig når disse har ligget såpass latent.

Når EU-lovgiver utformer en bestemmelse som direkte henspiller på eksisterende reguleringer i GDPR, er det bemerkelsesverdig at reguleringen ikke skjer på en mer oversiktlig, håndhevbar og harmoniserende måte. Især når artikkel 10 (5) regulerer et såpass viktig formål som å legge til rette for mottiltak mot skjevheter i høyrisiko KI-systemer.

Som redegjort for i punkt 4, foreligger det store overlapp og usikkerheter tilknyttet forpliktelsene som stilles av KI-forordningen artikkel 10 (5), og deres samspill med de eksisterende forpliktelsene som stilles etter GDPR. Det er tvilsomt hvorvidt disse utgjør «egnede og særlige» tiltak. Det er etter min mening ikke gitt at det supplerende rettsgrunnlaget i KI-forordningen artikkel 10 (5), i lys av hjemmelskravet etter GDPR artikkel 9 (2) bokstav g, ville stått seg ved en rettslig overprøving.

Håvard Sveier Ottemo, advokatfullmektig. Han arbeider i Advokatfirmaet Wiersholms avdeling for teknologi, media, telekom og immaterialrett.

6. Kilder

6.1. Bøker

Kuner mfl. (2020) Christopher Kuner mfl., The EU General Data Protection Regulation (GDPR) A Commentary, 1. utgave, Oxford University Press 2020.

Voigt og von dem Bussche (2024) Paul Voigt og Axel vom dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, 2. utgave, Springer 2024.

Artikler

Bekkum (2024) Marvin van Bekkum, «Using sensitive data to debias AI systems: Article 10(5) of the EU AI Act», Cornell University. Tilgjengelig: https://doi.org/10.48550/arXiv.2410.14501 (lest 27.11.2024).

Ottemo (2024) Håvard Sveier Ottemo, «Krysningspunktet mellom KI-forordningen og GDPR | KI-forordningens regulering av supplerende rettsgrunnlag for behandling av særlige kategorier av personopplysninger etter personvernforordningen», Universitet i Bergen, 2024. Tilgjengelig: *https://hdl.handle.net/11250/3177525* (lest 12.02.2025)

6.2. Lovkommentarer

Skullerud mfl. (2023) Åste Marie Bergseng Skullerud mfl., Personvernforordningen (GDPR) – Kommentarutgave, i Juridika, 2018, ajourført 1. april 2023.

NIS2: Hvilke virksomheter og leveranser vil omfattes av fremtidens krav til cybersikkerhet infrastruktur?

Av Kristian Foss

Bakgrunn:
NIS2-direktivet (Direktiv (EU) 2022/2555) erstatter det tidligere NIS-direktivet (Direktiv (EU) 2016/1148) og gir en utvidet ramme for cybersikkerhet på tvers av EU. Hensikten med NIS2 er å styrke sikkerheten og motstandskraften til IT-systemer og kritisk infrastruktur. I denne artikkelen vil vi se nærmere på hvilke enheter som blir omfattet av NIS2 i henhold til artikkel 2 og vedlegg 1 og 2.

Del 1: Hvilke virksomheter og leveranser omfattes? Del 2: Hvilke sikkerhetskrav gjelder og hvordan kan kravene oppfylles. Del 3: Hvilket personlige ansvar kan ledelsen og ansatte pådra seg dersom kravene ikke etterleves.

I denne første artikkelen i en serie på tre vil vi fokusere på hvilke virksomheter som vil omfattes av Network and information system-direktivet («NIS2»).[1] Spørsmålet om virkeområdet fortjener litt ekstra oppmerksomhet fordi det ikke er helt rett frem å besvare. En rekke virksomheter faller klart innenfor, men gråsonen er ekstra stor som følge av måten NIS2 er strukturert på.

Kristian Foss

Kortversjonen av de omkring 3200 ordene som bestemmer virkeområdet er at følgende private og offentlige virksomheter omfattes:[2]

a. virksomheter i bransjer som listet opp i NIS2 annex 1 og 2 (energi, transport, helse, digital infrastruktur, vann og kloakk, matproduksjon, tilvirkning av maskiner og utstyr, m.fl.)
b. virksomheter med over 50 ansatte og årlig omsetning eller balanse over 10 MEUR; eller
c. er særlige kritiske selv om virksomheten er mindre, med
d. datterselskaper og såkalt «partner-selskaper» (over 25 % eierandel eller annen kontroll), med mindre disse er lite tilknyttet virksomheten, og
e. andre selskaper i leveransekjeden, avhengig av risiko.

Se mer om hvilke virksomheter som er omfattet i pkt. 2.

NIS2 gjelder samfunnskritisk infrastruktur, døpt «network and informations systems» («NIS») i direktivets engelske utgave. NIS betyr grovt sagt infrastruktur for signaltransport med noe tilhørende logikk. Dermed oppstår blant annet spørsmålet om selvstendig programvare omfattes og eventuelt hvilken. Vi ser nærmere på dette i pkt. 1, før vi tar fatt på den omfattende katalogen av omfattede virksomheter i punkt 2.1.

> Dermed oppstår blant annet spørsmålet om selvstendig programvare omfattes og eventuelt hvilken.

Siden NIS2 er et direktiv vil vi ikke kjenne reglenes eksakte utforming før også Norge implementerer direktivet. Men dette minimumsdirektivet vil i alle fall gi en tydelig indikasjon på hva som blir minstemålet norske og europeiske virksomheter vil måtte etterleve. Har den norske virksomheten kunder eller leverandører i EU-land, vil direktivteksten være enda mer interessant.

Det første NIS-direktivet, ofte kalt NIS1, er fra 2016 og er enda ikke implementert i norsk rett.[3] [4]

1 DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

2 NIS2 art. 2 og 3, annex 1 og 2, ikke medregnet forordninger og direktiver vist til eller fotnoter.

3 Direktiv (EU) 2016/1148.

4 IKT-forskriften av 2003 har i mellomtiden vært det nærmeste vi har kommet et generelt cybersikkerhetsregelverk for norske virksomheter, selv om det er rettet inn mot finansbransjen. Ellers har vi hatt sektorbasert regulering, som vil bestå ved siden av NIS2.

Høringen for implementering av NIS1 var sist høst med frist 11. desember 2024, åtte år etter NIS1 kom. Justis- og beredskapsdepartementet opplyser om at høringsnotatet for NIS2 er under utarbeidelse, så vi får anta det ikke går nye åtte år får det implementeres.

Både NIS1 og NIS2 vil bli implementert gjennom forskrift, da digitalsikkerhetsloven av 2023 er helt overordnet og nærmest bare en fullmaktslov.[5] Loven vil tre i kraft når NIS1-forskriften er vedtatt av regjeringen.

1. Hvilke leveransetyper omfattes – hva med selvstendig programvare?

1.1 Hva er et NIS?

Direktivet har tatt sitt navn fra leveransetypen direktivet regulerer, nemlig *informasjons- og nettverkssystemer*. Det vil si

a. «et elektronisk kommunikationsnet som defineret i artikel 2, nr. 1), i direktiv (EU) 2018/1972
b. enhver anordning […], hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data, eller
c. digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a) og b) med henblik på deres drift, brug, beskyttelse og vedligeholdelse»

(NIS2 art. 6 (1), i den danske versjonen, mine uthevinger)

Et «**elektronisk kommunikationsnet**» er i følge direktiv (EU) 2018/1972 artikel 2, nr. 1

> *«transmissionssystemer, […], og, […], koblings- og dirigeringsudstyr og andre ressourcer, […], som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, […], i det omfang de anvendes til transmission af signaler, […] , uanset hvilken type information der overføres.»*

Vi snakker med andre ord om signaltransport i **nettverk**. Slike nett kan være trådløse eller kablede, så lenge de er elektromagnetiske eller lysbaserte, som i fiber. Her er altså reguleringen ikke fullt ut teknologinøytral. Skulle en ny overføringsmåte bli aktuell, kanskje kvanter, får vi anta at direktivet og/eller de nasjonale implementeringene vil oppdateres.

Et informasjons- og nettverkssystem – et NIS – kan også bestå av en «**anordning**». I direktivets engelske versjon «device», noe som oversetter til «innretning» eller «enhet» på norsk. Trolig en fysisk gjenstand med andre ord. Denne *anordningen* må utføre automatisk behandling av «digitale data» ved hjelp av et «program». Den engelske utgaven av direktivet bruker i likhet med den danske «program», og ikke «software». Man kan dermed tenke seg at også «firmware» omfattes, noe som er praktisk i nettverksutstyr. Prinsipielt er det heller ikke utelukket at ren maskinbasert logikk skulle kunne være omfattet, så lenge behandlingen er automatisk og den kan håndtere digitale data.

Det siste alternativet i c) gjelder **tilknyttet lagring og overføring** av digitale data ved hjelp av en *anordning* (b) eller et *elektronisk kommunikasjonsnett* (a), som nevnt over. Slike data må «behandles», «fremfindes», «overføres» eller «lagres». Uansett er det sentrale at det skjer noe med dataene knyttet til enheten eller nettet. Typisk vil enheten være en datamaskin med minne. Dermed omfattes for eksempel datasentre, med sine servere. I nettet vil typisk rutere og switcher behandle og overføre digitale data. Men også annet nettverksutstyr og PCer i næring og offentlige virksomheter vil omfattes. Det samme gjelder selve nettverkene som knytter enhetene sammen, lokalt (LAN), et større område (WAN) og internett.

I sum utgjør disse bestanddelene *NISet*, et moderne samfunns digitale infrastruktur. Formålet med NIS-direktivene er å sikre disse NISene, når de brukes av virksomheter som er viktige for samfunnet. Hvilke virksomheter dette er skal vi som nevnt se nærmere på i pkt. 2.1.

Hvilke sikkerhetskrav og hvordan kravene kan tilfredsstilles, skal vi behandle i del 2 av artikkelserien. Hvilket personlige ansvar ledelsen og ansatte kan pådra seg dersom kravene ikke etterleves skal vi ta for oss i del 3 av artikkelserien.

> I sum utgjør disse bestanddelene *NISet*, et moderne samfunns digitale infrastruktur.

1.2 Hva med frittstående programvare?

Et sentralt spørsmål er hvor langt opp i «stabelen» av maskin- og programvare reguleringen i NIS2 går. Som vist i det forrige punktet, kan det virke som at rekkevidden er begrenset til infrastrukturlaget med støttende programvare. Det er ikke nødvendigvis tilfelle.

Av NIS2 art. 21 (1) og (2) fremgår det at essensielle og viktige virksomheter skal pålegges forholdsmessige tiltak for å oppnå tilfredsstillende sikkerhet, for å hindre eller minimere konsekvenser av *hendelser* (*eng.* «incidents»). Hendelser er definert i NIS2 art. 6 (6) og lyder på dansk:

> »hændelse«: en begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de **tjenester**, der **tilbydes** af eller er **tilgængelige via** net- og informations systemer, i fare [mine uthevinger]

I definisjonen ligger at rekkevidden ikke er begrenset til NISet selv, men strekker seg også til «tjenester som tilbys eller er tilgjengelige *via* NI-

5 L20.12.2023 nr. 108 Lov om digital sikkerhet.

Ser». I dagens samfunn betyr det i prinsippet enhver programvare.

At rekkevidden er lang rimer også med siktemålet for direktivet: «å oppnå et høyt felles cybersikkerhetsnivå» (NIS2 art. 1 (1)). Cybersikkerhet skal forstås som i cybersikkerhetsforordningen (jf. NIS2 art. 6 (3)). Av cybersikkerhetsforordningen fremgår at [6]

> *«'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;» (art. 2 (1)).*

«Cybertrusler» er definert til

> *«'[…] any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;» (art. 2 (8)).*
>
> [mine uthevinger]

Cybersikkerhetsforordningen viser ikke direkte til tjenester som tilbys *via* NISer, men til «brukere» av NISer og «andre personer». Gitt formålet til NIS2 og den vide ordlyden i cybersikkerhetsforordningen, bør ikke definisjonene av «cybersikkerhet» og «cybertrusler» innskrenke forståelsen av «hendelser» i NIS2 art. 6 (6). For samfunnet vil det være likegyldig om strømforsyningen eller sykehusdriften bryter sammen som følge av svikt i infrastrukturlaget eller annen programvare som også er avgjørende for at de samfunnsviktige tjenestene leveres.

På denne bakgrunn er det rimelig å anta at de fleste frittstående, driftskritiske programvarer som utnytter et NIS for en samfunnsviktig virksomhet, er omfattet av NIS2. Det betyr i prinsippet nesten all slik normalt driftet programvare.

Selv om ordet «software» bare forekommer åtte ganger i de 40 900 ordene NIS2 består av, vil NIS2 dermed omfatte en mange ulike typer programvare og programvare. Noen sannsynlige eksempler er programvare for administrasjon av datasenter, elektroniske pasientjournalsystemer (EPJ), nettbankplattformer, styringssystemer for smarte nett, for flåtestyring (logistikk), Altinn, robotikk-kontroll, vannbehandlingsanlegg og sporingssystemer for avfallshåndtering.

Denne typen programvarer kan være avgjørende for at samfunnet og økonomien skal fungere, og gjør at de underlegges sikkerhetskravene, risikostyringstiltakene, rapporteringsforpliktelser og samsvarskravene i NIS2.

I tillegg legger direktivet vekt på «innebygget sikkerhet» (by design, by default), noe som krever at cybersikkerhetshensyn tas fra tidlig planlegging, gjennom hele livssyklusen til disse programvareproduktene. En lignende holistisk tilnærming må anlegges for leverandørkjeden. Begge deler kommer vi tilbake til i del 2 av denne artikkelserien.

Den vide og dype rekkevidden betyr at programvareleverandører til kunder som er omfattet av NIS2, indirekte blir omfattet. For disses kunder blir det avgjørende å sørge for å kontraktuelt sikre at programvaren etterlever kravene i NIS2. Se pkt. 2.4 om leveransekjedesikkerhet. For leverandørene kan proaktiv etterlevelse gi et konkurransefortrinn.

2. Hvilke virksomheter omfattes av nis2?

2.1 Mellomstore virksomheter viktig for samfunnet omfattes

2.1.1 Hvilke sektorer er viktige?

I NIS2 annex 1 og 2 jf. listes bransjer og virksomheter som vil reguleres (se NIS2 art. 2 (1)). Virksomhetene deles i to grupper;

a. **essensielle** (annex 1) og
b. **viktige** («important», annex 2).

innplassert i annexene i henhold til hvor kritisk sektoren er, type tjenester virksomhetene besørger og deres størrelse. [7]

Hoveddelen av virksomhetene i annex 1 var omfattet også av NIS1 fra 2016. Siden NIS1 først i disse dager skal gjøres til norsk rett (gjennom forskrift), vi vi for oversiktens skyld gjennomgå også annex 1. Se pkt. 2.1.3 og 2.1.4.

2.1.2 Hva er en mellomstor virksomhet?

Hovedregelen i NIS2 er at bare mellomstore og større virksomheter omfattes (art. 2 (1)). Definisjonen av mellomstore virksomheter fremgår av 2003/361/EF. Ifølge anbefalingens annex, art. 2 anses virksomheter med flere 50 ansatte og omsetning eller balanse over 10 MEUR som mellomstore.

Omsetning skal vurderes utfra de siste godkjente regnskaper, beregnet månedlig. Moms og skatter skal ikke regnes inn. For nystartede virksomheter skal det gjøres en godtroberegning. Se annexes art. 4.

«Ansatte» viser til årsverk, men ikke bare fra formelt sett ansatte personer, men også «eierledere» og andre. Innleide konsulenter ser imidlertid ikke ut til å omfattes. Se annexet, art. 5.

Merk at det holder om enten omsetning *eller* balansen er over grensen, så lenge antall ansatte er over 50.

Nivået som er satt betyr at de fleste betydningsfulle virksomheter i Europa omfattes, offentlige og private. Men i Norge vil trolig en del virksomheter som kan være viktige gå klar. Som det fremgår av pkt. 2.3 vil i mange tilfeller dette størrelseskravet likevel ikke få noen betydning, bare virksomheten er viktig nok.

2.1.3 Essensielle virksomheter (annex 1)

6 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

7 Fortalepunkt 15.

NIS2 utvider både innholdet i kategoriene av essensielle enheter som tidligere var omfattet av NIS1 og legger til nye hovedgrupper. I NIS2 er for eksempel offentlig *administrasjon* eksplisitt listet, noe den overraskende nok ikke var i NIS1, på tross av sin samfunnsviktige funksjon.[8]

Under følger en oversikt over virksomheter og bransjer som er omfattet. Opplistingen er ikke nødvendigvis uttømmende, men vil gi en oversikt. Mange av punktene viser videre til andre direktiver eller forordninger, som man kan slå opp i om man vil bore mer i ett virksomhetsområde.

Dersom disse rettsaktene gir lik eller bedre sikkerhet vil de gå foran NIS2.[9] Dette innebærer at virksomheter som faller utenfor det aktuelle sektorregelverket, reguleres av NIS2.

- **Energi**: All form for energiproduksjon, overføring og distribusjon, inkludert elektrisitet, fjernvarme, olje, gass og hydrogen. Kategorien energi omfatter også ladestasjoner for elektriske kjøretøy. Hydrogen og fjernvarme er nytt for i forhold til NIS1.
  - Elektrisitet: Også markedsoperatører og deltagere omfattes.
  - Fjernvarme vil typisk omfatte selskaper som Hafslund Fjernvarme.
  - Olje vil typisk omfatte virksomheter som Equinor, raffinerioperatører og rørledningsoperatører .
  - Gass vil typisk omfatte virksomheter som driver med flytende gass (LNG), naturgass, raffinering og annen behandling av gass.
  - Hydrogen vil typisk omfatte virksomheter som Norwegian Hydrogen, Greenstat og selvfølgelig Equinor.
- **Transport**: Sjøtransport (hav- og innlandsfrakt, men ikke individuelle fartøy), luft- og landtransport (flyselskaper, flyplasser, luftkontroll, jernbaneinfrastruktur og togselskaper, men ikke lastebilflåteoperatører). Store deler av verdikjeden er dermed dekket, på samme måte som i NIS1. Eksempler på regulerte virksomheter er dermed Statens Vegvesen, havnevesen som Oslo havn KF. Underkategorier omfatter:
  - flyselskaper,
  - flyplasser (typisk Avinor)
  - trafikkstyring, jernbane, vanntransport og veitransport gjenstand for egne direktiver og forordninger.
- **Banker og finansinstitusjoner**: NIS2 lister banker og andre finansinstitusjoner som omfattet, samtidig som det fremgår av fortalepunkt 28 at DORA skal gå foran.[10] En naturlig tolkning vil være at NIS2 omfatter eventuelle virksomheter i finansbransjen og systemer som ikke måtte være omfattet av DORA. Denne grensen bør gå opp av finansinstitusjoner.
- **Finansinfrastruktur**: Børser og uregulerte handelsplattformer, samt infrastrukturer som Central Counterparties (CCPs).
- **Helse**: Kategorien omfatter tre undergrupper, hvorav de to siste er nye i forhold til NIS1.
  - Den undergruppen første gjelder leverandører av helsetjenester, og vil typisk omfatte sykehus og legeklinikker.
  - laboratorier
  - forsknings- og utviklingsinstitusjoner for medisinske produkter, produsenter av medisiner og miksturer, produsenter av medisinsk utstyr ansett som kritisk under en offentlig helsekrise, som for eksempel pustemaskiner under covid-19-pandemien.
- **Drikkevann**: Leverandører og distributører av drikkevann for menneskelig konsum. Kommunale vannverk er typiske eksempler.
- **Avløpsvann**: Virksomheter som samler inn, blir kvitt eller behandler kloakk, omfattes i NIS2, som nytt i forhold til NIS1.
- **Digital infrastruktur:** Basis internettinfrastruktur som internettkoblingssentraler og DNS-tjenester, IKT-forvaltningstjenester (næring-til-næring), skylagringsoperatører, datasentere, innholdsleveringsnettverk (CDN), tilbydere av tillitstjenester (elektroniske signaturer, segl, tidsstempler og sertifikater for nettstedsautentisering), og elektroniske kommunikasjonsnettverk. Betydningen av fysisk sikkerhet understrekes spesielt i fortalepunkt 31. Også dette punktet er nytt i NIS2 i forhold til NIS1.
- **IKT tjenesteleverandører:** Enda en ny sektor dekket av NIS2 er leverandører av forvaltningstjenester og sikkerhetstjenesteleverandører. [11] Denne sektoren har blitt stor, og leverer trolig broparten av slike IT og sikkerhetsrelaterte tjenester.
- **Offentlig administrasjon:** Både sentral og regional*administrasjonen* omfattes, slik denne angis av nasjonal lovgivning. Også ny i NIS2.
- **Romfart**: Til sist i listen i annex 1 kommer romfart, som har blitt en stor bransje som mye samfunnsviktig infrastruktur avhenger av. NIS2 introduserer derfor regulering av den bakkebaserte infrastrukturen som støtter leveranse av rombaserte tjenester. Bakkestasjoner for mottak av satellittsignaler og oppskytingsanlegg for raketter vil være eksempler på dette.

8 Men offentlige *virksomheter* kunne bli omfattet også av NIS1, men da utfra virksomhetsklassifisering.

9 Fortalepunkt 23.

10 Forordning (EU) 2022/2554 (Digital operasjonell motstandskraft for finansnæringen, DORA).

11 «Managed service providers» og «managed security service providers».

2.1.4 Viktige virksomheter (annex 2):
Den andre kategorien av virksomheter listes i annex 2 og inkluderer en rekke andre sektorer som anses som «viktige», men ikke like kritiske som de essensielle enhetene. De fleste av disse er nye med NIS2:

- **Post- og leveringstjenester:** Så fremt virksomheten er en del av transportør-lenken, som for eksempel en hentetjenester, omfattes den. [12] Eksempler er Posten, Postnor og budtjenester, gitt at størrelseskravet er oppfylt.
- **Avfallshåndtering:** En rekke av landets større rennovasjonsselskaper vil være omfattet av NIS2.
- **Kjemisk produksjon og distribusjon:** Se nærmere i den aktuelle forordningen for hvilke typer kjemikalier som er omfattet.
- **Matproduksjon, -foredling og -distribusjon:** Slakterier, bakerier, fiskeoppdrettere, produsenter av ferdigmat og andre virksomheter involvert i matproduksjon, omfattes bare de er store nok. Den kanskje største vil være Orkla.
- **Tilvirkning:** Virksomheter som lager:
  - Medisinsk utstyr (inkludert ikke-kritisk utstyr i en krisesituasjon) og diagnoseutstyr for bruk utenpå kroppen.[13]
  - Datamaskiner, elektronikk og optiske produkter.
  - Maskineri og utstyr utgjør en stor undergruppe, som omfatter 21 kategorier maskineri som for eksempel motorer, turbiner, pumper, ventilasjonsutstyr, jordbruksutstyr, næringsmiddelutstyr, traktorer, ploger, tekstilmaskiner som angitt i detalj i klassifikasjonssystemet NACE rev.2. [14]
  - Motorkjøretøy, trailere og semitrailere, samt deler til disse, igjen som angitt i NACE rev. 2.
  - Annet transportutstyr, som for eksempel båter, tog, jagerfly, romskip.
- **Digitale leverandører**: I likhet med NIS1 omfattes leverandører av nettbaserte markedsplasser og søkemotorer. Nytt i NIS2 er plattformer for sosiale nettverk, som Facebook og TikTok.
- **Forskning**: Heller ikke forskningsorganisasjoner var omfattet av NIS1. Et eksempel kan være SINTEF. Begrunnelsen er bl.a. å unngå industrispionasje og tap av forretningshemmeligheter.[15]

Omfanget av virksomheter som er omfattet av NIS2 er betydelig utvidet sammenlignet med NIS1, noe som reflekterer den økende digitaliseringen av samfunnet. Kategoriseringen av virksomheter som essensielle eller viktige reflekterer en vurdering av både viktighet og sårbarhet. For eksempel er matproduksjon svært viktig, men anses mindre sårbart, trolig fordi det er mulig å distribuere uten IT-systemer og folk ofte har beredskapslagre.

Implementeringen av NIS2 forventes å styrke Europas generelle cybersikkerhet ved å sikre at flere sektorer oppfyller strenge sikkerhetskrav og rapporteringsforpliktelser.

> Kategoriseringen av virksomheter som essensielle eller viktige reflekterer en vurdering av både viktighet og sårbarhet.

2.2 Nærstående selskaper uten særlig selvstendighet omfattes

For å gjøre NIS2 reelt virkningsfullt reguleres også konsernforhold og mindre nære selskapstilknytninger, slik at også såkalte:
a. «denkede selskaper» og
b. «partner-selskaper»

omfattes. Se NIS2 art. 3 (1) a som viser til anbefaling 2003/361/EF art. 2. [16]

Lenkede selskaper er slike som den regulerte virksomheten kontrollerer via majoritetseierskap, stemmerett, avtale eller på annen måte. Typisk vil være aksjeeiereierskap over 50 %, slik som situasjonen vil være for datterselskaper. Se anbefalingen art. 3 (3).

Partnerselskaper er selskaper med løsere finansiell eller kontrollmessig tilknytning. Grensen er satt på 25 % eierandel eller annen kontroll, vurdert som for lenkede selskaper.

Uavhengige virksomheter er slike hvor ingen virksomhet har over 25 % kontroll, og omfattes ikke av NIS2 via denne indirekte reguleringen.

NIS2 nevner ikke eksplisitt at linkede og partnervirksomheter skal telles med ved beregning av virkeområde, men fortalepunkt 16 indikerer at det er tilfelle. Se under om dette.

Det er verdt å merke seg at et tilleggsvilkår for at NIS2 skal gjelde er at de lenkede og partnerselskapene har en **viss nærhet** i sin tilknytning. For å unngå en uforholdsmessig stor rekkevidde av NIS2, skal grad av selvstendighet vurderes. Av NIS2 fortalepunkt 16 følger:

> *«In order to avoid entities that have partner enterprises or that are linked enterprises being considered to be essential or important entities where this would be disproportionate, Member States are able to take into account the degree of independence an entity enjoys in relation to its partner or linked enterprises when applying*

12 Fortalepunkt 12.
13 «utvortes» som det heter på fint.
14 NACE: Statistical classification of economic activities in the European Community fra Eurostat

15 Fortalepunkt 88.

16 Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422) *https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32003H0361*

Article 6(2) of the Annex to Recommendation 2003/361/EC. In particular, Member States are able to take into account the fact that an entity is independent from its partner or linked enterprises in terms of the network and information systems that that entity uses in the provision of its services and in terms of the services that the entity provides. […]» [mine uthevinger]

Dermed får vi en avveining både av størrelse og nærhet.

Partner og tilknyttede selskaper må med dette ofte inkludere størrelsen på morselskapet og omvendt, men vurdering må gjøres. Reglene om nærhet og rekkevidde kan suppleres av nasjonale regler.

Selskaper som ikke omfattes via anbefalingen om tilknyttede virksomheter, kan naturligvis omfattes direkte om NIS2 øvrige vilkår skulle være oppfylt. For eksempel kan mindre virksomheter være betydningsfulle, noe vi skal se på i neste kapittel.

2.3 Mindre virksomheter med særlig kritisk funksjon omfattes

Nesten halve NIS 2 art. 2 regulerer hvilke virksomheter som er omfattet av direktivet *uansett størrelse*. Begrunnelsen er naturligvis at en rekke mindre virksomheter kan være samfunnskritiske.

Det er særlig interessant å merke seg tredje ledd, som sier at virksomheter som omfattes av EU-direktivet 2022/2257 skal omfattes uansett størrelse. Dette direktivet overlapper stort sett med NIS2 annex 1. Det betyr at størrelsesbegrensning blir mindre viktig for annex 1-virksomheter. Eksakt hvilke virksomheter som skal omfattes skal bestemmes i EU av myndighetene innen 17. juli 2026. Hva som vil gjelde i Norge, får vi nok vite først senere.

Andre ledd i art. 2 nevner følgende virksomheter som skal være omfattet uansett størrelse:

- Leverandører av offentlige tilgjengelige digitale kommunikasjonsnettverk og tjenester, som for eksempel internettleverandører som sørger for at brukere får tilgang til internett (a–i).
- Tillitstjeneste-leverandører, som nærmere regulert under i (EU) 910/2014 eIDAS-forodningen implementert i lov om elektroniske tillitstjenester (L15.06.2018 nr. 44), for eksempel virksomheter som leverer elektroniske signaturer og leverandører av sertifisering av nettsteder for å sikre autentisitet og sikkerhet (a–ii).
- Topnivå domene registrarer, som Norid (a–iii).
- Eneleverandører av tjenester for opprettholdelse av kritiske sosiale og økonomiske aktiviteter, for eksempel leverandører av stamnett og primærsamband, som Telenor (b).
- Leverandører der tjenesteforstyrrelser kan påvirke offentlig sikkerhet og helse, som for eksempel Telenors ruting av nødnumre (110, 112, 113) etter nummerforskriften av 2004 (c).
- Leverandører av tjenester som kan påføre «vesentlig høy risiko», særlig for sektorer som kan påvirkere flere land, som for eksempel underleverandører til en kraftdistributør (d).
- Leverandører som er kritiske på grunn av sin særlige viktighet nasjonalt eller regionalt, for særlige typer sektorer eller type tjenester (e). Dette kan for eksempel være NIX (Norwegian Internet eXchange).
- Utpekte offentlige virksomheter i sentral- og regionaladministrasjonen i henhold til risiko og som angitt i nasjonal rett (f).

Fjerde ledd i art. 2 nevner også domenenavn registratorer, som for eksempel Domeshop.

NIS2 utvider dermed beskyttelseskravene til et bredt spekter av enheter og tjenester for å sikre robusthet i den digitale infrastrukturen i Europa.

2.4 Selskaper i leveransekjeden må omfattes

Mange angrep starter hos underleverandørene til virksomheter. Forsyningskjedesikkerhet blir dermed en kritisk for å oppnå tilfredsstillende sikkerhet hos energiselskaper, transportører og andre omfattede virksomheter. Med voldsom digitalisering og avhengighet av NISer, er det selvsagt at NIS2 dermed stiller krav også til styring av sikkerheten i leverandørkjeden. Vi skal se på kravene til den sikringen, kort diskutere svakhetene i reguleringen og gi eksempler på mulige tiltak.

2.4.1 «All Hazard»-tilnærmingen

All hazard-tilnærmingen i NIS2 art. 21 (2) pålegger essensielle og viktige enheter å beskytte seg mot alle typer farer som kan påvirke sikkerheten i nettverks- og informasjonssystemer.[17] Denne tilnærmingen krever en omfattende vurdering av potensielle trusler, inkludert de som oppstår i forsyningskjeden. Kravet gjelder også NISenes fysiske omgivelser, og kan omfatte sikring mot tyveri, brann, flom, uautorisert fysisk tilgang, jordskjelv, eksplosjoner og sabotasje.

Ved å regulere sikkerheten i forsyningskjeden, kan offentlige og private virksomheter redusere risikoen for at svakheter hos underleverandører skal kompromittere hele systemet.

Art. 21 (2) lyder:

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect

17 Dansk NIS2 art. 21 (2): 2.«De i stk. 1 omhandlede foranstaltninger baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende:»

network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

[mine uthevinger]

Det mest iøynefallende i litra d er begrensningen til *direkte* underleverandører. En SaaS-tjeneste kan i dag lett består av fire ledd under kunden (for eksempel infrastrukturleverandør, plattformleverandør, SaaS-leverandør og systemintegrator). Da blir det viktig å merke seg at tiltakene *minst* skal omfatte direkte leverandør. Kravet til «all-fare-tilnærming» tilser at flere ledd i leveransekjeden må sikres for å «forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester», slik den danske utgaven av NIS2 art. 21 (1) uttrykker det. I samme retning fastsetter NIS2 art. 1 at målet er å «opnå et højt fælles cybersikkerhedsniveau».

Dermed er det klart at virksomheter i mange tilfeller vil være ansvarlige for å sikre flere ledd nedover i leveransekjeden. Men plikten begrenses av forholdsmessighetskravet som også fremgår av art. 21 (1). Begrensningen innebærer at tiltak skal vurderes utfra risiko, «state of the art», kostnader, virksomhetenes eksponering, størrelse og sannsynlighet for hendelser, og deres alvorlighetsgrad. Samfunnsmessig og økonomisk innvirkning skal også vurderes. For eksempel vil en leverandør av et journalsystem til et sykehus forventes å ha vesentlig bedre kontroll på leverandørkjeden enn en bilforhandler.

Art. 21 (3) d skiller heller ikke mellom virksomheter i EØS og utenfor, så lenge tjenesten ytes i EØS-området.

2.4.2 Ansvar for cybersikkerhet: Hvem i kjeden bør være ansvarlig?

NIS2 art. 21 (1) slår fast at det er essensielle og viktige virksomheter som er ansvarlig for sikkerheten i NISer. Det kan være en strømprodusent, et vannverk, renovasjonsselskap eller en fiskeoppdretter. Felles for disse og mange andre omfattede virksomheter er at de oftest mangler tung programvare- og cybersikkerhetskompetanse. De vil vanligvis kjøpe systemer inn fra tredjeparter, men likevel forblir ansvaret hos virksomheten.

Et nærliggende spørsmål er derfor hvilken enhet som er best egnet til å sikre cybersikkerheten i forsyningskjeden og hvordan denne bør og kan gjøres ansvarlig. Hovedleverandøren av produktet i forsyningskjeden vil ofte være den som er best posisjonert til å overvåke og sikre hele kjeden. Hovedleverandøren bygger systemet, har direkte kontakt med sine underleverandører og vet mye om hvilke underleverandører disse underleverandørene igjen benytter. Med en del innsats kan kontroll over hele leveransekjeden kanskje oppnås. For renovasjonsselskapet, vannverket og andre virksomheter vil denne jobben være vesentlig tyngre, og i mange tilfeller praktisk talt umulig.

En bedre regulering kunne dermed vært å pålegge ansvar direkte til aktørene i leveransekjeden. Dette er løsningen som personvernforordningen (pvf.) introduserte ved å gjøre ikke bare behandlingsansvarlige ansvarlige (som tidligere), men pålegge også databehandler plikter. Siden NIS2 er et minimumsdirektiv, vil en slik tilnærming være mulig i Norge, men neppe særlig effektiv uten at øvrige land i EØS implementerer en lik regel.

Den nye forordningen om Digital operasjonell motstandskraft for finansnæringen (DORA) har tatt logikken i pvf. et skritt videre, og inkorporer reguleringen av avtaler med underleverandører i en rekke bestemmelser.[18] Det er litt overraskende at ikke NIS2 har vært grundigere på dette området.

> Det er litt overraskende at ikke NIS2 har vært grundigere på dette området.

2.4.3 Kontraktuelle tiltak

NIS2s ordning er derimot basert på at den regulerte virksomheten iverksetter tiltak overfor sine leverandører. Av NIS2 fortalepunkt 85, fremgår det at kontrakter er et mulig slikt tiltak, på samme måte som databehandlingsavtaler er det etter pvf. art. 28. NIS2 stiller imidlertid ikke et eksplisitt krav til videre sikring nedover i kjeden slik pvf. art. 28 (4) gjør. Men gitt kravene til «all-fare»-tilnærmingen, er dette et kontraktuelt grep omfattede virksomheter bør vurdere for å få kontroll flere ledd ned i kjeden. Slike krav kan omfatte:

- Krav om overholdelse av spesifikke sikkerhetsstandarder og -protokoller.
- Regelmessige sikkerhetsvurderinger og revisjoner.
- Opplæring i cybersikkerhet for ansatte hos leverandører.
- Strenge retningslinjer for informasjonsdeling og tilgangskontroll.

Implementeringen av slike kontraktsmessige krav sikrer at alle leverandører, uavhengig av deres størrelse eller plass i forsyningskjeden, oppfyller de nødvendige sik-

18 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. Trådte i kraft i EU 17. januar 2025. Fortalepunkt 29 gir en innføring i tankegangen.

Illustrasjon: Colourbox.com

kerhetsstandardene. Dette bidrar til å skape bedre sikkerhet.

2.4.4 Andre tiltak

Siden det ofte ikke vil være mulig for en omfattet virksomhet, og kanskje heller ikke for en hovedleverandør i kjeden, å sikre alle ledd, bør man tenke alternativt. Mest nærliggende er å sørge for at løsningen vil være sikker selv om ledd nedover i kjeden blir kompromittert. Sikring kan skje gjennom robust sikkerhetsstruktur, overvåkning, redundans og opplæring, for å nevne noen eksempler. Her vil en sikkerhetsekspert kunne bidra med verdifulle råd.

2.5 Unntak

Som vanlig gjøres unntak fra direktivets anvendelsesområde for offentlig administrasjon innenfor nasjonal sikkerhet, ordensmakten, forsvar og rettsvesen (NIS2 art. 2 (6) og (7)).

Advokat Kristian Foss, Bull & Co advokatfirma (Dato: 24. februar 2025)

Shifting responsibility in IT agreements: From client-centric compliance to provider accountability

av Jaakko Lindgren og Sohrab Känkäinen

Client-centric compliance

In the early days of IT agreements, the responsibility for a system's legal compliance often rested on the client. This allocation was driven by two key factors: intellectual property rights (IPR) ownership and market practices of the time. Frequently, clients either owned or sought significant control over the IPR of the systems they commissioned. This ownership inherently made them responsible for ensuring the system's compliance with applicable laws and regulations.

Additionally, prevailing market norms placed more emphasis on clients managing their compliance. IT providers were primarily focused on delivering functionality and technical capabilities, while clients, with their specific industry knowledge, were expected to navigate the legal and regulatory landscape. For instance, a bank implementing a financial system would bear the responsibility for ensuring it adhered to financial regulations, as the system was tailored to their operational needs.

It can be argued that for a long time, the work of IT providers was akin to craftsmanship, where each client received a slightly customized solution. While IT providers were perceived as "industrial" companies, in terms of contracts, their work was more akin to "handicraft."

Eu regulation and market evolution

Recent years have brought about a significant shift in this dynamic, largely driven by changes in the regulatory environment and the technological landscape. The introduction of robust EU frameworks such as the GDPR, the AI Act, and the Digital Services Act has placed new, direct compliance obligations on IT providers. These regulations emphasize the need for providers to ensure their systems are lawful by design and compliant throughout their lifecycle, even as legal standards evolve.

Jaakko Lindgren

Sohrab Känkäinen

At the same time, the rise of cloud computing has fundamentally altered the ownership and operational control of IT systems. Unlike traditional on-premises deployments, where clients managed the environment and compliance, cloud solutions place significant control—and therefore responsibility—in the hands of the provider. Providers manage infrastructure, update systems, and often dictate how data is processed, making them central to compliance efforts.

For example, an HR technology company developing an AI-driven recruitment system must now ensure the system does not create biases in hiring decisions, as required under the AI Act. Previously, clients using the system would have carried the risk of non-compliance with anti-discrimination laws.

> Unlike traditional on-premises deployments, where clients managed the environment and compliance, cloud solutions place significant control—and therefore responsibility—in the hands of the provider.

It can be argued that IT providers now face increasing requirements regarding the legality of their operations. An IT provider cannot operate in the market unless it delivers legally compliant systems. This shift is also reflected in contract practices.

IT provider accountability

This shift in the regulatory and technological landscape has led to a re-evaluation of responsibility in IT agreements. Providers are now increasingly expected to bear the primary burden of ensuring that systems comply with relevant laws. This change reflects the reality that providers are better positioned to address compliance at the design and operational levels, particularly in cloud-based environments where they control the underlying infrastructure.

However, clients still retain responsibilities, albeit in a more focused capacity. While providers must ensure the system's baseline legality, clients are responsible for ensuring that their use of the system aligns with their specific legal requirements and operational contexts.

For instance, a cloud-based CRM system may be GDPR-compliant in its design, but it is up to the client to ensure that the data they input and the manner of their processing adhere to GDPR principles, such as obtaining proper consent from data subjects. A cloud-based electronic health records provider, for instance, ensures its system meets regulatory data security requirements. However, it is up to the hospital using the system to ensure that patient consent mechanisms and data-sharing policies comply with applicable medical data legislation.

Evolving contract negotiations

These changes have also reshaped the negotiation process in IT agreements. Where earlier contracts might have included broad indemnities and disclaimers shifting compliance risks to the client, modern agreements now focus on delineating shared responsibilities. Providers typically accept liability for ensuring that the system is compliant with general legal standards, while clients agree to take responsibility for their specific use cases.

For example, providers may warrant that the system complies with data protection laws, does not infringe third-party IPR, and incorporates mechanisms to adapt to regulatory updates. Clients, on the other hand, may commit to using the system lawfully and within the scope of its intended purpose, ensuring compliance with industry-specific regulations or internal policies.

Moreover, EU regulations often require providers to offer tools and guidance to help clients meet their obligations. For instance, a provider might offer audit logs, compliance dashboards, or data localization options to assist clients in aligning with regional laws.

Further, when negotiating an agreement concerning an AI-powered chatbot for customer service, a provider may guarantee that the system adheres to AI Act requirements, while the client must define responsible use policies, such as disclosing to users that they are interacting with AI rather than a human.

Why the shift matters

The reallocation of compliance responsibility reflects a broader transformation in how IT services are delivered and consumed. It acknowledges the increasing complexity of regulatory landscapes, where a single system may be used across multiple jurisdictions, each with its own legal requirements.

By placing greater responsibility on providers, the regulatory environment seeks to ensure that systems are built with compliance as a fundamental feature, rather than an afterthought.

At the same time, this shift aligns with the practical realities of cloud computing. Clients no longer have the direct control over systems that they once did, making it both logical and necessary for providers to take on more accountability.

This accountability has already taken shape in the context of the Digital Services Act. Under the Act, an e-commerce platform provider must ensure that product listings comply with consumer protection laws. Previously, individual sellers were solely responsible. Platforms like Amazon and eBay have thus had to introduce proactive content moderation methods to avoid liability for counterfeit or unsafe products.

The future of it agreements

As EU regulations continue to evolve and cloud services dominate the IT landscape, the allocation of responsibilities in IT agreements will further solidify around this shared model. Providers must embrace their role as compliance leaders, integrating legal requirements into their systems by design and maintaining them throughout the system's lifecycle.

Clients, for their part, must focus on ensuring that their operational use aligns with the intended legal and ethical purposes.

This new paradigm creates a more balanced and collaborative approach, reducing risks for both parties while fostering trust and adaptability. For IT agreements to remain effective in this changing environment, clear communication, precise contractual terms, and a mutual understanding of responsibilities will be essential.

This evolution not only reflects the demands of modern technology and regulation but also sets the stage for more resilient and legally sound partnerships in the future.

Jaakko Lindgren, Partner, Dottir Attorneys og Sohrab Känkäinen, Associate, Dottir Attorneys.

Behandlingsgrunnlag for bakgrunnssjekk ved ansettelser

Av Stig Eidissen

Arbeidsgivere må behandle en rekke personopplysninger ved rekruttering av nye ansatte. I de senere år er det blitt mer vanlig med såkalte bakgrunnsundersøkelser ved ansettelser. Et sentralt spørsmål er hvilke(t) behandlingsgrunnlag etter personvernforordningen arbeidsgivere kan benytte for bakgrunnsundersøkelser.

1. Sentrale utgangspunkter

Det finnes ingen klar definisjon av bakgrunnsundersøkelser ved ansettelser. Normalt kan slike undersøkelser bestå av en bekreftelse av utdanning og yrkeserfaring, sjekk av sosiale medier, kredittvurdering eller andre forhold. Arbeidsgiver kan hente inn opplysninger utover det søker selv fremlegger, enten for å bekrefte at opplysninger i søknaden er korrekt, eller for å avdekke forhold som ikke er nevnt i søknaden. Bakgrunnsundersøkelser kan ha nokså ulikt omfang og formål. Det kan for eksempel være tale om å ivareta sikkerhetshensyn, eller arbeidsgivers omdømme.

Det er et krav til at behandling av personopplysninger må ha hjemmel i personvernforordningens artikkel 6 nr. 1 bokstav a–f. Bestemmelsen gir seks mulige hjemler for behandling av personopplysninger, men det er tilstrekkelig å ha behandlingsgrunnlag i ett av alternativene.

Stig Eidissen

De mest relevante behandlingsgrunnlagene for alminnelige bakgrunnsundersøkelser i artikkel 6 nr. 1 må antas å være samtykke (bokstav a), avtalegjennomføring (bokstav b) eller berettigede interesser (bokstav f).

> Bakgrunnsundersøkelser kan ha nokså ulikt omfang og formål. Det kan for eksempel være tale om å ivareta sikkerhetshensyn, eller arbeidsgivers omdømme.

Behandlingsgrunnlagene i artikkel 6 er kun tilstrekkelige dersom det er snakk om alminnelige personopplysninger. For sensitive personopplysninger (såkalte «særlige kategorier av personopplysninger») må behandlingen ha grunnlag i ett av alternativene i artikkel 9 nr. 2 bokstav a–j. Definisjonen av sensitive personopplysninger i artikkel 9 nr. 1 er vid. Den omfatter blant annet personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, fagforeningsmedlemskap, helseopplysninger og opplysninger om en persons seksuelle forhold eller seksuelle orientering.

Når en bakgrunnssjekk omfatter sensitive personopplysninger, må både alminnelig behandlingsgrunnlag og særskilt grunnlag for å behandle sensitive personopplysninger være oppfylt. Dersom grunnlag for å behandle sensitive personopplysninger mangler, må bakgrunnssjekken begrenses til kun å gjelde ordinære personopplysninger.

Bakgrunnsundersøkelser kan være nærmere regulert i enkelte særlover som for eksempel sikkerhetsloven. Denne artikkelen er begrenset til arbeidsgivers alminnelige adgang til å foreta bakgrunnsundersøkelser. Disse vil normalt være vesentlig mindre omfattende og inngripende enn bakgrunnsundersøkelser som eksempelvis foretas etter sikkerhetsloven.

2. Hvilke rettsspørsmål som er uavklarte knyttet til behandlingsgrunnlag ved bakgrunnsundersøkelser

Det er nokså lite offentlig tilgjengelig veiledning å hente for norske arbeidsgivere som skal vurdere lovligheten av bakgrunnsundersøkelser. Datatilsynets veiledning omfatter per dags dato kun innhenting av kredittvurdering og politiattest.[1] Datatilsy-

1 *https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/for-ansettelse---bakgrunnsundersokelser/* , sist sjekket 10. februar 2025.

net har ingen veiledning for eventuelle undersøkelser utover dette.

Helse- og omsorgsdepartementet har nylig gjennomført en høring av forslag til lovendring for å foreta bakgrunnssjekk til personell i kritiske stillinger i helse- og omsorgssektoren. Høringsnotatet utreder ikke behandlingsgrunnlag i nevneverdig grad, men legger til grunn at det uten særskilt lovhjemmel, er «begrenset anledning til bakgrunnssjekk av den enkelte som innehar eller søker en kritisk stilling».[2] Dette er i så fall en urovekkende rettstilstand i en tid med sterkt behov for å unngå unødvendig risiko ved ansettelser i kritiske stillinger. Som jeg skal gjennomgå i det videre kan både private og offentliges arbeidsgiveres handlingsrom være en del større enn det Helse- og omsorgsdepartementet synes å ha forutsatt i høringsnotatet.

I litteraturen er spørsmålet om behandlingsgrunnlag ved bakgrunnssjekker blant annet omtalt av Blekastad og Hirst i *Personvern og kontroll i arbeidslivet* (Oslo 2021) på side 145–147. Blekastad og Hirst oppfatter at samtykke er det mest brukte behandlingsgrunnlaget. Et samtykke må være frivillig avgitt for å være gyldig, og det stilles spørsmål ved om dette vil være tilfelle ved en mulig ansettelse. Videre peker de på artikkel 6 nr. 1 bokstav b (avtalegjennomføring) som et mulig grunnlag, og bokstav f (berettigede interesser) som det mest passende grunnlag. Samtidig mener forfatterne at berettigede interesser ikke kan tjene som grunnlag for behandling av sensitive personopplysninger etter artikkel 9 nr. 2, og at grunnlaget for sensitive personopplysninger i så fall må være samtykke. jf. artikkel 9 nr. 2 bokstav a.

Når det gjelder samtykke, har EU-domstolen klargjort at kravet om frivillighet ikke er oppfylt dersom en person kan nekte samtykke uten at det er til skade for vedkommende. I tillegg heter det i fortalen at samtykke ikke bør brukes i tilfeller med klar maktskjevhet, spesielt dersom den behandlingsansvarlige er en offentlig myndighet (se blant annet sak C-200/23 avsnitt 100 med videre henvisninger til personvernforordningens fortale). Det foreligger ofte en maktskjevhet mellom en arbeidsgiver og en arbeidstaker.

Hvor grensen for frivillig samtykke går, er uklart, og gjør samtykke som behandlingsgrunnlag til dels uforutsigbart. Det europeiske personvernrådets retningslinjer indikerer at både arbeidsgivere og offentlige myndigheter har et visst handlingsrom til å benytte samtykke som behandlingsgrunnlag.[3] Dette på tross av at det foreligger maktskjevhet for slike behandlingsansvarlige. Retningslinjenes poeng knyttet til frivillighet kan forstås slik at det i en del tilfeller ikke er noen reell grunn til å frykte negative konsekvenser ved å nekte samtykke. I andre tilfeller er de negative konsekvensene under enhver omstendighet begrenset til saklige følger av at den behandlingsansvarlige ikke får behandlet personopplysninger. Uten at jeg går i dybden på dette her, er jeg selv enig med Blekastad og Hirst i at samtykke kan være et gyldig behandlingsgrunnlag for bakgrunnsundersøkelser. Samtidig fremstår samtykke rettslig sett som noe usikkert, og arbeidsgivere kan derfor foretrekke å benytte et annet behandlingsgrunnlag.

Samtykke er imidlertid ikke det eneste grunnlaget for å behandle sensitive personopplysninger. Artikkel 9 nr. 2 bokstav b om gjennomføring av særlige rettigheter på området arbeidsrett kan også være aktuelt.

Jeg er enig i at berettigede interesser er et passende behandlingsgrunnlag for bakgrunnsundersøkelser så lenge arbeidsgiver har et saklig behov for å gjennomføre slike undersøkelser, jf. også Blekastad og Hirst. Et spørsmål er likevel om arbeidsgivere kan bruke behandlingsgrunnlaget som umiddelbart fremstår naturlig i både ansettelsesforhold og i ansettelsesprosesser generelt, nemlig bokstav b om avtalegjennomføring.

Jeg vil i denne artikkelen først se nærmere på artikkel 6 nr. 1 bokstav b om avtalegjennomføring som alminnelig behandlingsgrunnlag for bakgrunnsundersøkelser. Deretter vil jeg se på artikkel 9 nr. 2 bokstav b om gjennomføring av arbeidsrettslige rettigheter eller forpliktelser som grunnlag for behandling av sensitive personopplysninger.

I den grad en bakgrunnssjekk omfatter opplysninger om straffedommer og lovovertredelser gjelder også kravene etter personvernforordningen artikkel 10. Jeg går ikke nærmere inn i dette her.

3. Generelt om nødvendighetskravet knyttet til behandlingsgrunnlag

Personvernforordningen stiller et grunnleggende krav til at behandlingen skal være *nødvendig* for å oppnå de aktuelle og lovlige formålene, jf. artikkel 5 nr. 1 bokstav c. Samtlige behandlingsgrunnlag inneholder, i en eller annen form, et krav til at behandlingen er *nødvendig*. Dette gjelder også de grunnlag jeg her skal se nærmere på – artikkel 6 nr. 1 bokstav b, og artikkel 9 nr. 2 bokstav b. Det å tolke nødvendighetskravet riktig, er derfor avgjørende for å forstå rekkevidden av de ulike behandlingsgrunnlagene. Dette er også et område hvor handlingsrom-

2 Se Helse- og omsorgsdepartementets «Høringsnotat – Krav om bakgrunnssjekk av personell i kritiske stillinger og funksjoner …), tilgjengelig her: *https://www.regjeringen.no/contentassets/218f9c7d87f74d7eb2f8db3cdacc37f8/horingsnotat-krav-om-bakgrunnssjekk.pdf*, sist sjekket 10. februar 2025)

3 Se European Data Protection Board – Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 av 4. mai 2020 på s. 8–9 (tilgjengelig her: *https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf*)

met for behandlingsansvarlige tidvis fremstilles uriktig snevert.

EU-domstolen har uttalt om nødvendighetskravet i ulike sammenhenger at det innebærer et krav til at behandlingen må være strengt nødvendig. Tross dette utgangspunktet, har EU-domstolen samtidig klargjort at nødvendighetskravet i ulike behandlingsgrunnlag er oppfylt dersom et tiltak bidrar til å oppfylle et bestemt formål, og dette med rimelighet ikke kan oppnås like godt gjennom mindre inngripende tiltak (se blant annet sak C-439/19 *Penalty Points* avsnitt 109–110). Synspunktet har støtte i forordningens fortalepunkt 39. Det er ellers i tråd med hvordan nødvendighetskrav ofte tolkes som forholdsmessighetskrav i EU/EØS-retten generelt. Det er for øvrig korrekt lagt til grunn av Høyesterett i dommen HR-2021-2403-A *Legelisten* (se avsnitt 54–55, som gjaldt artikkel 6 nr. 1 bokstav f).

En slik tolkning innebærer at nødvendighetskravet ikke skal forstås i retning av at behandlingen må være *uunnværlig* knyttet til de ulike behandlingsgrunnlagene. Eksempelvis vil det være behandlingsgrunnlag for å utøve offentlig myndighet etter artikkel 6 nr. 1 bokstav e dersom en behandling bidrar til bedre eller mer effektiv utøvelse av offentlig myndighet, og dette samtidig ikke med rimelighet kan oppnås like godt gjennom mindre inngripende tiltak.

Begrepet *nødvendig* stiller som utgangspunkt krav til at behandlingen skal være *forholdsmessig*, men heller ikke mer. Så er et slikt forholdsmessighetskrav skjønnsmessig, og må anvendes strengere jo mer inngripende bruk av personopplysninger det er tale om.

4. Avtalegjennomføring som alminnelig behandlingsgrunnlag

Behandling som er nødvendig for å oppfylle en avtale har et eget behandlingsgrunnlag i personvernforordningen artikkel 6 nr. 1 bokstav b. Behandlingsgrunnlaget kan også dekke en viss behandling forut for avtaleinngåelse. Behandlingsgrunnlaget er formulert slik:

«[…] behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse.»

Det følger av ordlyden at den for det første dekker behandling som er nødvendig for å oppfylle en avtale som den registrerte er part i. Bestemmelsen dekker også tiltak på den registrertes anmodning før en avtaleinngåelse. Generelt er artikkel 6 nr. 1 bokstav b det mest praktiske behandlingsgrunnlaget i arbeidsforhold.

Det er ingen holdepunkter i forordningen for at nødvendighetskravet skal forstås annerledes enn etter de øvrige behandlingsgrunnlagene, og slik det er utdypet i fortalepunkt 39.

Når det gjelder bokstav b, har EU-domstolen likevel uttalt at behandlingen må være objektivt uunnværlig for et formål som er en integrert del av ytelsen til den registrerte. Dette er samtidig presisert slik at behandlingen må være vesentlig for å kunne oppfylle kontrakten, og dermed at det ikke finnes andre praktiske løsninger som er mindre inngripende (storkammersak C-252/21 *Meta Platforms Inc* avsnitt 98–99).

Det er uklart hvorfor EU-domstolen legger til grunn et strengere nødvendighetskrav akkurat knyttet til bokstav b. Til dels kan grunnen være at saken gjaldt nettopp Facebook-eier Meta, som er blant selskapene som skaper størst personvernutfordringer i Europa. Metas anførsler knyttet til behandlingsgrunnlag i saken, fremstår delvis som et forsøk på en omgåelse av personvernreglene. Samme tolkning er imidlertid også lagt til grunn i senere saker.[4] Det må derfor antas at EU-domstolen fremover vil tolke nødvendighetskravet strengere for bokstav b, enn de øvrige behandlingsgrunnlag.

For øvrige behandlingsgrunnlag er det tilstrekkelig at et tiltak gir et reelt *bidrag* knyttet til enten oppfyllelse av rettslig plikt eller noe annet, men for avtalegjennomføring må det være tale om et *vesentlig* bidrag. Akkurat hvor strengt dette kravet skal forstås, er uklart. Men det er uansett neppe særlig tvilsomt at det å vurdere og undersøke søkere til en stilling er vesentlig i forkant av en ansettelse.

Spørsmålet om hva som er vesentlig for den enkelte stilling, må vurderes konkret. I den utstrekning en bakgrunnsundersøkelse er nødvendig for at arbeidsgiver på et riktig, dekkende og tilstrekkelig sikkert grunnlag skal kunne ta stilling til avtaleinngåelsen, bør den normalt anses nødvendig. Samtidig må ikke bakgrunnsundersøkelsen være uforholdsmessig inngripende overfor arbeidssøkerne.

Vilkåret om at arbeidsgivers undersøkelser er et tiltak som skjer etter anmodning fra den registrerte selv bør også normalt være kurant å oppfylle: Gjennom å søke en stilling, ber man samtidig arbeidsgiver om og vurderes som en kandidat. Arbeidsgivers undersøkelser er da et tiltak som skjer etter anmodning fra den registrerte selv.

Arbeidsgiver må i alle tilfeller sørge for å oppfylle det grunnleggende kravet om en åpen og rettferdig behandling av personopplysninger, jf. artikkel 5 nr. 1 bokstav a. Dersom bakgrunnsundersøkelser går lengre enn det som er påregnelig for en arbeidssøker, bør arbeidsgiver på en egnet form gi tilstrekkelig informasjon om undersøkelsene som skal foretas. I motsatt fall vil kravet i bokstav b om at tiltak skal skje etter anmodning fra den registrerte neppe være oppfylt.

Etter mitt syn bør bakgrunnsundersøkelser derfor som utgangspunkt kunne foretas med artikkel 6 nr. 1 bokstav b (avtalegjennomføring) som behandlingsgrunnlag. Det må i den utstrekning arbeidsgiver er avhengig av bakgrunnsundersøkelser for å være tilstrekkelig trygg på at man velger riktig søker til stillingen.

4 Se sak C-17/22 *HTB Neunte* avsnitt 44 og sak C-394/23 *Mousse* avsnitt 34.

Åpenhets- og rettferdighetskravet tilsier for også at arbeidsgiver må sørge for tilstrekkelig kontradiksjon om forhold som bakgrunnsundersøkelsen avdekker. Jeg går ikke nærmere inn i dette her.

5. Kvalifikasjonsprinsippet som hjemmel for sensitive opplysninger etter artikkel 9 nr. 2 bokstav b

5.1 Generelt om hjemmel for sensitive personopplysninger i artikkel 9 nr. 2 bokstav b

Personvernforordningen artikkel 9 nr. 2 gir ti ulike grunnlag for å behandle sensitive personopplysninger. Alternativet i bokstav b lyder som følger:

> *«Behandlingen er nødvendig for at den behandlingsansvarlige eller den registrerte skal kunne oppfylle sine forpliktelser og utøve sine særlige rettigheter på området arbeidsrett, trygderett og sosialrett i den grad dette er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett, eller en tariffavtale i henhold til medlemsstatenes nasjonale rett som gir nødvendige garantier for den registrertes grunnleggende rettigheter og interesser.»*

Bestemmelsen gir arbeidsgivere grunnlag for å behandle personopplysninger både for å oppfylle *forpliktelser* og utøve *rettigheter* innenfor området *arbeidsrett*. Ordlyden er vid. At bestemmelsen må tolkes i tråd med ordlyden er også i samsvar med fortalepunkt 52. Av fortalepunktet fremgår det at unntaket fra forbudet om å behandle sensitive personopplysninger bør tillates når det er fastsatt i unionsretten eller medlemsstatenes nasjonale rett, og det omfattes av nødvendige garantier som sikrer vern av personopplysninger (…), særlig behandling av personopplysninger på området arbeidsrett …». Det å ansette arbeidstakere faller innenfor ordlyden i «området arbeidsrett». En slik forståelse underbygges også av begrepsbruken ellers i forordningen. Artikkel 88 gir hjemmel til nasjonale særbestemmelser knyttet til ansettelsesforhold. Bestemmelsen nevner spesifikt rekruttering som en av mange behandlingssituasjoner i tilknytning til ansettelsesforhold.

Dette innebærer at artikkel 9 nr. 2 bokstav b må forstås slik at den åpner for at behandlingsansvarlige kan behandle sensitive personopplysninger ved ansettelser, så lenge dette er tillatt enten etter EØS-retten eller medlemsstatenes nasjonale rett.

5.2 Personopplysningsloven § 6 som nasjonalt rettsgrunnlag for behandling av sensitive personopplysninger

Personopplysningsloven § 6 gir en generell hjemmel for behandling av sensitive personopplysninger i arbeidsforhold. Bestemmelsen lyder som følger:

> *«Personopplysninger som nevnt i personvernforordningen artikkel 9 nr. 1 kan behandles når det er nødvendig for å gjennomføre arbeidsrettslige plikter eller rettigheter.»*

Det er i lovforarbeidene til bestemmelsen forklart at bestemmelsen åpner for behandling av sensitive personopplysninger på grunnlag av personvernforordningen artikkel 9 nr. 2 bokstav b. Samtidig er det presisert at bestemmelsen kun gjelder for behandling av opplysninger «på arbeidsrettens område, ikke for trygderettslige eller sosialrettslige formål». Det er videre understreket at bestemmelsen viderefører gjeldende rett etter den forrige personopplysningsloven (se Prop. 56 LS (2017-2018) s. 212). I den forrige personopplysningsloven ble det presisert at uttrykket arbeidsrettslige plikter eller rettigheter «omfatter alle plikter og rettigheter som hviler på et arbeidsrettslig grunnlag, uansett om grunnlaget er lovgivning, avtale mellom partene i arbeidslivet, eller individuelle arbeidsavtaler» (se Ot. Prp. nr. 92 (1998-1999) s. 110–111. Departementet understreket også i forarbeidene at de hadde valgt en ordlyd som lå tettere på den daværende direktivteksten enn det aktuelle lovutvalget hadde foreslått.

Det er nærliggende å forstå lovforarbeidene slik at personopplysningsloven § 6 er ment å gi nasjonal hjemmel for å behandle sensitive personopplysninger så langt personvernforordningen artikkel 9 nr. 2 tillater. En slik tolkning er også i tråd med ordlyden i bestemmelsen. Dette innebærer at kravet i artikkel 9 nr. 2 til behandlingsadgangen må fremgå av nasjonal rett, må anses oppfylt. Det avgjørende er derfor i hvilken utstrekning en bakgrunnssjekk kan anses for å være nødvendig for at den behandlingsansvarlige enten kan oppfylle sine forpliktelser, eller utøve sine særlige rettigheter, på området for arbeidsrett.

5.3 I hvilken utstrekning bakgrunnssjekk oppfyller forpliktelser eller utøver rettigheter innenfor området arbeidsrett

Vurderingen om en bakgrunnssjekk kan anses å oppfylle forpliktelser eller utøve rettigheter innenfor området arbeidsrett, må ta utgangspunkt i at formuleringen er meget vid. Etter ordlyden omfattes all form for oppfyllelse av forpliktelse eller utøvelse av rettigheter, så lenge dette skjer innenfor området arbeidsrett.

Innenfor området arbeidsrett er retten til å velge sine egne ansatte generelt sett på som en rettighet for arbeidsgiver. I forbindelse med innføring av forbudet mot etnisk diskriminering ved ansettelser i 1997, tok flere høringsinstanser opp spørsmålet om innføring av et generelt saklighetskrav ved ansettelser i privat sektor. Arbeidsdepartementet uttalte da at arbeidsgivers «rett til å velge sine ansatte er tradisjonelt en viktig del av arbeidsgivers styringsrett».[5] Selv om diskrimineringsvernet er bygd ut si-

5 Se Ot. prp. nr. 67 (1996-1997) Om lov om endringer i lov av 4 februar 1977 om arbeidervern og arbeidsmiljø m.v. s. 46).

den den gang, er utgangspunktet i privat sektor fremdeles at arbeidsgiver selv velger sine egne ansatte. Høyesterett har konkret slått fast at arbeidsgiveren i kraft av sin styringsrett bestemmer hvilke kvalifikasjoner som skal kreves for ansettelse, og hvordan ulike kvalifikasjonskrav skal veies mot hverandre. Domstolene kan kun prøve om det foreligger misbruk av styringsretten, og foreta en saklighets- og forsvarlighetskontroll av kvalifikasjonskravene[6].

I utgangspunktet er det derfor grunnlag for å si at det å undersøke og å velge den best kvalifiserte søkeren er en rettighet for arbeidsgivere innenfor området arbeidsrett. Et motargument mot dette er at retten til å velge egne ansatte egentlig bare er et uttrykk for den generelle avtale- og handlefriheten til virksomheter. I den forstand kan det argumenteres med at det ikke er tale om noen særskilt rettighet innenfor området arbeidsrett.

Tradisjonelt er imidlertid det å fastsette kvalifikasjonskrav, vurdere søkere, og å ansette den best kvalifiserte, sett på som en arbeidsrettslig rettighet for arbeidsgivere. Det er derfor innenfor ordlyden i personopplysningsloven § 6, og sannsynligvis tilstrekkelig for å være dekket av personopplysningsloven § 6 generelle hjemmel til å gjennomføre arbeidsrettslige forpliktelser eller rettigheter. Etter personvernforordningen artikkel 9 nr. 2 bokstav b er det uansett et krav at nasjonal rett skal gi tilstrekkelige personverngarantier for berørte privatpersoner. Dette kommer jeg tilbake til nedenfor.

Dersom man forholder seg til offentlig sektor, er kvalifikasjonsprinsippet på sin side et sentralt rettslig prinsipp ved ansettelser.[7] Det fungerer både som en rettighet, men også som en forpliktelse for offentlige arbeidsgivere. Sivilombudet behandler ofte klager mot offentlige arbeidsgivere på bakgrunn av angivelige brudd på kvalifikasjonsprinsippet. For offentlig sektor er det derfor på det rene at det å velge ut kvalifiserte og den best kvalifiserte søkeren til en stilling, også er tale om å oppfylle *forpliktelser* på området arbeidsrett. Det er derfor enda mindre tvilsomt at kvalifikasjonsprinsippet er dekket av personopplysningsloven § 6 for offentlige arbeidsgivere.

5.4 Ivaretakelse av nødvendige garantier for personvernet

En forutsetning for å behandle sensitive personopplysninger etter artikkel 9 nr. 2 bokstav b, er at nasjonal rett gir «nødvendige garantier for den registrertes grunnleggende rettigheter og interesser». Det er lite veiledende praksis om hva som ligger i dette kravet.

Norsk rett har på sin side en del sentrale begrensninger for å verne om arbeidstakeres personvern i rekrutteringssituasjoner.

For det første er det mulig at bakgrunnsundersøkelser må anses som kontrolltiltak etter arbeidsmiljøloven § 9-1, og derfor må oppfylle krav til saklighet og forholdsmessighet. Det som gjør rekkevidden av bestemmelsen noe usikker, er at den etter ordlyden kun gjelder for kontrolltiltak mellom arbeidsgiver og arbeidstaker. I utgangspunktet omfattes ikke arbeidssøkere. At arbeidssøkere kan være omfattet, støttes imidlertid blant annet av den konkrete bestemmelsen i aml. § 9-3, som setter begrensninger for innhenting av helseopplysninger ved ansettelse. Jeg går ikke nærmere inn i dette spørsmålet her. Spørsmålet har uansett begrenset betydning for søkernes personvern, fordi personvernforordningen uansett stiller nokså sammenlignbare krav til saklig grunn og forholdsmessighet.

Uavhengig av om bakgrunnsundersøkelser generelt faller innenfor arbeidsmiljølovens generelle krav til kontrolltiltak, gir arbeidsmiljøloven § 9-3 uansett arbeidssøkere et vern mot innhenting av uforholdsmessige helseopplysninger ved ansettelse. Videre setter aml. § 13-4 begrensninger for innhenting av opplysninger om politiske standpunkt. Hva som anses som nødvendige garantier må vurderes i lys av de rettigheter personer allerede har etter personvernforordningen. Personvernforordningens generelle begrensninger i artikkel 5, kombinert med blant annet regler om innsyn, retting og sletting, er også viktige. Reglene sperrer blant annet for at arbeidsgivere kan gjennomføre uforholdsmessige bakgrunnsundersøkelser ved ansettelser.

Samlet sett tilsier dette at norsk rett generelt har nødvendige garantier for den registrertes grunnleggende rettigheter og interesser knyttet til ansettelsesprosesser for at personopplysningsloven § 6 sammenholdt med kvalifikasjonsprinsippet er gyldig som nasjonalt rettsgrunnlag etter personvernforordningen artikkel 9 nr. 2 bokstav b.

6. Oppsummering

Arbeidsgivere har behandlingsgrunnlag til å gjennomføre nødvendige bakgrunnssjekker ved ansettelse etter personvernforordningen artikkel 6 nr. 1 bokstav b. For sensitive personopplysninger gjelder personvernforordningen artikkel 9 nr. 2 bokstav b, jf. personopplysningsloven § 6 og kvalifikasjonsprinsippet som nasjonalt rettsgrunnlag. Dette innebærer at arbeidsgivere kan gjennomføre bakgrunnsundersøkelser også for sensitive personopplysninger uten den rettslige usikkerheten som knytter seg til samtykke som behandlingsgrunnlag.

Stig Eidissen har Master i rettsvitenskap fra 2010 og PhD i rettsvitenskap fra 2020. Han arbeider i det daglige som advokat i KS Kommunesektorens organisasjon og som Førsteamanuensis II ved UiT Norges arktiske universitet.

6 HR-2014-831-A avsnitt 69. Se også Jan Fougner, *Norsk arbeidsrett. Styringsrett, samarbeid og arbeidstakervern* (Universitetsforlaget, 2019) s. 107.

7 Se blant annet Prop. 94 L (2016-2017) Lov om statens ansatte mv. (statsansatteloven) punkt 9.1.

Bedre personvern med samtykkebasert deling av data

Av Steinar Skagemo

Innledning

Datatilsynet og Teknologirådet arrangerte Personverndagen den 28. januar 2025. Temaet i år var en ordentlig klassiker: Hvordan lykkes med datadeling og personvern? Innleggene var preget av et ønske om å få til datadeling uten at det går på bekostning av personvernet. Jeg mener premisset er feil. Deling av data kan *styrke* personvernet. Men da må vi passe på at vi gjør det riktig. Min klare oppfatning er at vi idag beveger oss i en retning der vi svekker mange personers personvern unødvendig, fordi offentlig sektor unngår å bruke samtykkebasert deling.

I denne artikkelen vil jeg først se nærmere på hvordan digital[1] deling av opplysninger styrker personvernet – uavhengig av om delingen er basert på samtykke eller ei. Deretter vil jeg se på det som kanskje er den største utfordringen ved deling: Økt risiko for personopplysninger på avveie.

For å tydeliggjøre hvordan risikoen for opplysninger på avveie påvirkes av om deling skjer basert på lovhjemmel eller samtykke, vil jeg gå gjennom eksempler på hvordan inntektsopplysninger fra Skatteetaten deles, henholdsvis med lovhjemmel og samtykke.

Det er både uklarhet og delte meninger om offentlig sektor har lov til å dele data basert på samtykke. Så for å forsvare at temaet i denne artikkelen i det hele tatt er verdt å diskutere, vil jeg vise hvorfor jeg mener samtykkebasert deling er lovlig. I forlengelsen av det ser jeg nærmere på hvordan kravet om frivillighet kan ivaretas, ved hjelp av en avgjørelse i Personvernnemnda som gjaldt reglene for bostøtte.

Steinar Skagemo

I de siste delene av artikkelen ser jeg først på et eksempel på de negative effektene når vi *ikke* kan dele egne opplysninger etter eget ønske. Deretter skriver jeg om et samarbeid mellom KS og Skatteetaten som har ført til en drastisk økning i kommunenes tilgang til inntektsopplysninger, der bruk av samtykke ikke blir vurdert. Videre foreslår jeg noen tiltak for å få en riktigere balanse mellom hjemmel og samtykke fremover. Avslutningsvis foreslår jeg hvordan vi kan sikre et bedre personvern når data først deles basert på lovhjemmel.

Fordeler ved digital deling av personopplysninger

Hvis vi tar utgangspunkt i den tradisjonelle måten vi har formidlet inntektsopplysninger på ved søknader om ytelser i offentlig sektor, har det typisk vært en kombinasjon av å skrive inn verdiene på et papirskjema, eller taste dem inn på et skjema på en nettside. I begge tilfeller er det nødvendig å legge ved dokumentasjon som bekrefter opplysningene. Dokumentasjonen er typisk skatteoppgjøret og lønnsslipper.

Hvis vi sammenligner med den tradisjonelle måten å gjøre det på, er det spesielt på to måter digital deling av personopplysninger direkte fra Skatteetaten bidrar til å styrke personvernet:[2] bedre datakvalitet og dataminimering.

Digital deling kan gi bedre datakvalitet fordi det reduserer faren for feil, enten som følge av tastefeil eller at søkeren misforstår hvilke opplysninger det blir spurt etter. (Det forutsetter selvsagt at det ikke er en misforståelse mellom avgiver og mottaker om *meningen* i dataene som deles.)

Når det gjelder dataminimering kan det oppnås på to måter. For det første i form av mindre overskuddsinformasjon. Dokumentasjonen som legges ved inneholder ofte tilleggsinformasjon som ikke er relevant for saksbehandlingen.[3] For det andre kan dataminimering oppnås ved at delingstjenestene settes opp til å svare på spørsmål/vilkår, istedenfor å levere de detaljerte opplysningene som er grunnlaget for å bestemme om vilkåret er oppfylt. For eksempel kan et API svare på om en person er over 18 år, uten å levere ut fødselsdatoen. Tilsvarende kan gjelde for inn-

1 Temaet er digital deling og hvordan det påvirker personvernet. Men jeg vil for enkelhets skyld bare bruke «deling» heretter.

2 Daværende seksjonssjef for informasjonssikkerhet i Difi, Lillian Røstad, skrev en kronikk som svar til Datatilsynet i 2014, for å vise hvordan deling kan styrke personvernet og informasjonssikkerheten. Se: *https://www.digi.no/artikler/deling-er-ikke-farlig/289733*

3 Dette ble bl.a. trukket frem av daværende skattedirektør Hans Christian Holte ved lanseringen av Samtykkebasert lånesøknad, se: *https://www.skatteetaten.no/presse/nyhetsrommet/enklere-a-soke-boliglan/*

tektsgrenser eller antall barn under 18 i husstanden, i tillegg til mer komplekse, utledete verdier.

Bedre datakvalitet gjennom mindre fare for misforståelser, og dataminimering, gjennom at det kun er de relevante opplysningene som deles, trekker begge deler i retning av en tydeliggjøring av hvilke opplysninger om innbyggeren som skal behandles. Sånn sett bidrar begge deler til å gi innbyggerne bedre informasjon om behandlingen, som igjen styrker personvernet.

Felles for de fordelene for personvernet som jeg har nevnt over, er at de kan oppnås uavhengig av om delingen skjer med lovhjemmel eller med samtykke fra brukeren. Dersom vi av ulike grunner *lar være* å dele opplysninger, går vi glipp av disse personvernfordelene for innbyggerne. Å la være å dele har derfor en effekt på personvernet.

Økt risiko for opplysninger på avveie gir redusert kontroll

Deling av personopplysninger er åpenbart ikke bare en kilde til fordeler for personvernet. Siden jeg er spesielt opptatt av å få frem forskjellen mellom deling basert på lovhjemmel og samtykke, vil jeg se nærmere på en trussel for personvernet som påvirkes i stor grad av om delingen skjer på den ene eller andre måten: Risikoen for personopplysninger på avveie.[4]

«Fysiske personer bør ha kontroll over egne personopplysninger» står det i fortalepunkt 7 til personvernforordningen, og i flere sammenhenger blir kontroll over egne opplysninger trukket frem som en kortversjon av hva personvern handler om.[5] Når egne personopplysninger kommer på avveie, har man helt klart mistet kontrollen over dem; vi vet ikke hvem som har opplysningene eller hva de brukes til.

> Dersom vi av ulike grunner *lar være* å dele opplysninger, går vi glipp av disse personvernfordelene for innbyggerne. Å la være å dele har derfor en effekt på personvernet.

Etter min mening reduseres kontrollen over egne opplysninger allerede *før* opplysningene faktisk kommer på avveie, dersom det skjer noe som øker risikoen for at det kan skje. Det kan sammenlignes med at banken min bestemmer seg for å konvertere min høyrentekonto til et aksjefond, uten at jeg får et valg om å beholde pengene på høyrentekontoen. Selv om det ikke skjer noen endringer i første omgang, eller kanskje jeg til og med blir rikere, har noen tatt en beslutning som endrer risikoen jeg utsettes for.

Når det gjelder spørsmålet om graden av kontroll over risikoen for personopplysninger på avveie, er det etter min mening relevant å stille spørsmålet om jeg er i en situasjon der jeg kan *hindre* at opplysninger om meg blir utsatt for økt risiko. Hvis jeg ikke har mulighet til å hindre den økte risikoen, betyr det at jeg har fått redusert kontrollen over egne opplysninger, og dermed er personvernet mitt svekket.

Deling av inntektsopplysninger med lovhjemmel

For å tydeliggjøre hvordan risikoen øker ved deling, skal jeg se nærmere på Skatteetatens deling av inntektsopplysninger med andre via API.

Skal Skatteetaten løse sitt samfunnsoppdrag er det nødvendig at inntektsopplysningene er tilgjengelige for relevante saksbehandlere og systemer internt i Skatteetaten. De må samtidig beskytte seg mot hacking og utro tjenere for å hindre at opplysningene kommer på avveie.

Skatteetaten har en lang historie med å gjøre inntektsopplysningene tilgjengelig for andre, som f.eks. SSB, Nav og Husbanken. For disse finnes det lovhjemler som gir dem direkte tilgang til inntektsopplysninger fra Skatteetaten.

Det at opplysningene gjøres tilgjengelige for andre, fører til at det oppstår noen nye måter opplysningene kan komme på avveie på.

Skal for eksempel Husbanken få tilgang til opplysningene, tilbyr Skatteetaten et grensesnitt for maskin-til-maskin-kommunikasjon, et API. Skatteetaten må i den forbindelse sikre API-et mot ulike former for innbrudd og uautorisert bruk, for eksempel hindre at noen andre enn Husbanken klarer å bruke API-et til å hente ut inntektsopplysninger. Dette har Skatteetaten lang erfaring med. Et viktig spørsmål er om risikoen for at noen klarer å komme seg forbi Skatteetatens sikkerhetsmekanis-

4 En ulempe som er spesifikk for digital deling, men som jeg ikke vil gå nærmere inn på her, er at de som avgir opplysningene får vite hvem som mottar dem. Hvis brukeren selv sender inn dokumentasjon om inntekt, får ikke Skatteetaten vite at en person søker bostøtte. Dette er også et av poengene til Personvernnemnda i saken jeg omtaler senere i artikkelen. Å løsrive avgiver og mottaker ved digital deling er forøvrig teknisk mulig, for eksempel med en tredjepart i mellom. Det er også en av fordelene flere trekker frem ved innføringen av såkalte «lommebøker» (wallets) for deling av opplysninger.

5 Se bl.a. regjeringens sider «Hva er personvern?», *https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/hva-er-personvern/id448290/* Datatilsynet har flere ganger brukt formuleringen «Den enkeltes rett til å ha kontroll med egne personopplysninger» som definisjon av personvern, se bl.a. *https://www.nokios.no/wp-content/uploads/presentasjoner/2017/s3b-gdpr-datatilsynet-martha-eike.pdf*

mer, øker dersom Skatteetaten lar flere aktører få tilgang til API-ene de tilbyr. Etter min mening kan det like gjerne være motsatt: Desto flere aktører Skatteetaten åpner API-ene for, desto mer oppmerksomhet får antageligvis både den tekniske og organisatoriske sikkerheten rundt API-en. I beste fall går altså risikoen ned. Dersom det er en økning i risiko for hver ny aktør som får tilgang, er økningen neppe særlig stor. De fleste sikkerhetsmekanismene, som for eksempel brannmurer og overvåkning, vil være upåvirket av om det legges til en ny aktør.

En økt risiko for opplysninger på avveie er med andre ord i liten grad knyttet til selve Skatteetaten som mål for hackere og utro tjenere. Den viktige endringen er at nye aktører som får tilgang til Skatteetatens API-er, blir nye mål for hackere eller utro tjenere som er på jakt etter inntektsopplysningene våre.

For å fortsette med Husbanken som eksempel: Ettersom Skatteetaten ikke kan vite på forhånd hvem som er aktuelle for å søke bostøtte fra Husbanken, må de stole på at Husbanken bare henter ut inntektsopplysninger når det er rettslig grunnlag for det, altså i forbindelse med saksbehandling.[6] En utro tjener eller hacker som lykkes med å få tilgang til de rette rollene eller systemene hos Husbanken, vil derfor kunne hente inntektsopplysninger om hvem de vil fra Skatteetatens API. Skatteetaten har ikke noen måte å vite om API-kall fra Husbanken er legitime eller ei.[7]

Det betyr at for hver ny aktør som får direkte tilgang til inntektsopplysninger fra Skatteetaten, øker risikoen for opplysninger på avveie, fordi angrepsflaten i form av organisasjoner (personer/roller og systemer) med tilgang til opplysningene, blir større.[8]

Men vi kan si noe mer presist om hvordan den økte risikoen treffer alle de som Skatteetaten har inntektsopplysninger om. Det er et skille mellom den gruppen som *uansett* vil utsettes for økt risiko, fordi de søker om bostøtte.[9] For denne gruppen er datadelingen en fordel, både for personvernet (dataminimering, økt datakvalitet og ingen økt risiko for opplysninger på avveie), samt gjennom enklere søknadsprosess og raskere saksbehandling. Men alle de andre som har inntektsopplysninger hos Skatteetaten får derimot ingen fordeler.[10] Isteden fører datadelingen kun til økt risiko for opplysninger på avveie, og redusert kontroll over egne opplysninger for denne gruppen.

Vi kan sette opp dette som et forholdstall. Alle personer Skatteetaten har inntektsopplysninger om er personer Skatteetaten *trenger* inntektsopplysninger om, for å løse samfunnsoppdraget sitt. Det er med andre ord et 1:1-forhold til personer Skatteetaten *har tilgang* til inntektsopplysninger om og som de *trenger* opplysninger om.

Husbanken derimot, har tilgang til inntektsopplysningene til alle som finnes i Skatteetatens systemer, til tross for at de bare behandler saker om ca. en tidel av befolkningen hvert år.[11] Det er derfor et 1:10-forhold mellom personer Husbanken trenger opplysninger om, og personer som får økt risiko for opplysninger på avveie, uten at opplysningene er relevante for Husbanken.

Det er sikkert delte meninger om et forholdstall på 1:10 er lavt, og derfor lett å akseptere, eller om det er altfor høyt. Her kommer det også inn momenter som hvor stor betydning tilgangen har for de som har minst, og er mest avhengig av bostøtte. Det er uansett ikke noen tvil om at lovgiver har ønsket at Husbanken skal ha tilgang til inntektsopplysninger fra Skatteetaten, og disse tilgangene er gitt gjennom lov- og forskriftsprosesser der det har

6 Fra vilkårene for deling: «Partene, som er Skatteetaten og Konsumenten, plikter å følge sine lovpålagte krav til innhenting, utlevering og behandling av opplysningene. Opplysningene som utveksles skal ikke benyttes til formål som faller utenfor det rettslige grunnlaget.» (min utheving) Kilde: *https://www.skatteetaten.no/globalassets/deling/dokumenter/delingsvilkar-1.3-konsument.pdf*

7 Det er helt sikkert noen mekanismer som vil slå alarm og stanse tilgangen dersom det kommer uvanlig mange forespørsler fra Husbanken over kort tid, men med varsom bruk av en slik ulovlig tilgang, er det grunn til å tro at det vil være mulig å hente ut opplysninger om mange personer over tid. Husbanken vil trolig også forsøke å sikre at det er sammenfall mellom saker i saksbehandlingssystemet og oppslag mot Skatteetatens API, og på den måten fange opp misbruk. Men det endrer ikke poenget med at den digitale delingen med Husbanken åpner en ny vei inn til inntektsopplysningene i Skatteetaten, og at informasjonssikkerheten i Husbanken er avgjørende for hvor vanskelig det er å utnytte den.

8 At risikoen uunngåelig øker, betyr selvsagt ikke at vi *aldri* bør åpne for direkte tilgang til inntektsopplysninger basert på lovhjemmel.

9 Hvis vi ikke hadde hatt deling av inntektsopplysninger mellom Skatteetaten og Husbanken, men prosessen isteden hadde vært basert på at søkerne sendte inn opplysninger og dokumentasjon som så ble registrert i Husbankens systemer, ville hackere eller utro tjenere som lyktes med å få uautorisert adgang til Husbankens systemer, også fått tilgang til inntektsopplysninger om alle som søker bostøtte.

10 Det kan argumenteres for at den gruppen som ikke selv søker bostøtte har fordelen av datadelingen gjennom at kostnadene til administrasjon av bostøtteordningen blir lavere og at det reduserer faren for misbruk, og dermed blir det lavere skatter og et bedre sikkerhetsnett. Men dette er fordeler som i stor grad også kan oppnås ved samtykkebasert deling.

11 Dette er min gjetting basert på at antall søkere om bostøtte i 2023 ifølge Husbankens årsrapport var 190.000 og at jeg antar at hver søker representerer en husstand med mellom to og tre personer.

vært mulig å komme med motforestillinger.[12]

Men det finnes eksempler der forholdstallene er mye større, og hvor det er uklart om prosessen med å gi lovhjemmel har gitt en god diskusjon om avveiningene. På dokumentasjonssiden til Skatteetatens API-er finner vi en rekke tjenester og aktører. Der står det også om tilgangen er basert på hjemmel eller samtykke. En av ordningene i lista er reindriftstilskudd, og tilgangen er basert på lovhjemmel.[13]

Ifølge Landbruksdirektoratets nettsider er ca. 3000 personer involvert i reindrift i Norge.[14] På samme måte som med bostøtte, er det vanskelig å se for seg at Skatteetaten på forhånd har en oversikt over hvem som kvalifiserer til reindriftstilskudd. Jeg antar Skatteetatene må stole på den Statsforvalteren som behandler søknadene, når sistnevnte sender forespørsler om inntektsopplysninger til Skatteetatens API. Gitt at hver eneste av de 3000 personene involvert i reindrift søker driftstilskudd (noe som neppe er sannsynlig) er forholdstallet 1 til 2500 mellom de som uansett ville utsatt seg for risiko ved å sende Statsforvalteren inntektsopplysninger om seg selv som del av en søknad, og de som får egne opplysninger utsatt for økt risiko for å komme på avveie fordi delingen er basert på lovhjemmel.[15]

Som eksemplene over viser vil deling av data basert på lovhjemmel øke risikoen for at opplysningene som er tilgjengelige i API-et kommer på avveie. For hver etat som får lovhjemmel til å hente data fra API-et, øker angrepsflaten.[16] Det rammer ulikt mellom de som uansett ville delt opplysningene sine med mottakerne, og som dermed oppnår forbedret personvern, og resten, som kun får svekket personvernet. For ulike etater og tjenester er det store forskjeller i forholdstallet mellom disse gruppene. Innbyggernes kontroll over egne opplysninger reduseres for hver ny aktør som får tilgang til opplysningene basert på lovhjemmel, siden det fratar dem muligheten til å stoppe deling av egne opplysninger.

Deling av inntektsopplysninger med samtykke

Fra å se på hvordan deling basert på lovhjemmel svekker kontrollen over egne opplysninger, skal jeg se nærmere på hva som skjer ved samtykkebasert deling.

Mange norske lesere har sannsynligvis erfaring med løsningen «samtykkebasert lånesøknad» (SBL). SBL ble lansert i juni 2017[17], og som ifølge estimater fra 2018 gir samfunnet 13 milliarder i gevinster over 10 år.[18]

Før SBL var det mulig å søke banklån digitalt, og prosessen var som mange digitale tjenester fortsatt er idag: Underveis i søknaden ble brukeren bedt om å oppgi samlet inntekt, gjeld og formue for forrige år og lønn for de siste månedene. Siden dette var opplysninger søkeren fylte ut selv, trengte bankene dokumentasjon som bekreftet opplysningene. Det siste steget i søknaden var derfor å laste opp bilder eller pdf-er av skatteoppgjør og lønnsslipper. Brukeren hadde med andre ord en rolle i å «punche» opplysninger fra papir/pdf, mens banken måtte bruke tid på å kontrollere om de innsendte opplysningene var korrekte.

SBL forbedrer denne prosessen på to måter. Søkeren blir bedt om å samtykke til at banken kan hente opplysningene fra Skatteetaten. Det sparer brukeren både for å finne frem og deretter punche dataene selv, og til slutt laste opp bilder/pdf-er. Samtidig slipper banken å kontrollere de oppgitte opplysningene mot dokumentasjonen, fordi de får dataene direkte fra kilden (Skatteetaten).

Det er flere forhold ved SBL som bidrar til bedre personvern, sammen-

12 I 2015 ble det gjort endringer i lov om bostøtte, som ga tydelige hjemler til innhenting av opplysninger fra andre både til saksbehandling og kontroll, og Datatilsynet uttalte seg positivt til endringene. Se mer om bostøtteordningen og lovendringen senere i artikkelen.

13 Se: *https://skatteetaten.github.io/api-dokumentasjon/api/inntekt?tab=Om+tjenesten*

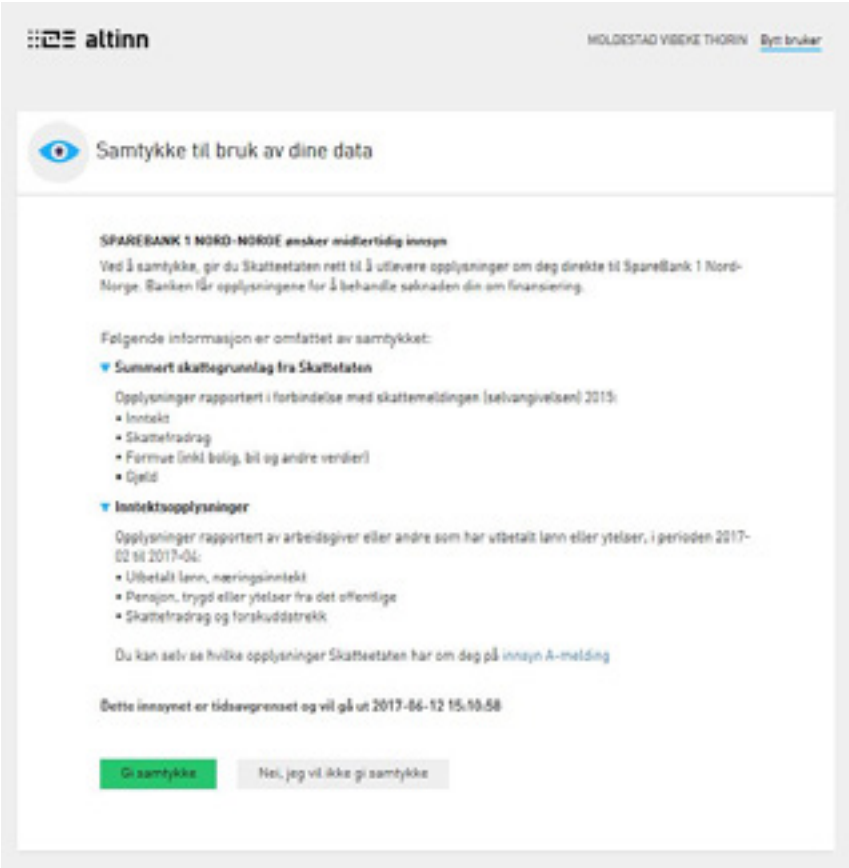
14 Se: https://www.landbruksdirektoratet.no/nb/reindrift/reindrift-i-norge/reindriftsnaeringen

15 Hvilke vurderinger ligger bak lovhjemmelen for å dele inntektsopplysninger digitalt i forbindelse med reindriftstilskudd? Hjemmelen fremgår av forskrift om reindriftstilskudd, og den aktuelle regelen som gir adgang til å hente opplysninger direkte fra Skatteetatens API kom inn gjennom en forskriftsendring i 2023, se: *https://lovdata.no/pro/#document/LTI/forskrift/2023-06-21-1014*. Forskriftsendringen fulgte av reindriftsavtalen. Såvidt jeg har klart å finne ut har ikke regelendringen som førte til lovhjemmel for å hente inntektsopplysninger, vært på høring.

16 I noen tilfeller kan kanskje Skatteetaten til en viss grad vite på forhånd hvilke personer det er relevant for etatene å be om opplysninger om, for eksempel aldersgrupper, kommunetilhørighet eller lignende.

17 Se pressemeldingen fra Skatteetaten: *https://www.skatteetaten.no/presse/nyhetsrommet/enklere-a-soke-boliglan/*

18 Se *https://forenkling.brreg.no/dsop-oppsummerer-2018-enklere-hverdag-og-store-gevinster/*
SBL er resultat av et samarbeid mellom finansnæringens interesseorganisasjon, Finans Norge, og de to statlige virksomhetene Skattedirektoratet og Brønnøysundregistrene. Finans Norge representerte bankene, Skattedirektoratet samler inn og satt på oppdaterte opplysninger om nordmenns inntekt, og Brønnøysundregistrene hadde på den tiden ansvaret for Altinn, som ble videreutviklet slik at en innlogget bruker kunne gi et samtykke til å utlevere opplysninger fra Skatteetaten. SBL vant Digitaliseringsprisen i 2018.



lignet med den gamle løsningen. For det første fører løsningen til høyere datakvalitet, siden det er mindre fare for at brukeren taster feil, eller misforstår hvilke opplysninger søknadsskjemaet spør etter. Korrekte data gir lån som står i forhold til lånetakernes låneevne. Og motsatt.

SBL bidrar også til dataminimering. Kun opplysninger som skattemyndighetene mener bankene har rett til å motta for behandling av lånesøknaden, blir utlevert fra Skatteetaten.

Dette er eksempler på positive effekter for personvernet ved digital deling av opplysninger. For å forstå effekten av at delingen er samtykkebasert, skal vi se nærmere på hvordan SBL påvirker risikoen for personopplysninger på avveie.

Hvis vi sammenligner med bostøtte fra Husbanken, så er situasjonen den samme for alle som ønsker lån: For å få lån må jeg godta at banken trenger å vite noe om økonomien min. Alle som søker lån får dermed økt risiko for opplysninger på avveie som følge av at banken de søker hos, får tilgang til inntektsopplysningene.

Hva med alle de som ikke søker lån? Som det fremgår av skjermbildet over er det Skatteetaten som ber brukeren bekrefte om inntektsopplysninger skal utleveres til banken. For å bekrefte må brukeren være autentisert via ID-porten. Banken har med andre ord *ikke* tilgang til inntektsopplysninger hos Skatteetaten, før brukeren «åpner opp» for banken ved å klikke på «Gi samtykke». Derfor kan ikke hackere bruke banken som en måte å få tilgang til inntektsopplysninger hos Skatteetaten (bortsatt fra om de som søker om lån i den spesifikke banken, naturligvis).

Bruk av samtykke på den måten det gjøres i SBL innebærer en form for teknisk sikkerhet jeg mistenker at mange ikke er klar over, eller undervurderer effekten av. Det kan isåfall forklares med at vi har hatt samtykkebasert deling lenger enn vi har hatt gode, digitale løsninger for å håndtere samtykke.

Deling av informasjon basert på samtykke er mye eldre enn SBL. Men i mange tilfeller har samtykke blitt gitt til den aktøren som ønsker å motta opplysninger, i form av et kryss på et papir. Da må etaten som skal avgi opplysningene stole på aktøren som påstår å ha innhentet samtykke. I de fleste tilfeller er det for arbeidskrevende å gjøre en kontroll på om den som ga samtykke faktisk gjorde det, om det ble gjort frivillig og om vedkommende forstod hva det ble samtykket til.

Slik samtykkebasert deling tidligere ble løst, er det uklart hvilke mekanismer som sikret at opplysningene bare ble utlevert dersom den det gjelder ga sitt samtykke. Ofte var sikkerheten basert på tillit mellom virksomhetene som utveksler data, og ikke en teknologisk løsning for å hindre urettmessig deling av data.

Digitale samtykkeløsninger derimot, åpner for at *aktøren som skal avgi opplysninger*, selv har kontrollen på dialogen med innbyggeren som skal gi sitt samtykke. Det betyr at de selv bestemmer hvordan brukeren identifiserer og autentiserer seg[19], og hvilken informasjon brukeren får om konsekvensene av samtykket – hvilke opplysninger som utleveres, og til hvem.[20]

Hva betyr bruken av samtykke i SBL for risikoen for opplysninger på avveie? Ettersom banken kun får tilgang til inntektsopplysninger fra Skatteetaten fra de som faktisk samtykker til utlevering i forbindelse med lånesøknaden, så er forholdstallet 1:1 –

19 Dette merker forøvrig brukere av SBL ved at de blir bedt om å logge seg på på nytt når de skal gi samtykke. De har allerede logget seg på nettbanken, men Skatteetaten krever innlogging via ID-porten.

20 Det kan argumenteres for at bruk av samtykke gir bedre oppfyllelse av informasjonsplikten om behandling av opplysninger enn ved deling basert på lovhjemmel. Men slik jeg ser det så gjør samtykke det enklere å gjøre det riktig, siden det uansett er dialog med den som opplysningene gjelder, men det er fortsatt *mulig* å gi god informasjon også ved lovhjemmelbasert deling (selv om det ikke er så vanlig).

banken får bare tilgang til opplysninger om personer som søker om lån.

Det betyr at risikoen for opplysninger på avveie ikke øker, eller øker minimalt, når det legges til rette for samtykkebasert deling. En av angrepsflatene er autentiseringsmekanismen (ID-porten eller en av eID-ene som kan brukes der). Men dersom noen lykkes i å få uautorisert tilgang gjennom påloggingsløsningen, vil de oppnå direkte tilgang til brukerens opplysninger gjennom innsynsløsninger, for eksempel tjenesten «Mine inntekter og arbeidsforhold» hos Skatteetaten. Ved forsøk på slik hacking/misbruk, blir tjenestene som benytter samtykkebasert deling bare en omvei for å nå målet om tilgang til opplysninger. Risikoen som følge av at opplysninger er tilgjengelige på nettet gjennom innsynsløsninger, beskyttet av ID-porten, er vi med andre ord allerede utsatt for. Samtykkebasert deling av de samme opplysningene, som i SBL, fører dermed ikke til økt risiko for opplysninger på avveie.

Da SBL ble lansert, var det med et lite utvalg pilotetater. Siden den gang har mange flere banker fått tilgang til samtykkeløsningen og tilbyr samme type lånetjenester. Som redegjort for ovenfor er likevel risikoen for opplysninger på avveie omtrent uendret. Datadeling basert på samtykke øker kontrollen over egne opplysninger fordi det hindrer at egne opplysninger utsettes for økt risiko for å komme på avveie, selv om andre velger å dele data fra samme kilde.[21] For å si det på en annen måte: Mine inntektsopplysninger er ikke tilgjengelig for BN Bank, selv om naboen min søker lån der.

Kan offentlig sektor bruke samtykke til deling av data?

Som jeg har vist over har samtykkebasert deling av data en fordel ved at risikoen for opplysninger på avveie bare øker for de som selv gjør en aktiv handling for å dele dataene sine. Det kan sees på som et steg mot pareto-optimalitet for personvernet: Noen får styrket personvern uten at det svekkes for andre. Dette bør være en relevant grunn til å vurdere deling basert på samtykke fremfor lovhjemmel i flere tilfeller enn idag. Samtykkebasert deling er spesielt fordelaktig hvis det er mange aktører som skal ha tilgang, eller det er relativt få personer det skal deles opplysninger om, sett i forhold til hvor mange personers opplysninger som utsettes for økt risiko.

Men er det *lov* å basere datadeling på samtykke? På den ene siden burde det være nok å vise til at det allerede blir gjort, som nevnt gjennom deling av inntektsopplysninger fra Skatteetaten i SBL. Et annet eksempel er Lånekassen som deler saldo på studielån med bankene. Dermed får de som har studielån oversikt over studielånet sitt hver gang de er i nettbanken, istedenfor å logge inn ens ærend på Lånekassens nettsider. Et tredje eksempel, som betyr mye for de det gjelder, er muligheten for å samtykke til å dele informasjon fra Nav om uførhet med forsikringsselskapene. Det har ført til forenkling og kortere tid til utbetaling for brukere.[22]

Det er usannsynlig at det som mange mener er de mest erfarne etatene i Norge på temaet juss og digitalisering, skulle tilby å dele opplysninger basert på samtykke dersom det var ulovlig. Også i andre land er samtykke sentralt for digitaliseringen. I den forrige digitaliseringsstrategien i Danmark, var et av de prioriterte tiltakene å etablere bedre løsning for samtykke. Under satsingsområdet «Sammenhæng, gennemsigtighed og tillid som grundlag for den offentlige service» finner vi tiltaket «Let og tryg brug af samtykke: Det skal være nemmere at forstå, hvilke data man deler med det ofentlige. [...]»[23] Utvikling av «Digitalt samtykke» er nå et prosjekt i regi av den danske Digitaliseringsstyrelsen.[24]

Grunnen til at det likevel er verdt å stille spørsmålet er at det ofte blir trukket frem at samtykke etter GDPR ikke kan brukes av offentlige etater, på grunn av skjevt styrkeforhold.

At den oppfattelsen er utbredt, er kanskje heller ikke så rart, siden det står følgende i Datatilsynets veiledning om samtykke:

> *«I vurderingen av om et samtykke er frivillig, må man også se på styrkeforholdet mellom virksomheten og den enkelte. For eksempel vil normalt ikke offentlige myndigheter eller arbeidsgivere kunne bruke samtykke som behandlingsgrunnlag siden den enkelte er i et avhengighetsforhold til virksomheten.»*[25]

Nå vil noen kanskje innvende at styrkeforholdet bare blir et problem når det er snakk om å bruke samtykke til å dele data med en annen *offentlig* virksomhet. I Digital Agenda (2016) var budskapet at hjemmel er en forutsetning for gjenbruk av data i offentlig sektor, og at samtykke er lite egnet.[26] Men hvem som

21 Selv om jeg er positiv til SBL, mener jeg likevel det er endringer som kan gjøres for å styrke personvernet, f. eks. for å gjøre det enda tydeligere hvilke opplysninger som deles («Show, don't tell»).

22 Se: *https://dokumentasjon.dsop.no/dsop_su_om.html*

23 Digitalisering der løfter samfundet. Den fællesoffentlige digitaliseringsstrategi 2022-2025 (Regeringen, KL, Danske Regioner, juni 2022). Se: *https://digst.dk/media/oyddkfru/digst_fods_webtilgaengelig.pdf*

24 Se: *https://digst.dk/it-loesninger/digitalt-samtykke/*

25 Se: *https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/om-behandlingsgrunnlag/samtykke/*

26 Digital Agenda for Norge (2016, kapittel 7.3: «Hjemmel som forutsetning for gjenbruk». Se: *https://www.regjeringen.no/no/dokumenter/meld.-st.-27-20152016/id2483795/?ch=2#kap7-3* Hvorvidt dette var ment å utelukke samtykke, måtte statsråd Jan Tore Sanner svare for i skriftlig spørsmål stilt av stortingsrepresentant Torstein Tvedt Solberg, se: *https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qnid=44614*

mottar opplysningene kan etter min mening ikke ha noe å si for hvordan den siterte setningen fra Datatilsynets veiledning skal forstås. Ved deling av inntektsopplysninger fra Skatteetaten, lånesaldo fra Lånekassen og uførestatus fra Nav, er det i alle tre tilfellene *offentlige myndigheter* brukeren samtykker overfor. Samtykket gis til den som avgir opplysningene, ikke til den som mottar dem.

Jeg mener det er to måter å begrunne lovligheten på.[27] Det ene argumentet er basert på at *behandlingsgrunnlaget* ikke er samtykke. Behandlingsgrunnlaget er derimot hjemmel i lov. Forvaltningsloven og en rekke særlover har egne regler om at taushetsplikten ikke er til hinder for å dele opplysninger dersom den det gjelder samtykker, se for eksempel fvl. § 13a nr. 1 og skatteforvaltningslovens § 3-7 bokstav a. Siden disse reglene om samtykke og taushetsplikt står i nasjonal lov, er ikke det rettslige behandlingsgrunnlaget etter GDPR samtykke (artikkel 6 nr. 1 bokstav a), men enten rettslig plikt eller offentlig myndighet (artikkel 6 nr. 1 bokstav c eller e).

Det andre argumentet legger vekt på at veiledningen fra Datatilsynet formodentlig dreier seg om situasjoner der offentlige virksomheter «utøver offentlig myndighet i forbindelse med den konkrete behandlingssituasjonen», og å dele data basert på samtykke er ikke å anse som myndighetsutøvelse.[28]

Samtykkebasert deling kan være lovlig, men det betyr selvsagt ikke at det *alltid* er lovlig. Jeg mener at en riktig beskrivelse av dette poenget er det som står i Justis- beredskapsdepartementets veileder «Taushetsplikt, opplysningsrett og opplysningsplikt i forvaltningen – en veileder», i kapitlet som omtaler samtykke fra den som har krav på taushet, er en riktig beskrivelse:

> *«I noen tilfeller vil forvaltningen ha en maktposisjon overfor borgeren. Det er viktig at forvaltningen forvisser seg om at borgeren forstår at han eller hun har rett til å nekte å samtykke, og hvilke konsekvenser samtykket har.»*[29]
> *(min understreking)*

Et eksempel på en slik situasjon kan være dersom samtykke til å dele data blir en *forutsetning for* å oppnå en tjeneste eller ytelse fra offentlig sektor. Da blir det relevant å stille spørsmål om samtykket er frivillig. Den enkleste måten å sikre frivillighet på er å gi brukeren alternative måter å fremskaffe opplysningene, noe jeg straks skal komme nærmere inn på.

Noen avviser å bruke samtykke til deling av data med henvisning til at et gyldig samtykke forutsetter muligheten til å trekke det tilbake. Men da tror jeg de blander sammen et samtykke som gjør at mottageren mottar dataene, og et eventuelt samtykke som sikrer mottageren et rettslig grunnlag for å behandle dataene de mottar. I offentlig sektor vil jo det siste normalt være på plass gjennom lov og forskrift som regulerer den aktuelle stønaden, f.eks. bostøtte, reindriftstilskudd eller barnehagebetaling. Også her synes jeg veilederen fra Justis- beredskapsdepartementet rydder opp i misforståelsen på en god måte:

> «Et samtykke kan trekkes, men tilbaketrekkingen virker bare fremover. Hvis forvaltningen allerede har gitt opplysninger videre på grunnlag av samtykke, må det mottakende organet fortsatt kunne bruke de opplysningene det har fått. Tilbaketrekkingen av samtykket hindrer derimot at personer med taushetsplikt fortsetter å gi opplysninger på grunnlag av samtykket.»[30]

Spesielt om frivillighet - erfaring fra Husbanken

Jeg har valgt bostøtte fra Husbanken som eksempel på digital deling av inntektsopplysninger, fordi de tidligere hadde et krav til samtykke fra søkeren for å kunne hente opplysningene fra Skatteetaten.[31] Hus-

27 De tre eksemplene på samtykkebaserte tjenester er alle del av DSOP-samarbeidet, og det ligger mye god dokumentasjon på DSOPs nettsider, se: *https://dokumentasjon.dsop.no/* . Men dokumentasjonen går ikke inn på detaljene for jussen rundt samtykke. Gjennom uformell dialog med personer involvert i de ulike prosjektene, har jeg fått litt mer detaljer, men jeg synes ikke det er riktig å gjengi det her, siden det ikke er offisielle svar fra etatene. Det viktigste for meg er uansett å få frem at det ikke bør være noe tvil om lovligheten.

28 Formuleringen er hentet masteroppgaven ved det juridiske fakultet fra 2022, «Offentlige myndigheters bruk av samtykke som rettslig grunnlag for behandling av personopplysninger», side 35. I oppgaven sammenlignes også veiledningen fra det norske og det danske datatilsynet. Sistnevnte har en mye mer nyansert beskrivelse av offentlig sektors adgang til å bruke samtykke. Oppgaven er tilgjengelig her: *https://www.duo.uio.no/bitstream/handle/10852/96386/Masteroppgave_Offentlige-myndigheters-bruk-av-samtykke.pdf?sequence=1*

29 Justis- og beredskapsdepartementet 2023: «Taushetsplikt, opplysningsrett og opplysningsplikt i forvaltningen – en veileder», se *https://www.regjeringen.no/no/dokumenter/taushetsplikt-opplysningsrett-og-opplysningsplikt-i-forvaltningen-en-veileder/id2963083/?ch=5#id0086*

30 Se forrige fotnote

31 Det var altså ikke Skatteetaten som ba søkeren om å samtykke til å utlevere opplysningene, men Husbanken som ba brukeren om samtykke til å hente opplysninger fra Skatteetaten. Siden Skatteetaten dermed ikke forholdt seg direkte til brukeren, så måtte Husbanken uansett ha tilgang til å hente data fra Skattetatens API, uten brukerens involvering, med den samme risikoen som ved lovhjemmelbasert deling.

banken er avhengige av oppdaterte opplysninger for å fatte vedtak.

Problemet var at dersom søkeren ikke samtykket, ble ikke søknaden om bostøtte behandlet. En slik kobling mellom samtykke og ytelse skaper tvil om samtykket er frivillig. Personvernnemnda behandlet dette i 2015 (sak 2014-03), og flertallet kom til at det ikke kunne være en forutsetning å samtykke til innhenting av data for å få behandlet søknaden.

Personvernnemndas flertall gir eksempler på legitime grunner til at søkeren ikke ønsker å samtykke til at Husbanken henter opplysninger direkte fra kildene, og de beskriver samtidig en alternativ løsning på problemstillingen: «*For å avhjelpe en slik uheldig situasjon [at Husbanken ikke kan hente opplysninger], kan søker velge, i henhold til vanlige saksbehandlingsprinsipper, selv å fremlegge den informasjon som saksforberedende instans anser påkrevd.*»[32] (min understreking) På den måten blir ikke samtykke et krav for å få en ytelse, men et frivillig alternativ.[33]

Bostøtteloven ble etterhvert endret slik at samtykkekravet ble fjernet. Høringen av lovendringen ble gjennomført før personvernnemndas avgjørelse kom. Det kan forklare at den alternative løsningen som Personvernnemnda beskrev, ikke ble drøftet i høringsnotatet. Departementet skrev følgende om bakgrunnen for lovforslaget:

> *«Det er ikke tilfredsstillende at innhenting og bruk av opplysninger er avhengig av at søkeren samtykker. Reelt sett har ikke søkeren noe annet alternativ enn å samtykke hvis vedkommende skal få sin søknad behandlet. Et slikt samtykke oppfyller derfor neppe kravet til informert og frivillig samtykke etter personopplysningsloven § 2 nr. 7.» Departementet foreslår derfor å fjerne samtykkekravet.»*[34] *(min understreking)*

Det er riktig at de som søkte bostøtte reelt sett ikke hadde ~~noe~~ annet valg enn å samtykke. Men de *kunne hatt et valg*, dersom det ble lagt til rette for det. Alternativet ville vært det som dengang var, og fortsatt antageligvis er, det mest vanlige i slike søknadsprosesser, å få opplysningene fra søkeren selv. Eller for å bruke formuleringen fra Personvernnemnda: «*kan søker velge [...] selv å fremlegge den informasjon som saksforberedende instans anser påkrevd*.»

Jeg mistenker at historien om bostøtteloven som ble endret for å fjerne krav til samtykke, har bidratt til at mange jurister sitter med det feilaktige inntrykket av at samtykkebasert deling av data mellom offentlige virksomheter ikke er tillatt. Det er lett å få bekreftet en slik feiloppfatning ved å lese Datatilsynets veiledning om rettslig grunnlag.[35]

Ikke-deling av inntektsopplysninger

Jeg startet artikkelen med å se på fordeler for personvernet ved digital deling. Dersom opplysninger *ikke* deles, men må oppgis og dokumenteres av innbyggeren selv, så går innbyggeren med andre ord glipp av noe som kan styrke deres personvern. Det er derfor ikke alltid sånn at man kan ivareta personvernet best mulig ved å la være å dele.

For å illustrere dette kan vi se for oss en situasjon der en innbygger er i konflikt med en offentlig myndighet. I den sammenhengen er styrkeforholdet skjevt, og innbyggeren føler seg liten og rådvill. I en sånn situasjon vil det være verdifullt å søke hjelp hos en advokat.

Utfordringen er at det er kostbart med advokat. Vedkommende er ikke klar over at det finnes en ordning med økonomisk støtte til rettshjelp, som forvaltes av Statsforvalteren. Men hen har flaks, og får et treff ved et søk på nettet etter juridisk bistand: Et advokatfirma tilbyr gratistjenesten «Kan du få fri rettshjelp?»[36] Brukere av tjenesten kan registrere inntektsopplysninger, før de deretter får svar om de har rett til fri rettshjelp. Bakgrunnen for konflikten er at en etat har krevd tilbakebetaling etter å ha gitt støtte, fordi innbyggeren ikke klarte å levere korrekt dokumentasjon. Det å finne frem til relevante opplysninger, og å sende inn riktig dokumentasjon, er en vanskelig oppgave for en som ikke har oversikt og orden.

I en sånn situasjon ville det vært nyttig for innbyggeren å kunne samtykke til at Skatteetaten delte relevante inntektsopplysninger med tjenesten. Det ville gjøre prosessen

32 Se: *https://personvernnemnda.no/2014/08/20/pvn-2014-03-husbanken/*

33 Jeg er klar over at et viktig poeng for Husbanken var å få oppdaterte opplysninger om inntekt gjennom året, som en kontroll av at det ikke skjedde større endringer i inntekten. Etter min mening er det ikke noen prinsipiell forskjell i å samtykke til innhenting eller levere opplysninger selv i forbindelse med søknaden, og til slik jevnlig oppdatering av opplysninger. Kan hende ville ikke Husbanken hatt kapasitet til å håndtere søkernes opplysninger på den måten, men såvidt jeg vet er det ingen som vet sikkert hvor stor andel av søkerne som ville velge å samtykke slik at Husbanken fikk opplysningene direkte fra Skatteetaten. Det er jo god grunn til å tro at mange ville foretrekke det siden det krever mindre manuelt arbeid. Et annet argument mot samtykke kan være hensynet til de svakeste; at alt som øker kompleksiteten i *prosessen for å få bostøtte, først og fremst rammer de som trenger bostøtte aller mest.*

34 Se: *https://www.regjeringen.no/globalassets/upload/kmd/boby/bostotteloven_horingsnotat.pdf*

35 Se tidligere omtale av Datatilsynets veileder. Datatilsynets høringssvar til endringen i bostøtteloven tok forøvrig heller ikke opp at den problematiske koblingen mellom samtykke og behandling av søknaden kunne blitt løst ved å gi brukeren et alternativ. Se: *https://www.regjeringen.no/no/dokumenter/Horing--endringer-i-bostotteloven/id2005783/?showSvar=true&consterm=&page=1&isFilterOpen=true*

36 Tjenesten er fiktiv, men det finnes nettsider som informerer om muligheten, og forklarer hva vilkårene er. Det er ganske mye informasjon å lese og forstå. Dette *er for øvrig også en tjeneste som jeg ser for meg at vil kunne tilbys av organisasjoner som f.eks. Skattebetalerforeningen, Løvemammaene eller Stiftelsen Rettferd.*

enklere, raskere og resultatet sannsynligvis riktigere. I neste omgang kunne den samme samtykketjenesten blitt brukt til å søke om fri rettshjelp hos Statsforvalteren. Den digitale søknaden som finnes for dette idag, krever at brukeren manuelt fyller ut inntektsopplysninger og deretter laster opp dokumentasjon.

Idag er det ikke mulig å samtykke til deling av inntektsopplysninger hverken med advokattjenesten eller Statsforvalteren – altså hverken med en privat aktør eller en offentlig virksomhet. Manglende mulighet til å dele egne opplysninger, er etter min mening også et eksempel på *begrensninger i kontroll over egne opplysninger*, som dermed fører til et svakere personvern.[37] Det er fristende å bruke sammenligningen med bankkontoen igjen, men forhåpentligvis er poenget tydelig nok.

Eksempelet kan forhåpentligvis bidra til å illustrere poenget i den tidligere nevnte veilederen fra Justis- og beredskapsdepartementet, der det står at «I noen tilfeller vil forvaltningen ha en maktposisjon overfor borgeren.» At det i *noen* tilfeller kan være problematisk, betyr at det i *andre* tilfeller er helt uproblematisk. I eksempelet jeg nettopp ga, kan man til og med si at reglene som gir innbyggerne rett til å dele data kan bidra til at de får *styrket sin egen maktposisjon* vis-à-vis myndighetene.

Spesielt om kommunenes drastisk økte tilgang til inntektsopplysninger

Jeg håper jeg har fått tydelig frem at deling basert på samtykke kan gi noen fordeler for personvernet, og at det er lov å basere deling fra og mellom myndigheter på samtykke. Derfor bør det etter min mening gjøres en vurdering av om samtykke eller lovhjemmel er den beste løsningen når opplysninger skal deles.

En slik vurdering blir dessverre ofte ikke gjort. En god illustrasjon er samarbeidet mellom KS og Skatteetaten, som har pågått i ca. ti år, om deling av inntektsopplysninger med kommunene.[38] De siste årene har dette samarbeidet resultert i store endringer. Alle landets 357 kommuner er i ferd med å få tilgang til inntektsopplysninger på et økende antall tjenesteområder, bl.a. oppholdsbetaling for barnehage og SFO.

Hvor mye øker risikoen for at inntektsopplysninger kommer på avveie når kommunene får tilgang til opplysningene? Selv om antall kommuner er relativt konstant, øker antallet ansatte og systemleverandører for hver ny kommunal tjeneste som får en slik tilgang. Det er identifisert ca. tredve lovpålagte kommunale tjenester der inntektsopplysninger fra Skatteetaten benyttes i saksbehandlingen. Ettersom det ikke finnes noen måte å reservere seg på, mener jeg det utgjør et stort inngrep i kontroll over egne opplysninger, fordi det er en voldsom økning i antall virksomheter og ansatte som har direkte tilgang til inntektsopplysninger fra Skatteetaten.

Samarbeidet mellom KS og Skatteetaten om tilgang til inntektsopplysninger har pågått som en serie prosjekter siden 2015, og det er åpenbart at arbeidet har bidratt til verdifull innsikt om bl.a. utfordringene knyttet til uklarheter i begrepsbruk i lover og forskrifter, ulikheter i forståelsen av reglene på tvers av kommuner, usikkerhet om kommunenes adgang til å gi egne regler osv. Men på et viktig område mener jeg arbeidet lider av en stor svakhet: Samarbeidet har for tidlig og på feil grunnlag, låst seg til at delingen skal skje med lovhjemmel.

Den første delen av arbeidet var en konseptutredning som munnet ut i en kombinert rapport og veileder i 2017 for hvordan det skulle jobbes videre med kommunenes tilgang til inntektsopplysninger.[39] I rapporten fremgår det at samtykke ble vurdert som et *juridisk hinder* for deling av data.[40] Videre understrekes det at de identifiserte hindrene er generelle, på tvers av ulike kommunale tjenester.[41] Dessuten viser rapporten at Skatteetaten hadde identifisert hvilken hjemmel i eget regelverk de ønsket å benytte som grunnlag for å avgi opplysninger: «Skatteforvaltningsloven § 3-3 bokstav h er hjemmelen [Skatteetaten] ønsker at kommunene forholder seg til og som krever en hjemmel i den aktuelle innbyggertjenesten sin lovbestemmelse.» (s. 24). § 3-3 handler om at taushetsplikten ikke er til hinder for å gi ut opplysninger til andre offentlige myndigheter som trenger dem til sine lovpålagte oppgaver. Dette ønsket fra Skatteetaten i sin tid, er naturlig å tolke som at regelen i skatteforvaltningslovens § 3-7 bokstav a, «opplysninger gjøres kjent i den utstrekning de som har krav på taushet samtykker», *ikke* var ønsket.

37 Jeg mener ikke at dette er en svekkelse av personvernet i forhold til nåsituasjonen. Det er en svekkelse i forhold til hva som både teknologisk og rettslig bør være relativt enkelt å realisere, siden vi allerede har SBL og dermed de nødvendige byggeklossene.

38 I 2017 ga jeg innspill til noen av deltagerne i dette samarbeidet, men uten at jeg fikk gjennomslag for mine synspunkter. Jeg har vært i tvil om jeg burde nevne dette i artikkelen, og konkludert med at det er ryddig å være åpen om det. Forhåpentligvis bidrar det til ekstra kritisk lesing.

39 Veileder - Konseptutredning for bruk av inntektsopplysninger fra a-ordningen, se: *https://www.ks.no/globalassets/fagomrader/digitalisering/veileder-nak-2017.pdf*

40 Dette fremgår av en figur i kapittel 6.2.2 i rapporten. Dette er til tross for at rapporten etter min mening har en god beskrivelse av det juridiske rundt samtykkebasert deling i kapittel 6.2.3.1.4, bl.a. med henvisning til forvaltningslovens § 13a nr 1.

41 Slik jeg tolker rapportens beskrivelse av organisering av arbeidet og deltagere i møter der hindrene ble identifisert, var det primært jurister og saksbehandlere med erfaring fra tjenesteområdet økonomisk sosialhjelp som deltok, og ikke for eksempel it-arkitekter med kunnskap om digitale samtykkeløsninger.

At det ikke synes å ha blitt foretatt noen reell vurdering av samtykke som alternativ til lovhjemmel for noen av tjenesteområdene siden 2017, viser seg også i rapportene fra prosjektene de siste årene. Det er laget rapporter for de enkelte tjenesteområdene og en sluttrapport.[42] I sluttrapporten er ikke samtykke nevnt en eneste gang, mens det i f. eks. i rapporten «Rettslig grunnlag for utlevering av inntekts- og skatteopplysninger til bruk ved vedtak om tildeling av kommunale bostøtteordninger» kun er nevnt argumenter *mot* samtykke, eksempelvis at det er komplisert å håndtere samtykke i IT-systemer.[43]

Et tilleggspoeng ved samarbeidet om kommunenes tilgang til inntektsopplysninger er at KS og Skatteetaten mener tilgangen ofte kan etableres med utgangspunkt i eksisterende lovgivning. Det eksisterende regelverket inneholder etter deres mening tilstrekkelige hjemler for å gi kommune tilgang:

> *«I det juridiske arbeidet har vi prioritert å finne handlingsrommet i eksisterende rettskilder heller enn å endre regelverk. Dette fordi endring av lovverket ofte tar uforholdsmessig lang tid, slik at de gode løsningene ikke kommer på plass selv om alt bortsett fra jusen legger til rette for det.»*[44]

Når skatteforvaltningslovens § 3-3 bokstav h gjør det mulig å hjemle tilgang til opplysninger i eksisterende lovgivning for de kommunale tjenestene, blir det ikke gjennomført noen regelverksendringer med tilhørende høringer. Som tidligere nevnt viser dokumentasjonssidene til Skatteetaten hvilke tjenester som har tilgang til API-er basert på hjemmel eller samtykke. Men det står ikke nærmere angitt *hvilken konkret* lovhjemmel det siktes til som gir mottakeren rett til å hente opplysninger direkte fra Skatteetaten. For kommunale tjenester finnes informasjonen til gjengjeld delvis i sluttrapporten fra samarbeidsprosjektet. Sluttrapporten inneholder en oppsummering av hva som er kommunenes hjemmel på ulike tjenesteområder, og lenker til de konkrete utredningene for hvert område.[45] For enkelte tjenesteområder er det kommentert følgende: *«Lov og forskrift har ikke tilstrekkelig hjemmelsgrunnlag for å hente opplysninger fra Skatteetatens delingstjeneste, her må FoU-prosjektets samlede rettskildegrunnlag brukes i tillegg».*

Samtykke er altså enten ikke nevnt, eller det er negativt omtalt. Men hvordan har KS og Skatteetaten vurdert forholdet mellom de som uansett utsetter seg for økt risiko for opplysninger på avveie ved å søke kommunale tjenester, og resten av befolkningen? Jeg har ikke funnet noe i dokumentene fra samarbeidet mellom KS og Skatteetaten som problematiserer hvordan man kan avgrense hvilke personer hver kommune kan hente opplysninger om. Dersom det er slik at hver kommune kun kan hente opplysninger om personer med folkeregistrert adresse i egen kommune, så har det stor betydning for forholdstallet mellom disse to gruppene. Men det er uklart om dette er praksis, fordi spørsmålet hverken er tatt opp i veilederen fra 2017 eller i noen av de senere rapportene fra samarbeidet som jeg har lest. Videre er det uklart for meg om en kommune må kunne behandle opplysninger om søkere fra andre kommuner. Barnehage er ihvertfall *en* tjeneste som er åpen for søkere fra andre kommuner, for å gjøre det mulig å skaffe barnehageplass før man har flyttet til et nytt hjem.

For å oppsummere, så har samarbeidet mellom KS og Skatteetaten om deling av inntektsopplysninger svært tidlig konkludert med at samtykke er uegnet, for *alle* relevante tjenesteområder. Samtidig har de etablert en arbeidsmetodikk som gjør at det ofte ikke er nødvendig å gjennomføre regelverksendringer. Isteden tolkes nødvendige lovhjemler inn i eksisterende regelverk. Dette fører til at innbyggeren hverken har påvirkningsmulighet gjennom å kunne nekte deling av egne opplysninger, *eller* mulighet til å påvirke gjennom høringer.

Veien videre: Opprydding om samtykke

Når samtykke av ulike årsaker blir definert som uaktuelt, ender vi dessverre med en situasjon der vi diskuterer om det er riktig å dele data, eller ei, og baserer oss på lovhjemmel når vi mener svaret er ja. Det er mange gode grunner til at data bør deles, og det er også sterke politiske føringer om å dele mer, bl.a. målet om «Kun én gang». Dermed blir konklusjonen normalt ja til deling uten at vi gjennomfører den viktige drøftingen av *hvordan* det er riktig å dele i de ulike situasjonene for å oppnå best mulig personvern.

Spørsmålet nå er hvordan vi kan endre situasjonen.

Etter min mening bør det være standard at jeg *har mulighet til å dele* opplysninger om meg selv, med de jeg ønsker å dele med.[46] Istedenfor

42 Sluttrapporten inneholder lenker til de andre rapportene, men ikke alle lenkene fungerer. Sluttrapporten er tilgjengelig her: *https://www.ks.no/contentassets/9259453972fd48f9b20a97ffda9f038f/Sluttrapport-fra-prosjekt-Kommunesektorens-behov-for-digital-tilgang-til-nodvendige-opplysninger-fra-Skatteetaten.pdf*

43 Se side 14 i rapporten, som for øvrig ser ut til å være et juridisk arbeid, uten deltagere med spesialisering innen IT: https://ksdigital.no/wp-content/uploads/2024/09/Rettslig-grunnlag-for-deling-pa-det-boligsosiale-omradet.pdf

44 Notat om samarbeidet mellom KS og Skatteetaten til SKATEs fagdag i 2022, se: https://www.digdir.no/media/2883/download

45 Se sluttrapportens kapittel 6.3.

46 Dette er slik jeg oppfatter det også det som er målet med Dataforvaltningsforordningen, som var på høring i høst, nemlig at offentlig sektor skal legge til rette for å dele beskyttede data, f.eks. med samtykke fra den det gjelder.

at det utelukkende settes søkelys på faren for at innbyggerne lar seg lure til å dele data med noen som misbruker opplysningene, bør vi også legge vekt på tre andre forhold: For det første vil denne muligheten for deling i mange tilfeller brukes til å dele opplysninger med andre offentlige etater, og dermed bidra til målet om «Kun én gang». For det andre er det den offentlige etaten som er avgiver av opplysningene og dermed har dialogen med brukeren som skal samtykke. Det kan for eksempel fremgå tydelig i dialogen at avgiveren ikke tar ansvar for sikkerheten og personvernet hos mottakeren. Og for det tredje bør vi huske at slik deling kan hjelpe innbyggerne med å navigere i sine rettigheter og plikter, på en måte offentlig sektor selv dels ikke prøver, og dels aldri vil kunne klare, på grunn av begrensede muligheter til å ta ansvar for *rådgiving*. Å legge til rette for deling kan med andre ord gi innbyggerne mulighet til å la seg hjelpe av teknologi for å styrke sin maktposisjon overfor myndighetene.

For å få til endringer tror jeg det er nødvendig at relevante myndigheter klargjør både hva som er lovlig og hva som er ønskelig. Et åpenbart første steg er å følge opp Personvernkommisjonens forslag fra 2022:

> *«Personvernkommisjonen anbefaler at regjeringen utreder om en samtykkebasert gjennomføring av «kun-en-gang'-prinsippet vil kunne avhjelpe noen av personvernulempene som oppstår ved deling av personopplysningen mellom offentlige etater.»*[47]

Det er vel og merke viktig at utredningen ikke kun ser på deling mellom offentlige etater, men også hvordan det henger sammen med deling med private aktører.

Men i parallell bør ideelt sett relevante, eksisterende dokumenter oppdateres før en større utredning er gjennomført. Datatilsynet bør starte med å oppdatere sin veileder om rettslig grunnlag, f.eks. ved å se på hvordan deres danske søsterorganisasjon nyanserer informasjonen om samtykke. Videre bør det tas inn en setning i Digitaliseringsrundskrivet om at det ved deling av data skal gjøres en vurdering mellom samtykke og lovhjemmel.[48] Digitaliseringsdirektoratet bør også endre teksten i sin veileder om digitaliseringsvennlig regelverk, der de oppfordrer til å lage hjemler for deling, som det er vanskelig å tolke på annen måte enn at deling *ikke* skal baseres på samtykke.[49] Digitaliseringsdirektoratet har dessuten en artikkel på sine nettsider som diskuterer samtykke, og anerkjenner at det er mye usikkerhet og uklarhet ved bruk av samtykke. Artikkelen har mange gode poeng, men jeg mistenker at den havner i skyggen av veilederen om digitaliseringsvennlig regelverk og Datatilsynets veiledning.[50]

Datatilsynets veileder om DPIA bør oppdateres for å tydeliggjøre at ved deling av data må man skille mellom to grupper: Den gruppen som uansett vil få opplysninger utsatt for risiko, og de som blir omfattet av økt risiko, dersom det blir etablert deling basert på lovhjemmel. Uten å se på konsekvensene for disse gruppene opp mot hverandre, er det vanskelig foreta en helhetlig vurdering. Med deling basert på samtykke kan personvernet til én gruppe forbedres, uten at det svekker personvernet til andre. Med hjemmel aksepterer man en økt risiko for en gruppe for å få økt personvern for en annen gruppe.

> Med deling basert på samtykke kan personvernet til én gruppe forbedres, uten at det svekker personvernet til andre.

Fra detaljerte opplysninger til vilkårsprøving

I diskusjoner om dette temaet tidligere, har jeg hatt problemer med å få frem at jeg ikke er *imot* deling basert på lovhjemmel. Jeg har vært opptatt av å få frem fordelene med samtykke fordi jeg mener disse to alternativene må vurderes opp mot hverandre i hvert enkelt tilfelle. Derfor vil jeg til slutt også si noe om potensialet for å forbedre personvernet når deling skjer basert på lovhjemmel.

En fordel med deling basert på lovhjemmel, som jeg tror kan utnyttes mye bedre enn idag, er muligheten for radikal dataminimering ved å flytte logikken som skal utføres på opplysningene fra mottakeren av dataene og inn i API-et hos avgiveren av dataene. For å illustrere det med inntektsopplysninger: Siden deling med lovhjemmel tilsier at mottakeren har hjemmel for saksbehandlingen, betyr det at vi i en del tilfeller kan vite detaljert hvordan inntektsopplysningene brukes for å teste om vilkår er oppfylt. Isåfall er det mulig å flytte denne vilkårsprøvingen til API-et hos Skatteetaten.

Som vi så i forbindelse med deling av inntektsopplysninger med kommunene, så gjøres det en nøye gjennomgang av regelverkene for de ulike kommunale tjenestene, for å identifisere hvilke opplysninger kommunene har hjemmel til å få fra Skatteetaten. Istedenfor å stoppe

47 Se: *https://www.regjeringen.no/no/dokumenter/nou-2022-11/id2928543/?ch=5#kap6-5*

48 Se: *https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id3025117/*

49 «Lag hjemler som gjør det mulig å dele nødvendige data med virksomheter dere trenger å samarbeide med i og utenfor egen sektor.». Se: *https://www.digdir.no/datadeling/generelle-anbefalinger-lage-digitaliseringsvennlig-regelverk/2868#3_del_data_nr_dere_kan_skjerm_nr_dere_m*

50 Se: *https://www.digdir.no/sammenhengende-tjenester/bruk-av-samtykke-i-offentlig-sektor/3707*

Illustrasjon: Colourbox.com

der, kunne de også forsøkt å identifisere nøyaktig hvordan opplysningene brukes som del av vilkårsprøvingen i reglene. Istedenfor en API-forespørsel etter en rettighetspakke som gir et sett med detaljerte inntektsopplysninger, kunne forespørselen istedenfor vært et uttrykk som returnerer ja eller nei, dersom for eksempel summen av elementene x, y, z minus summen av elementene æ, ø, å er lavere enn en grenseverdi. Sikkerhetsmekanismer i API-et kunne sjekke at de ulike mottakerne kun sendte spørringer i tråd med deres rettslige behov.[51] Dersom deling basert på lovhjemmel ble løst på denne måten blir det mye mindre økning i risikoen for opplysninger på avveie, både for den gruppen som ufrivillig får økt risikoen for opplysninger på avveie, men *også* for de som uansett kommer til å dele data med mottakeren.[52]

Antagelig ville denne typen deling også fungere som en pådriver for automatiseringsvennlig regelverk hos de som ønsker å motta inntektsopplysninger, siden det bør være lavere terskel for å ha hjemmel til å hente et ja-nei-svar fra Skatteetaten, enn et sett av detaljerte inntektsopplysninger. Kanskje vil det også gjøre mottakerne mindre attraktive som mål for hackere og utro tjenere, ettersom de ikke lenger er en del av angrepsflaten for å få uautorisert tilgang til detaljerte opplysninger fra Skatteetaten. Uansett er det grunn til å anta at utgifter til informasjonssikkerhet og personvern til en viss grad øker når mengden detaljerte opplysninger en virksomhet har tilgang til øker, så om ikke annet er det et potensiale for å redusere kostnader ved en slik tilnærming.[53]

Steinar Skagemo er forvaltningsinformatiker og jobber i Brønnøysundregistrene. Han har tidligere jobbet i Difi og Oslo kommune. Artikkelen er skrevet av forfatter på eget initiativ.

Jeg, og ikke minst leseren, skylder en stor takk til medredaktør Trine Shil Kristiansen, som har påpekt en rekke uklarheter og foreslått forbedringer til teksten.

51 En litt lignende løsning er Microdata.no, som leveres av SSB og SIKT. Her kan det foretas analytiske spørringer på detaljerte data hos SSB, slik at kun resultatene av spørringene deles med brukeren. Se: *https://www.microdata.no/*

52 Det kan godt tenkes at det vil være mulig å bruke samme tilnærming for beregningsregler, og ikke bare vilkårsprøving.

53 Det er ingenting i veien for å bruke den samme metoden for å oppnå dataminimering ved samtykkebasert deling heller, selvsagt. I noen tilfeller kan metoden med vilkårsprøving hos den aktøren som har dataene fra før, danne grunnlaget for å identifisere hvem som har rett på en ytelse (såkalt proaktive tjenester), og deretter invitere de det er aktuelt for til å sende søknad og samtykke til deling av detaljerte opplysninger. Det kan balansere et mål om å gjøre det enklere å få tjenestene man har krav på, uten at det blir delt for mange detaljer om hver enkelt innbygger.

Én flue med to smekk? Risikoen for dobbeltforfølgelse ved delt tilsynsmyndighet for sporing på nett

Av Ole-Martin Moe og Hanne Pernille Gulbrandsen

Ny ekomlov og regulering av cookies

Cookies (informasjonskapsler) og annen sporingsteknologi er på alles tunger. Dette gjelder særlig fordi Norge ved nyttår fikk en ny lov om elektronisk kommunikasjon (ekomloven) der det nå er bestemt at det kreves et samtykke i tråd med personvernforordningen (GDPR) for at man lovlig skal kunne plassere cookies og annen sporingsteknologi i dine og mine digitale enheter.

Sporing gjennom cookies, browser fingerprinting, piksler og lignende sporingsteknologi spiller en sentral rolle i den digitale økonomien. Felles for denne typen teknologi er at den enkelt forklart gjør virksomheter i stand til å se hvordan du bruker tjenestene deres på nett, for eksempel hva du klikker på, hvor lenge du leser et bestemt innhold og hvilken side du var inne på før du gikk inn på denne virksomhetens nettsider. Alt avhengig av hvordan virksomheten har satt opp sporingen.

Slik sporingsteknologi brukes til å få nettsteders kjernetjenester til å fungere. Dette kan for eksempel være i en nettbutikk der cookies brukes til å huske hva du har puttet i handlekurven mens du ser på andre varer. Sporingsteknologi brukes ofte også til å analysere brukeratferd, tilpasse innhold og målrette markedsføring på nett. Selv om slike verktøy bidrar til å skape en mer tilpasset digital hverdag, innebærer de også ofte en omfattende behandling av personopplysninger.

Ole-Martin Moe

Hanne Pernille Gulbrandsen

Den nye ekomloven, som trådte i kraft 1. januar 2025, søker å møte disse utfordringene. Ekomloven § 3-15 stiller krav om at virksomheter som bruker informasjonskapsler eller lignende teknologi, som hovedregel må innhente samtykke fra brukerne. Frem til nå har det vært stor usikkerhet knyttet til hva som utgjør et gyldig samtykke for denne typen sporingsteknologi. Dette fordi Norge, sammenlignet med EU, har hatt en særegen regel i den nå opphevede ekomloven § 2-7b om at samtykke kunne bli gitt gjennom forhåndsinnstillinger i nettleseren.[1]

I den nye ekomloven er det, i samsvar med EU-domstolens forståelse av kommunikasjonsverndirektivet[2], presisert at virksomheter må ha et samtykke fra brukeren som oppfyller kravene til et gyldig samtykke etter personvernforordningen, se ekomloven § 3-15. Datatilsynet og Nasjonal kommunikasjonsmyndighet (NKOM) har fått delt tilsynsmyndighet for denne bestemmelsen. § 3-15 inneholder også et unntak fra kravet om samtykke ved bruk av informasjonskapsler

> Frem til nå har det vært stor usikkerhet knyttet til hva som utgjør et gyldig samtykke for denne typen sporingsteknologi

1 *https://www.datatilsynet.no/contentassets/211ea735e77246158ea3d14ae5aea26e/felles-horingssvar-fra-forbrukertilsynet-og-datatilsynet---forslag-til-ny-ekomlov.pdf* (sist besøkt 03.02.25).

2 EU-domstolen presiserte allerede i 2019 i sak C-673/17 (Planet49) at kravet til samtykke etter Europaparlaments- og råds direktiv (EU) 2018/1972 av 11. desember 2018 om fastsettelse av et europeisk regelverk for elektronisk kommunikasjon artikkel 5.3 skulle forstås på samme måte som etter personvernforordningen.

mv. som er «strengt nødvendig» for å levere en informasjonssamfunnstjeneste etter den aktuelle sluttbrukerens eller brukerens uttrykkelige forespørsel. Cookies og sporing som rammes av dette unntaket behandles ikke nærmere i denne artikkelen.

Ansvarsfordelingen mellom Datatilsynet og Nasjonal kommunikasjonsmyndighet (NKOM) skal sikre at både personvernmessige og tekniske aspekter ved informasjonskapsler håndteres. Likevel skaper denne delte tilsynsrollen nye utfordringer og særlig knyttet til faren for dobbeltforfølgelse. Hva skjer når begge organene behandler samme sak fra ulike perspektiver, men ender opp med overlappende sanksjoner? Hvordan sikrer vi at prinsippet om *ne bis in idem*, fastsatt i Den europeiske menneskerettighetskonvensjonen (EMK), respekteres?

I denne artikkelen ser vi nærmere på faren for dobbeltforfølgelse ved håndhevingen av ekomloven § 3-15 i kontekst av tilsyn med adferdsbasert markedsføring.

Sporing på nett

Informasjonskapsler, er små datafiler som lagres på en brukers enhet når de besøker en nettside. Disse filene brukes til en rekke formål, blant annet for å tilpasse nettsider, lagre brukerpreferanser og spore brukeratferd.

Andre teknologier, som fingerprinting, gjør det mulig å identifisere en brukers enhet ved hjelp av tekniske kjennetegn som nettlesertype, skjermoppløsning og installerte skrifttyper. Fingerprinting gir en unik «signatur» som kan brukes til å spore brukeren, selv uten informasjonskapsler.

Denne typen sporingsteknologi kan gi oss som brukere mange fordeler og en mer tilpasset brukerreise. Samtidig reiser de også spørsmål om personvern og brukerkontroll. Det er her ekomloven § 3-15 og personvernforordningen kommer inn. Regelverkene krever at virksomheter som bruker cookies eller annen sporingsteknologi for å legge til rette for adferdsbasert markedsføring må innhente et aktivt, informert og frivillig samtykke før slike verktøy kan tas i bruk.

For eksempel kan en bruker som besøker en nettbutikk og ser på en bestemt sofa, senere oppleve å få vist annonser for den samme sofaen – eller lignende produkter – på andre nettsteder. Dette skjer fordi cookies registrerer hvilke sider brukeren har besøkt og sender denne informasjonen tilbake til nettbutikken eller til annonseleverandører.

En vanlig måte å dele inn behandlingen av personopplysninger i prosessen med å vise adferdsbasert markedsføring er som følger[3]:

1. **Samtykke fra brukeren**
   Når en bruker besøker et nettsted, blir vedkommende ofte presentert med et samtykkebanner. Dette banneret informerer om bruken av informasjonskapsler og ber om brukerens tillatelse til å plassere cookies for ulike formål, inkludert tilpasset markedsføring. Samtykket må være frivillig, spesifikt, informert og gitt gjennom en aktiv handling, i tråd med personvernforordningen.

2. **Plassering av informasjonskapsler**
   Hvis brukeren gir sitt samtykke, plasseres en informasjonskapsel i brukerens nettleser. Denne kapselen kan enten være plassert av eieren av nettstedet (publisisten) eller av tredjeparter, for eksempel annonseleverandører, som har avtaler med nettstedseieren.

3. **Innsamling av brukerdata på nettstedet**
   Informasjonskapselen begynner å samle inn informasjon om brukerens interaksjoner med nettstedet. Dette kan inkludere:
   - Hvilke sider som besøkes.
   - Hva brukeren klikker på.
   - Hvor lenge brukeren oppholder seg på ulike sider.
   - Produkter som legges i handlekurven eller kjøpes.

4. **Sporing på tvers av nettsteder**
   Enkelte informasjonskapsler, særlig tredjepartscookies, er designet for å spore brukeren på tvers av nettsteder. Dette vil si cookies som er plassert av andre enn eieren av nettstedet, for eksempel et annonseselskap. Dette gjør det mulig å samle inn data om hvilke nettsteder brukeren besøker etter det første nettstedet, og gir et mer helhetlig bilde av brukerens nettaktivitet.

5. **Kategorisering og profilering av brukeren**
   Dataene som samles inn, analyseres og brukes til å kategorisere brukeren i spesifikke grupper basert på interesser, demografi, eller kjøpsadferd. Dette kan inkludere antagelser om alder, kjønn, inntekt eller preferanser. Profileringen gjøres ofte av annonseleverandører eller analysefirmaer.

6. **Bruk av data i adferdsbasert markedsføring**
   Basert på brukerens profil, kan annonsører målrette annonser som vises på ulike nettsteder. For eksempel kan en bruker som har søkt etter løpesko, få vist annonser for slike produkter på andre nettsteder. Informasjonen kan også brukes til å optimalisere annonseplasseringer og budsjetter hos annonsører.

7. **Deling av data mellom aktører**
   Innsamlede data kan deles eller

3 *https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/rettigheter-og-plikter/rapporter/kommersialisering-norsk-endelig.pdf* Noen av cookiesene i denne listen vil kunne anses som strengt nødvendig i en gitt cookies. Det vil ikke omtales i denne sammenheng.

selges til andre aktører i annonseøkosystemet, inkludert datameglere og plattformer for programmatisk annonsering. Dette øker rekkevidden av dataene og gjør det mulig for flere aktører å dra nytte av den samme informasjonen. I dette systemet er det

Hva omfattes av ekomloven § 3-15

Ekomloven § 3-15 fastsetter at «lagring av opplysninger i brukernes kommunikasjonsutstyr» eller «tilgang til slike opplysninger» kun er tillatt dersom brukeren har gitt sitt samtykke. Bestemmelsens virkeområde er altså pkt. 1 og 2 i oversikten over, mens den etterfølgende behandlingen av personopplysninger omfattes av personvernforordningens virkeområde.[4]

Denne bestemmelsen gjelder ikke bare informasjonskapsler, men også annen sporingsteknologi som lokal lagring og piksler.

Kravene til samtykke er de samme som i personvernforordningen: Det skal være frivillig, spesifikt, informert og gitt gjennom en aktiv handling, jf. personvernforordningen artikkel 4 nr. 11 og artikkel 7. Dette innebærer blant annet at standardinnstillinger som aktiverer cookies, uten at brukeren foretar en bevisst handling[5], ikke er tilstrekkelig. Dette er en største endringen fra den nå opphevede ekomloven fra 2003.

Tilsynsansvaret for § 3-15 er delt mellom Datatilsynet og NKOM etter forskrift om delegering av myndighet etter lov om elektronisk kommunikasjon (ekomloven) del I, nummer 12:

Departementets myndighet etter § 3-15 delegeres til Datatilsynet og Nasjonal kommunikasjonsmyndighet på følgende måte:

a. Datatilsynet skal ha ansvar for å vurdere om samtykke i første ledd er i samsvar med personvernforordningen, vurdere om kravene til informasjonen som skal gis er tilstrekkelig og om det er lagt til rette for at samtykke kan trekkes tilbake.
b. Nasjonal kommunikasjonsmyndighet skal ha ansvar for å vurdere om den teknologiske løsningen er omfattet av bestemmelsens første ledd og om vilkårene for teknisk lagring eller adgang til opplysninger etter andre ledd er oppfylt.
c. Datatilsynet skal føre tilsyn etter § 15-1 første ledd med om samtykkekravet i § 3-15 første ledd er oppfylt, innhente opplysninger til dette formålet etter § 15-2 andre ledd og ilegge nødvendige sanksjoner etter § 15-11 første ledd og § 15-12 første ledd bokstav a.

Selv om innsamling av personopplysninger kan deles inn i ulike faser slik vi har beskrevet ovenfor, er disse i praksis ofte overlappende. Det kan være utfordrende fra både et teknisk og juridisk ståsted å isolere de ulike delene av adferdsbasert markedsføring fra hverandre. Selv om ansvarfordelingen i forskriften gir mening i teorien, kan den i praksis føre til overlappende behandlinger og risiko for dobbeltforfølgelse når NKOM og Datatilsynet sammen eller hver for seg skal vurdere om eieren av et nettsted har opptrådt i tråd med loven eller ikke.

Tilsynsmyndighetene jobber ifølge Datatilsynet for tiden med felles veiledning om ekomloven § 3-15. Vår oppfordring er at tilsynsmyndighetene også gjør grundige vurderinger og for eksempel utarbeider felles retningslinjer basert på typetilfeller for hvordan tilsynsmyndigheten skal utøves. Med myndighet til å ilegge gebyrer på opptil 20 millioner euro eller 4 % av global omsetning etter personvernforordningen og inntil 5 % av siste års salgsinntekt etter ekomloven er det avgjørende for tilsynsobjektenes rettssikkerhet at denne delte myndigheten utøves innenfor forvaltningslovens rammer.[6]

Hvorfor oppstår faren for dobbeltforfølgelse?

Faren for dobbeltforfølgelse oppstår fordi Datatilsynet og NKOM har overlappende kompetanseområder under ekomloven § 3-15 og fordi teknologien og behandlingen av personopplysninger som reguleres i bestemmelsen kan gjøre det vanskelig å sette et skarpt skille for hvor Datatilsynets myndighet starter og NKOMs slutter. Mens Datatilsynet vurderer om samtykke oppfyller kravene i personvernforordningen, vurderer NKOM de tekniske sidene ved implementeringen av sporingsteknologi. NKOM har også ansvar for å vurdere hvorvidt en bruk av sporingsteknologi er omfattet av unntakene i ekomloven § 3-15 annet ledd.

§ 3-15 annet ledd lyder slik:

Første ledd gjelder ikke for teknisk lagring av eller adgang til opplysninger

a. utelukkende for det formål å overføre kommunikasjon i et elektronisk kommunikasjonsnett, eller
b. som er strengt nødvendig for å levere en informasjonssamfunnstjeneste etter den aktuelle sluttbrukerens eller brukerens uttrykkelige forespørsel

Av disse to unntakene er det særlig bokstav b som kan gjøre det vanskelig å trekke en grense for hvor NKOMs myndighet slutter og Da-

4 Se Prop. 93 LS (2023–2024) Lov om elektronisk kommunikasjon (ekomloven) og samtykke til godkjenning av EØS-komiteens beslutninger nr. 274/2021, 275/2021, 276/2021 og 277/2021 om innlemmelse i EØS-avtalen av forordningene (EU) 2018/1971, (EU) 2019/2243 og (EU) 2020/1070 og direktiv (EU) 2018/1972, s. 290.

5 Det avgrenses her mot omtale av unntakene i ekomloven § 3-15 andre ledd.

6 Se personvernforordningen artikkel 83 og ekomforskriften (2024) § 11-3.

Illustrasjon: Colourbox.com

tatilsynets myndighet begynner. Vurderingen av strengt nødvendig skal speile kravene i kommunikasjonsvernsdirektivet (direktiv 2002/58/EC) artikkel 5 nr. 3 og endringsdirektivet (direktiv 2009/136/EF). I endringsdirektivets fortalepunkt 66 står følgende om unntaket:

En undtagelse fra forpligtelsen til at give oplysninger og give ret til at nægte lagring eller adgang bør begrænses til de situationer, hvor den tekniske lagring eller adgang er strengt nødvendig til det legitime formål, der består i at gøre det muligt at benytte en specifik tjeneste, som abonnenten eller brugeren udtrykkeligt har anmodet om.

Vurderingstemaet overlapper med dataminimeringsprinsippet i personvernforordningen artikkel 5 nr. 1 bokstav c som innebærer at personopplysninger skal «være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for».

Ved siden av den overlappende reguleringen kan også praktiske hensyn skape fare for dobbeltforfølging og dobbeltstraff. Både NKOM og Datatilsynet kan initiere tilsyn med virksomheter på eget initiativ eller basert på klager eller tips fra enkeltpersoner og oppslag i mediene. Dersom begge tilsyn har mottatt en klage for samme forhold er det avgjørende at de har rutiner for samordning for å unngå at begge undersøker og sanksjonerer i den samme saken. For eksempel kan en

virksomhet som bruker cookies uten gyldig samtykke få én sanksjon fra Datatilsynet for brudd på personvernregelverket og én fra NKOM for tekniske mangler. Selv om begge vedtakene kan være saklige hver for seg, kan samlet reaksjon stride mot EMKs prinsipp om *ne bis in idem*.

Samordningsplikten i forvaltningsloven

Det er ikke upraktisk at flere forvaltningsorganer har myndighet til å ilegge sanksjoner for samme forhold.

Hva som utgjør ett og samme forhold vurderes ut fra kriteriene som gjelder ved avgjørelsen av hva som er en og samme «offence» (den norske oversettelsen: «straffbar handling») etter EMK protokoll 7 artikkel 4. «Samme forhold» foreligger etter EMDs praksis hvis det faktum som ligger til grunn for den administrative sanksjonen, er det samme eller vesentlig det samme som det som ligger til grunn for den strafferettslige forfølgningen.

Forvaltningsloven § 47 pålegger offentlige organer å samordne sin myndighetsutøvelse med påtalemyndigheten (første ledd) og med andre forvaltningsorganer (andre ledd) for å unngå dobbeltbehandling og motstridende vedtak. Bestemmelsen er en sentral del av norsk forvaltningsrett og reflekterer lovgivers ønske om en rettferdig og effektiv forvaltning. Formålet med samordningsplikten er «[…] å legge til rette for at dobbeltforfølgning unngås i sanksjonssaker, noe som igjen sikrer et passende samlet reaksjonsnivå mot lovbrudd og at belastningen ved gjentatt straffeforfølgning unngås», jf. Prop. 62 L (2015–2016) s. 200.

Samordningsplikten kan deles inn i to deler:

- Materiell samordning, som sikrer at ulike vedtak som gjelder samme forhold, er konsistente og ikke motstrider hverandre.
- Prosessuell samordning, som skal forhindre at virksomheter blir påført unødvendige byrder gjennom parallelle prosesser.

Forarbeidene til forvaltningsloven, særlig Ot.prp. nr. 3 (1976-77), understreker at samordning ikke bare er en praktisk nødvendighet, men også en rettslig forpliktelse. Når flere forvaltningsorganer har overlappende ansvarsområder, er det avgjørende at de samarbeider for å sikre en helhetlig og rettferdig behandling. I tråd med legalitetsprinsippet må dette gjelde med styrke jo strengere sanksjoner forvaltningsorganer kan ilegge.

Dobbeltforfølgelse er en utfordring for rettssikkerheten, fordi det kan medføre at virksomheter blir ilagt urimelige byrder. EMK tilleggsprotokoll nr. 7 artikkel 4 fastsetter at ingen skal straffes eller sanksjoneres to ganger for samme forhold. Dette prinsippet gjelder også i norsk rett, og Høyesterett har gjentatte ganger understreket betydningen av *ne bis in idem*.

I *Rt-2010-1121* (*Tilleggsskatt*) presiserte Høyesterett at administrative og strafferettslige sanksjoner som gjelder samme forhold, må være samordnet for å unngå brudd på EMK. Dette understreker behovet for at tilsynsmyndigheter som Datatilsynet og NKOM samarbeider tett i saker som involverer ekomloven § 3-15.

Hvordan samordningsplikten kan bidra

Samordningsplikten i forvaltningsloven § 47 kan bidra til å redusere risikoen for dobbeltforfølgelse ved å sikre at tilsynsmyndighetene koordinerer sine aktiviteter. Dette kan gjøres gjennom klare retningslinjer for ansvarsdeling, deling av informasjon mellom organene og en felles forståelse av hvordan overlappende saker skal håndteres.

Ved å oppfylle samordningsplikten kan Datatilsynet og NKOM sørge for at én myndighet tar hovedansvaret i saker som involverer både personvern og tekniske spørsmål. Dette vil ikke bare sikre rettssikkerheten for virksomheter, men også styrke tilliten til forvaltningen.

Andre land har utviklet ulike tilnærminger til samordning mellom tilsynsorganer. I EU er «one-stop-shop»-mekanismen under personvernforordningen et eksempel på hvordan grenseoverskridende saker kan behandles av én ledende tilsynsmyndighet. I Tyskland har samarbeidsavtaler mellom delstatlige datatilsyn bidratt til å sikre enhetlig praksis.

Norge kan hente inspirasjon fra slike ordninger for å forbedre samarbeidet mellom Datatilsynet og NKOM, spesielt i komplekse saker som gjelder informasjonskapsler og sporingsteknologi.

Veien videre

Den nye ekomloven representerer et viktig skritt for å sikre brukernes rettigheter i en digital hverdag. Samtidig reiser loven utfordringer knyttet til samordning og risiko for dobbeltforfølgelse. Forvaltningsloven § 47 gir et rammeverk for å håndtere disse utfordringene, men det forutsetter at tilsynsmyndighetene tar sin samordningsplikt på alvor. En effektiv koordinering mellom Datatilsynet og NKOM er avgjørende for å sikre rettferdighet, tillit og forvaltningens legitimitet.

Hanne Pernille Gulbrandsen, partner og advokat i Deloitte Advokatfirma AS og Ole Martin Moe, manager og advokatfullmektig i Deloitte Advokatfirma AS.

Hvem har ansvaret for feil knyttet til KI-systemer innen helse?

Av Julia Desiré Fuglestad Brodshaug

Systemer med kunstig intelligens (KI-systemer) utvikler seg raskt, og blir en stadig større del av helsevesenet. Teknologien kan brukes til alt fra diagnostikk, til behandling og oppfølging[1].

Innen kreftbehandling kan bilder og målinger tolkes på nye og mer effektive måter ved hjelp av KI, og helsepersonell kan få beslutningstøtte til å velge best mulig behandling for den enkelte pasient.[2] Logistikk vil kunne settes bort til KI-baserte løsninger, og på denne måten frigjøre ressurser som kan brukes på å bedre befolkningens helsetilbud.

Spørsmålet blir imidlertid hvem som står igjen med ansvaret når det oppstår feil knyttet til KI-systemer innen helse, og kravene til forsvarlig helsehjelp og informasjonsbehandling ikke overholdes.

Hvilke ansvarsroller finner vi i GDPR, AI Act og norsk helselovgivning?

En forsvarlig delegasjon av ansvar, og klare ansvars- og kompetansegrenser er en viktig del av forsvarlighetskravet innen helseretten. Hvilket ansvar som påhviler den enkelte, avhenger av rollen vedkommende person eller virksomhet har. Det knyttes ansvar til både bruk og utvikling av kunstig intelligens i helsehjelp.

Julia Desiré Fuglestad Brodshaug

Etter helselovgivningen er sentrale aktører i denne sammenheng «helsepersonell» og «virksomheten». «Helsepersonell» etter hpl. § 3 omfatter blant annet leger, sykepleiere og helsefagarbeidere. Med andre ord aktører som utfører «helsehjelp» slik dette er definert i hpl. § 3 tredje ledd. Med «virksomheten» menes, etter en ordlydsfortolkning, blant annet sykehus og andre institusjoner og virksomheter som organiserer helsehjelp.

Aktørene som er involvert etter GDPR (jf. personopplysningsloven), i behandlingen av helseopplysninger knyttet til KI-verktøy, er blant annet behandlingsansvarlig, databehandler og den registrerte. Reglene om ansvar etter personvernforordningen vil primært gjelde den behandlingsansvarlige[3]. På bakgrunn av dette er det sentralt å fastlegge hvem som er behandlingsansvarlig for helseopplysningene i det enkelte tilfellet, fordi vedkommende har mange forpliktelser.

Med «behandlingsansvarlig» menes den som alene eller sammen med andre «bestemmer formålet med behandlingen» av opplysningene og hvilke midler som skal benyttes, jf. GDPR artikkel 4 punkt 7. Den behandlingsansvarlige kan være en «fysisk» eller «juridisk» person. Videre kan også en «offentlig myndighet», en «institusjon» eller andre «organer» regnes som behandlingsansvarlig, jf. GDPR artikkel 4 punkt 7. Etter pasientjournalloven § 2 e er definisjonen av «dataansvarlig» et synonym med behandlingsansvarlig. «Databehandleren» etter GDPR artikkel 4 punkt 8 er den som behandler personopplysninger, herunder helseopplysninger, på vegne av den behandlingsansvarlige.

Den «registrerte» defineres som en fysisk identifiserbar person, jf. GDPR artikkel 4 punkt 1. I dette ligger det at den «registrerte» indirekte eller direkte må kunne identifiseres ved hjelp av ulike «identifikatorer» som eksempelvis navn eller identifikasjonsnummer. Det stilles flere krav etter GDPR som skal sikre at personvernet til den registrerte ivaretas.

Sentrale aktører etter AI Act er «provider» (heretter «leverandøren») og «deployer» (tidligere «user», heretter «brukeren»). AI act er et nylig vedtatt juridisk rammeverk som skal regulere kunstig intelligens

1 Direktoratet for E-helse «Forprosjekt - Utredning om bruk av kunstig intelligens i helsesektoren», nettside, 2019, Kunstig intelligens i helse (lest februar 2025).

2 Direktoratet for E-helse «Forprosjekt - Utredning om bruk av kunstig intelligens i helsesektoren», nettside, 2019, Kunstig intelligens i helse (lest februar 2025).

3 Datatilsynet, «Hva er en behandlingsansvarlig?», nettside, 2019, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/behandlingsansvarlig-og-databehandler/hva-er-en-behandlingsansvarlig/ (lest 22.11.2023).

på en forsvarlig måte[4]. Det følger av AI Act artikkel 3 (3) at med «leverandøren» menes den som utvikler et KI-system og skal sette det de har utviklet ut i markedet, eller skal ha det i en tjeneste under sitt eget navn eller varemerke[5]. Bestemmelsen gjelder også for en offentlig autoritet, et byrå eller andre organer. Dette gjelder både dersom KI-systemet tilbys gratis eller mot kompensasjon. Med «brukeren» menes juridiske eller fysiske personer, offentlig autoritet, byrå eller organ som bruker AI-systemer under sin myndighet, jf. AI Act artikkel 3 (4). Et unntak gjelder der AI-systemet brukes i en personlig sammenheng, i en ikke-profesjonell aktivitet.

Påvirker den digitale utviklingen ansvarsfordelingen innen helse?

Etter kravet til forsvarlighet, jf. hpl. § 4, må helsepersonell i dag forholde seg til utviklingen av kunstig intelligens innen helse, samt ny kunnskap om hva som kan forventes av dem på bakgrunn av dette[6]. En forutsetning for at helsepersonell skal kunne oppfylle dette individansvaret, er at virksomheten legger til rette for at den enkelte skal kunne opptre forsvarlig[7].

Beslutningen om at helsepersonell skal bruke KI-systemer i helsehjelp, forutsetter som regel at dette er en beslutning som er tatt av virksomhetens ledelse. Dersom virksomheten bestemmer at kunstig intelligens skal brukes i behandlingen av pasienter, kan det argumenteres for at utgangspunktet er at det er virksomhetens ansvar å rette opp i eventuelle uforsvarlige forhold knyttet til dette, jf. hpl. § 16, jf. forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten § 9.

Det kan stilles spørsmålstegn ved om en økt bruk av KI-utstyr i helsehjelpen i praksis vil innebære at mer av ansvaret for forsvarlig helsehjelp flyttes fra helsepersonellet over til virksomheten.

Der det ikke er tilrettelagt for at helsepersonellet skal kunne overprøve og kvalitetssikre eksempelvis beslutningsstøtteverktøy, vil ansvaret for feil som oppstår i forbindelse med dette kunne tilfalle virksomheten, jf. hpl. § 16. Videre er det sykehusets ansvar at helsepersonellet har fått tilstrekkelig opplæring i hvordan KI-utstyret skal brukes, jf. hpl. § 16. Det kan argumenteres for at KI-systemer med økende innflytelse reduserer helsepersonellets kliniske skjønn. Dette vil i så fall kunne påvirke hvordan ansvaret burde fordeles når det oppstår feil.

Der medisinsk utstyr med kunstig intelligens får uforutsette konsekvenser, vil virksomhetsansvaret videre grense mot blant annet produktansvaret etter produktansvarsloven. Lov om medisinsk utstyr vil også gjelde slike KI-verktøy.

Hvem har ansvaret for helseopplysningene som brukes i KI-verktøy?

Helsepersonellets individansvar innebærer også en plikt til å behandle opplysninger på en forsvarlig måte. Dette innebærer blant annet at helsepersonell har taushetsplikt etter helsepersonelloven kapittel 5. Videre har helsepersonell en plikt til å dokumentere etter helsepersonelloven kapittel 8. Ansvaret som følger av disse pliktene kan grense mot behandlingsansvaret.

All behandling av helseopplysninger skal kunne knyttes til en behandlingsansvarlig (i helselovgivningen omtalt som «dataansvarlig»)[8]. Det er som oftest virksomheten, eksempelvis sykehuset, som regnes som den behandlingsansvarlige i en helserettslig sammenheng, jf. GDPR artikkel 4 nummer 7. På denne måten kan en virksomhet både ha virksomhetsansvaret for helsehjelpen og behandlingsansvaret for personopplysningene. Sagt med andre ord, kan samme aktør dermed ha flere ansvarsroller samtidig.

For å videre bygge opp ansvarslandskapet, er det verdt å nevne bestemmelsene i den nylig vedtatte AI Act. Målet med denne lovgivningen er blant annet å sikre at KI-teknologi blir utviklet og brukt på en forsvarlig måte. AI Act utgjør med dette et ytterligere regelverk som pålegger ulike aktører forpliktelser for å sikre at bruken og utviklingen av kunstig intelligens-systemer innen helse, ikke skal føre galt av sted.

I AI Act er det leverandøren som er underlagt flest forpliktelser. Brukeren er imidlertid også en sentral aktør. En slik bruker kan for eksempel være et sykehus som kjøper inn et beslutningsstøtteverktøy som skal bidra til å stille diagnoser på pasienter. Dette innebærer at flere av forpliktelsene som før kun ble lagt på leverandøren, nå også gjelder for brukerne etter AI Act[9]. Sett i lys av GDPR, vil dette innebære at brukere etter AI Act i flere tilfeller også må underlegges reglene knyttet til den behandlingsansvarlige etter GDPR[10]. Videre vil leverandøren ha ansvar som behandlingsansvarlig i sin opptrening og utvikling av KI-systemet, ettersom vedkommende i sammenheng med dette faller inn under definisjonen i GDPR artikkel

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

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

6 Hauglid 2023, hpl. §4 note 1.

7 Hauglid 2023, hpl. § 4 note 1.

8 Helse- og omsorgsdepartementet, «Informasjonshåndtering i spesialisthelsetjenesten», rundskriv, på s. 8, 12. april 2019, https://www.regjeringen.no/contentassets/2612793fd9274d42aea938cc9764f4d0/190412_rundskriv_informasjonshaandtering_spesialisthelsetjenesten.pdf.

9 Anna Tamuly, «Hvordan samspiller risikovurderingene i AI Act med risikovurderingene i GDPR?», *Lov & Data*, 2023 punkt 2, https://lod.lovdata.no/article/2023/09/Hvordan%20samspiller%20risikovurderingene%20i%20AI%20Act%20med%20risikovurderingene%20i%20GDPR.

10 Europaparlamentets og Rådets direktiv (EU) 2016/679.

Illustrasjon: Colourbox.com

4. Når opptreningsperioden er ferdig, og vedkommende leverandør selger KI-systemet til en bruker, vil vedkommende leverandør overfor denne brukeren ofte ha rollen som databehandler. Dette vil innebære at samme aktør kan ha flere ansvarsroller[11] som endrer seg avhengig av hvor i prosessen man er. Dette utgangspunktet kompliseres ytterligere ved at det finnes ulike former for kunstig intelligens, med ulike prosesser og former for maskinlæring.

Avsluttende bemerkninger

I sammenheng med forsvarlighetskravet kan en uklar, overlappende og komplisert ansvarsfordeling stride mot kravet om klare ansvars- og kompetanseforhold. Dette kan utgjøre en risiko for den enkelte pasient sitt krav på forsvarlig helsehjelp og informasjonsbehandling. Det er viktig at hovedaktørene innen bruk og utvikling av KI-utstyr innen helse har en tydelig tildelt ansvarsrolle slik at regelverket kan overholdes. Denne artikkelen har vist at de ulike ansvarsrollene kan grense mot hverandre og tidvis overlappe. Videre har artikkelen fremhevet at samme aktør kan ha flere roller samtidig, og at rollene kan endre seg og byttes om under ulike stadier i utviklingen og bruken av det samme KI-systemet. Artikkelen er ment som et utgangspunkt for juridisk drøftelse rundt ansvarsfordelingen ved feil knyttet til KI-systemer innen helse i tiden som kommer.

> Det er viktig at hovedaktørene innen bruk og utvikling av KI-utstyr innen helse har en tydelig tildelt ansvarsrolle slik at regelverket kan overholdes

Julia Desiré Fuglestad Brodshaug, jobber som jurist i Helfo. Korrekturlest av Simen Hafstad-Moi, jurist i Helfo.

11 Anna Tamuly, «Hvordan samspiller risikovurderingene i AI Act med risikovurderingene i GDPR?», *Lov & Data*, 2023 punkt 2, https://lod.lovdata.no/article/2023/09/Hvordan%20samspiller%20risikovurderingene%20i%20AI%20Act%20med%20risikovurderingene%20i%20GDPR.

Justisdepartementets planseksjon 1976–1981

Av Trygve Harvold

Bakgrunn:
Departementet ønsket seg en planleggingsenhet som i første omgang kunne arbeide med koordinering, prioritering og langtidsplanlegging i budsjettsaker samt koordinering av forskningsoppgaver innen justissektoren og administrativt utviklingsarbeid. Man tenkte seg en planleggingsseksjon organisert på linje med de øvrige avdelingene i departementet. Utredningskontoret kunne da gå inn som en del av den nye enheten. I 1975 ble utredningskontoret (ledet av byråsjef Hjalmar Austbø), flyttet ut av avdelingen og gjort om til en egen seksjon: Planseksjonen. Austbø ble nå underdirektør for denne aller første seksjonen i Justisdepartementet. Ved siden av tinglysingsfeltet fikk Planseksjonen også ansvaret for departementets budsjett som inntil da hadde vært lagt til 2. sivilkontor.

Kilde: Ole Kolsrud: Rekonstruksjon og reform. Regjeringskontorene 1945–2005, s. 79.

Jon Bonnevie Høyer og jeg begynte samtidig i Justisdepartementets nyopprettete Planseksjon i januar 1976. Vi hadde begge søkt stillingen som byråsjef, hvor det i utlysningsteksten blant annet sto at «seksjonen skal arbeide med … behandling av departementets løpende tingslysingssaker … og utrede spørsmålet om bruk av EDB i justissektoren.» Seksjonen arbeidet i tillegg med blant annet behandling av departementets langtidsbudsjett og koordinering av forskning. Seksjonen ble ledet av underdirektør Hjalmar Austbø.

Jon kom fra Regjeringsadvokaten mens jeg kom fra en vit.ass. stilling

Trygve Harvold

ved Institutt for Privatrett ved UiO. Heldigvis var det Jon som fikk byråsjefstillingen, og dermed ansvaret for den løpende saksbehandlingen av tinglysingsklager, mens jeg ble ansatt som konsulent og anvist et skrivebord i et lite kontorfellesskap i tredjeetasje over gamle restaurant «Justisen» i Grubbegata, og ellers overlatt til meg selv. Ingen hadde ennå funnet ut av hva jeg skulle gjøre, og dette passet meg bra, fordi jeg allikevel var travelt opptatt med å skrive ferdig en bok om rettslige informasjonssystemer sammen med Jon Bing. Fordi jeg kom på jobb hver morgen og skrev flittig gjennom hele dagen, trodde alle jeg allerede var tildelt oppgaver, og jeg fikk dermed jobbe i fred i flere uker med boken. Til slutt begynte imidlertid folk å snakke med meg og misforståelsen fort oppklart, og jeg ble satt til å jobbe med «bruk av EDB i tinglysingen».

Det var to hovedgrunner til at akkurat denne problemstillingen var svært aktuell på den tiden. For det første hadde gjennomsnittlig ventetid for å få tinglyst et dokument økt fra 14 dager i 1971 til mer enn 60 dager i 1975 som følge av at antall tinglysingsforretninger hadde økt med mer enn 60 % i perioden. For det andre regnet man med at forslaget til ny pantelov ville bli vedtatt av Stortinget i 1980. Denne loven ville åpne for utvidet pant i løsøre, noe som garantert ville medføre en ytterligere økning i tinglysingsvolumet. Man innså at man med det eksisterende opplegget aldri ville klare å oppfylle tinglysingslovens frist om to uker behandlingstid.

Alternativet var databaserte systemer. På den tiden var det imidlertid ikke innlysende hvordan slike systemer burde se ut. Man besluttet derfor å etablere et prøveprosjekt ved et tinglysingskontor nær Oslo. Den gang var det ca. 100 tinglysingskontorer i Norge. De var tilknyttet sorenskriverembeter, og slett ikke alle var veldrevet, dvs. uten restanser. Men sorenskriver Johannes E. Ruud drev et slikt kontor på Strømmen og han var også interessert i å være prøvekanin.

Høsten 1976 ble det besluttet å sette i gang et prøveprosjekt på Strømmen basert på lokal registrering av dokumenter, overføring via telenettet til Statens driftssentral for oppdatering av basen, og tilbakeføring via telenettet av de oppdaterte opplysningene om eiendommen, altså et klient-tjener opplegg. Jeg fikk oppdraget med å lage spesifikasjonen til systemet, som så ble programmert i Rasjonaliseringsdirektoratet. Dette tok ca. et år og uttestingen av systemet begynte ved utgangen av 1977.

Kåre Fløisand var direktør i Rasjonaliseringsdirektoratet og full av energi og initiativ. Han var helt sentral i både etableringen av prøve-

prosjektet på Strømmen og senere i etableringen av Løsøreregisteret ved Brønnøy sorenskriverembete.

Fordi den nye panteloven åpnet for utvidede muligheter til pant i løsøre var nødvendigheten av å etablere et løsøreregister helt akutt. Så samtidig som vi arbeidet med Strømmen-prosjektet, arbeidet vi med å etablere et løsøreregister. Prosjektene hadde fellestrekk, men var allikevel forskjellig. Løsøreregisteret måtte bli et nytt system basert på én lokasjon og ville kreve langt større bevilgninger. Å få det etablert ville kreve politisk enighet i Stortinget. Det var Jon Bonnevie Høyer som kom opp med taktikken om å bruke distriktspolitikk som et middel til få igjennom en rask beslutning. Vanligvis ble det mye bråk i forbindelse med å flytte eksisterende forvaltningsorgan ut av Oslo, men å etablere et helt nytt organ, som ingen forbandt noe særlig med, mente han ville gå greit. Så mens han skrev en begrunnelse for systemet, beskrev jeg maskinkravene til systemet og utarbeidet flytdiagrammer for den nødvendige programvaren, som senere ville bli programmet av Rasjonaliseringsdirektoratet – alt ting som måtte være klart før budsjettbehandlingen i Stortinget.

I begynnelsen av 1978 ble det sendt ut brev til tinglysingskontorene ved landets sorenskriverembeter med spørsmål om man var interessert i å være vert for et nytt løsøreregister som skulle etableres i Distrikts-Norge. I Planseksjonen gikk vi de neste dagene spent rundt og så på telefonen. Det kom flere tilbakemeldinger på forespørselen, men etter en bestemt telefon spratt Jon i været med hendene i været og et stort smil rundt munnen, og vi skjønte at saken i praksis var i boks. Telefonen var fra sorenskriver og ordfører i Brønnøy Bodil Aakre. Hun var også tidligere stortingsrepresentant 1965–1969 og kunne tilby gode lokaler og tilstrekkelig arbeidskraft fordi telefonsentralen i Brønnøysund snart skulle digitaliseres. Saken skled gjennom Stortinget uten motforestillinger.

Samtidig gikk prøveprosjektet på Strømmen sin gang. Hele 1978 gikk med til å teste systemet og sette det i drift. Feil og mangler ble identifisert og rettet. Fra og med 1 januar 1979 ble alle tinglysingsdokumenter som kom til Strømmen registrert i det nye systemet. Og Strømmen var det første stedet de nyansatte i Brønnøysund dro for å besøke.

Mens dette foregikk, jobbet vi i Planseksjonen også med en helt annen problemstilling, nemlig ønsket om å gjøre sentrale rettskilder lettere tilgjengelig, i første omgang for saksbehandlerne i forvaltningen. Allerede da jeg var vit.ass. på universitetet hadde Jon Bing og jeg samarbeidet med Fløisand i Rasjonaliseringsdirektoratet. Direktoratet hadde blant annet gått til innkjøpt av det engelske tekstsøkesystemet STATUS, som var utviklet ved UK Atomic Energy Authority for søking i lovtekst. Tønnes Ore ved Rasjonaliseringsdirektoratet og jeg omprogrammerte mer eller mindre hele systemet til det vi håpet var en mer brukervennlig versjon. Vi kalte resultatet NOVA*STATUS (norsk versjon av STATUS).

> Mens dette foregikk, jobbet vi i Planseksjonen også med en helt annen problemstilling, nemlig ønsket om å gjøre sentrale rettskilder lettere tilgjengelig.

Men selv om vi hadde et tekstsøkesystem hadde vi ikke noen digitaliserte lover vi kunne fôre det med. Digitalisering av tekst var nesten prohibitivt dyrt på 1970-tallet. Å gå til Stortinget å be om noe slikt, anså vi for helt nytteløst.

Men så kom nok en gang utviklingen oss i møte. Blysatsen som ble brukt til å trykke *Norges Lover* var utslitt. I 1978 opprettet styret i Det juridiske fakultets lovsamlingsfond en arbeidsgruppe for å utrede de organisatoriske, økonomiske og tekniske forutsetninger for å kunne produsere et digitalt trykkegrunnlag for 1981-utgaven. Arbeidsgruppen besto av Jon Bing og meg. Resultatet forelå i begynnelsen av 1979, og styret spurte om jeg ville lede redaksjonen som skulle utføre jobben. Jeg søkte derfor om permisjon fra departementet fra og med 1. mai 1979. Resultatet av det hele var at redaksjonen, som vi hadde kalt Lovdata, i begynnelsen av 1981 satt med en digitalisert versjon av lovene, samt kunnskapen og teknologien som i prinsippet gjorde det mulig å digitalisere resten av regelverket. Men da trengte vi en ny organisasjon, for det lå ikke i Lovsamlingsfondets mandat å påta seg en slik oppgave.

Problemet var å overbevise den politiske ledelsen i departementet (og professorene ved fakultetet) om å omorganisere Lovdata til en selvstendig enhet. Også her viste Jon Bonnevie Høyer sitt organisatoriske talent ved å begrunne opprettelse i et eget pro memoria hvor han blant la vekt på at det var ønskelig å unngå en kommersialisering av det planlagte systemet og at systemet burde være helt uavhengig av potensielle parter i rettskonflikter. Han mente derfor at både aksjeselskap og forvaltningsorgan var lite egnet som organisasjonsform og foreslo at Lovdata ble etablert som en allmennyttig, selvfinansierende stiftelse. Kravet om selvfinansiering ble begrunnet både med uavhengighet og med at det ville gjøre det lettere å dekke et markedsbehov som ville være voksende og i sterk utvikling.

Avtalen mellom departementet og fondet om opprettelsen av Lovdata sukret pillen for fondet gjennom et pengebidrag fra departementet. For å berolige politikerne ble det opprettet et «Råd for rettsinformasjon» som skulle holde Lovdata i ørene. Dette rådet forsvant ut

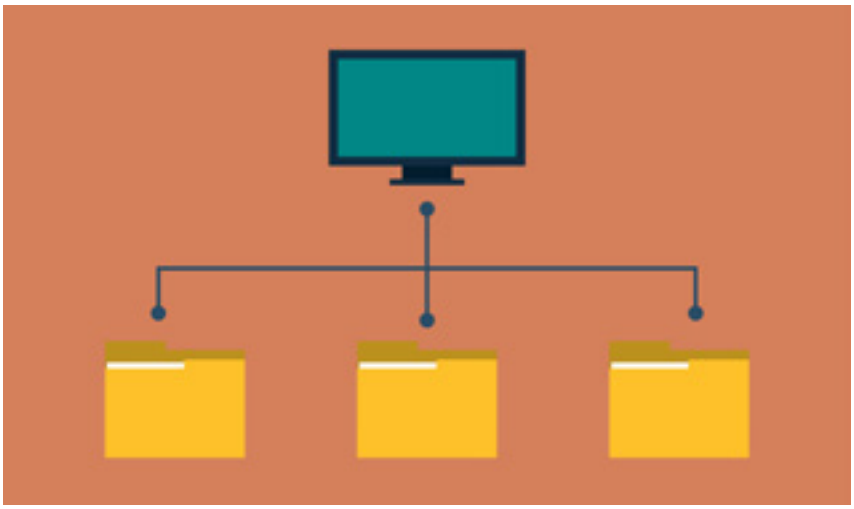
av bildet etter hvert, ettersom det egentlig ikke hadde noen annen funksjon enn å få Lovdata opprettet. Den virkelige beslutningsmakten lå jo uansett i Lovdatas styre som representerte hele justissektoren i Norge. I prosessen som ledet frem til enighet om avtalen var professor Knut Selmer og underdirektør Hjalmar Austbø helt avgjørende i bearbeidelsen av hver sin institusjon.

At Lovdata ble opprettet som en stiftelse var på ingen måte gitt på forhånd. Jeg vet faktisk ikke om noe annet land hvor det rettslige informasjonssystemet er organisert på denne måten. Det vanlige er at det enten drives i statlig regi eller som et privat aksjeselskap. I større land har man ofte begge deler. At denne løsningen faktisk var mulig i Norge i 1981, tror jeg blant annet skyldes at vi var så tidlig ute at det ennå ikke var sterke etablerte interesser som kunne forhindre etableringen.

Hvordan gikk det så med disse tre prosjektene som i løpet av bare noen få år sprang ut av Planseksjonen.

Lovdata hadde noen vanskelige år i begynnelsen. Det tok tid å utvikle basene og det var vanskelig å konkurrere med tradisjonelle trykksaker i et konservativt juristmarket. Men både den teknologiske utviklingen og Lovdatas organisasjonsform var på stiftelsens side. Fordi organisasjonene og institusjonene som utgjorde justissektoren i Norge satt i styret, fikk Lovdata tilgang til rettskildene og kunne knytte dem sammen i et henvisningssystem som var unikt. Og den teknologiske utvikling medførte at trykksakene uansett ble utkonkurrert på områder som krevde hurtige oppdateringer og distribusjon.

Løsøreregisteret i Brønnøysund var en suksess fra dag en, blant annet fordi man var heldig med å få ansatt svært dyktige mennesker til å videreutvikle og drive systemet. Det var så vellykket at det ble starten på en kjedereaksjon hvor stadig flere



Illustrasjon: Colourbox.com

registre ble lagt dit. Allerede i 1981 kom Ektepaktregisteret og Regnskapsregisteret, og antallet er etter hvert vokst til over 20. I 1988 ble Brønnøysundregistrene skilt ut som egen statlig forvaltningsetat og dermed var forbindelsen med Brønnøysorenskriverembete slutt. Men den tilknytningen hadde uansett bare vært et grep Bonnevie Høyer brukte for i det hele tatt å få registeret etablert.

Prøveprosjektet på Strømmen fikk en mer trøblete utvikling. En ting var å digitalisere grunnboken i et relativt lite og veldrevet tinglysingskontor, noe helt annet var å skalere dette opp til hele landet. Det ville bli dyrt og man klarte ikke å få det inn i statsbudsjettet. Jon Bonnevie Høyer foreslo derfor i 1986 å finansiere digitaliseringen ved salg av informasjon online fra den elektroniske grunnboken, dvs. den selvfinansierende Lovdata-modellen overført til tinglysingskontorene. For å få til dette ble Tinglysingsdata AS stiftet i 1987 av AL Kommunedata og Statens Datasentral AS. Selskapet fikk enerett på salg av informasjon fra den elektroniske grunnboken samt 85 % av gebyrinntektene av pantattestene. Det viste seg imidlertid at salget ikke ble som forventet og staten måtte overta selskapet i 1992. Selve digitaliseringen begynte i 1989 og pågikk helt til 1995. Fordi grunnbøkene befant seg i kasser i tinglysingskontorene som igjen befant seg i domstolene, medførte digitaliseringen av grunnboken også den første innføringen av moderne datautstyr i domstolene. Men når først grunnbøkene var digitalisert var det liten grunn til å fortsette med lokal registrering rundt omkring i tingrettene. I 2002 vedtok derfor Stortinget at tinglysing av rettigheter i fast eiendom skulle overføres fra tingrettene til Statens kartverk. Vedtaket ble gjennomført i løpet av 2004–2007.

Noter

Innføringen av IT i domstolene og blant annet prøvesjosjektet på Strømmen er beskrevet av Even Nerskogen i «IT i domstolene», Complex 1 2003.

Opprettelsen av Løsøreregisteret sett fra Brønnøysundregistrenes sin side er beskrevet av Harald Harnang i «Brønnøyregistran – Værsågod!», 2003.

Opprettelsen av Lovdata sett fra Senter for rettsinformatikk sin side er beskrevet av Iver Tangen Stensrud i «Retten i det digitale Norge», 2020.

Trygve Harvold, direktør i Lovdata fra 1981 til 2010.

Personvernlovgivning fra 1970-tallet og til i dag

Av Arve Føyen

1. Personvern – Introduksjon

I 2024 var det 40 årsjubileum for det samfunnet George Orwell beskrev i boken «1984» (publisert i juni 1949). En liten påminnelse fra boken er at «Partiets» endelige mål ikke bare er å overvåke og kontrollere folks handlinger, men å kontrollere deres tanker og ødelegge deres menneskelighet. Hovedpersonen Winstons nederlag representerer totalitarismens triumf over individuell frihet og menneskeverd. I det samfunnet som beskrives i boken er alle overvåket av myndighetene. «Storebror» følger med på alt, både i det private og i det offentlige liv. Befolkningen blir hele tiden påminnet om dette med slagordet «Storebror ser deg».[1]

Hvordan har så vernet om individuell frihet, menneskeverd og personopplysninger stått seg i de 40 årene som har gått siden det Orwellske samfunnet ble beskrevet i «1984»?

2. Personvern – utviklingstrekk og utfordringer

Personvern har gjennomgått store endringer siden begynnelsen av 1970-tallet, drevet av teknologisk utvikling, økt bruk av digitale løsninger, og strengere lovgivning. Denne artikkelen tar for seg sentrale utviklingstrekk innen personvern i Norge og internasjonalt, med et særlig fokus på teknologiske utfordringer, endringer i lovgivning over tid, og innføringen av GDPR.

Arve Føyen

2.1. Litt begrepsbruk [2]

Personlig integritet innebærer individets rett til å leve sitt liv uten unødvendig innblanding fra andre, inkludert staten, bedrifter og private aktører. Denne retten strekker seg til å beskytte individets personlige sfære, inkludert deres fysiske og psykiske velvære.

Personlighetens rettsvern refererer til juridiske beskyttelser som anerkjenner individets rett til å kontrollere og beskytte sitt eget privatliv, bilde, navn og øvrige personlige kjennetegn. Dette omfatter både vern mot krenkelser og urettmessig utnyttelse av individets personlighet i for eksempel media og reklame.

Personvern er et bredere konsept som omfatter beskyttelsen av individers rettigheter og friheter i sammenheng med behandling av deres personopplysninger. Dette omfatter retten til privatliv og retten til å kontrollere hvordan ens personopplysninger samles inn, brukes, oppbevares og deles. Personvern er derfor en viktig del av både personlig integritet og personlighetens rettsvern.

I utredningen «Individ og integritet» (NOU 2009: 1) fremgår det at Person*opplysnings*vern dreier seg om regler og standarder for behandling av personopplysninger som har ivaretakelse av personvern som hovedmål.[3] Personopplysningsvern spesifikt refererer til de tiltak og reguleringer som er innført for å beskytte opplysninger om enkeltindivider mot misbruk og uautorisert tilgang. Dette inkluderer lovgivning som personopplysningsloven og GDPR, helseregisterloven, og politiregisterloven, som legger sterke føringer for hvordan og for hvilke formål data skal innhentes, behandles, tilgjengeliggjøres, lagres og beskyttes, for å sikre at individets rettigheter ivaretas.

Disse begrepene er nært forbundet og overlapper på mange måter, men de representerer også ulike aspekter av individets rett til beskyttelse mot inngrep i deres private liv. Samlet sett utgjør de et rammeverk som søker å balansere behovet for fri informasjonsflyt med hensynet til beskyttelse av individets friheter verdighet og rettigheter.

2.2. Bakgrunn – utvikling av personopplysningsvernet

Utviklingen av personopplysningsvernet som juridisk og samfunnsmessig diskusjonstema knyttet til bruk av datamaskiner begynte på 1960-tallet og akselererte inn i 1970-tallet. Denne perioden var preget av en økende bevissthet om

1 Basert på Wikipedia

2 Basert på fremstillingen i NOU 2009:1 kapittel 4.1

3 NOU 2009 kapittel 4.1.5

datateknologiens potensial til å samle, behandle og lagre store mengder informasjon om enkeltpersoner. Samtidig vokste bekymringene for hvordan denne informasjonen kunne misbrukes av både offentlige og private aktører.

Den teknologiske utviklingen innen databehandling og informasjonsteknologi førte til en omfattende diskusjon om behovet for å beskytte individers personopplysninger. På 1970-tallet ble det i flere land, inkludert Norge, iverksatt undersøkelser og utredninger om personvernproblemer knyttet til både offentlig og privat bruk av personopplysninger. Internasjonale organisasjoner som Europarådet og OECD bidro også til utviklingen av personvernprinsipper som skulle ligge til grunn for fremtidig lovgivning. Sveriges datalov fra 1974 var den første i sitt slag, og markerte starten på en lovgivningsbølge innen personvern i Europa.

Erik Samuelsens forskningsrapport fra 1972 om personvern[4] var en banebrytende studie som utforsket de juridiske og samfunnsmessige aspektene ved beskyttelse av individers personopplysninger. Rapporten fremhevet de teknologiske utfordringene knyttet til databehandling og informasjonsteknologi, og hvordan disse kunne utgjøre en trussel mot personlig integritet.

Samuelsen analyserte behovet for lovgivning for å regulere innsamling, lagring og behandling av personopplysninger. Han understreket viktigheten av å balansere informasjonsflyt med beskyttelse av individets rettigheter. Hans arbeid var med og legge grunnlaget for senere utvikling av personvernlovgivning i Norge, og bidro til den økende bevisstheten rundt personvernproblematikk på 1970-tallet.

På 1970-tallet ble det nedsatt to offentlige utvalg for å undersøke problemstillinger knyttet til behandling av personopplysninger og personvern i Norge. Den første utredningen, NOU 1974: 22 – Persondata og personvern, tok for seg de grunnleggende prinsippene og utfordringene knyttet til personvern, i en tid med rask teknologisk utvikling. Rapporten fokuserte på hvordan personopplysninger ble samlet inn, lagret og brukt i privat sektor, samt behovet for regler og reguleringer for å beskytte individers rettigheter.

Den andre utredningen, NOU 1975: 10 Offentlige persondatasystem og personvern, rettet oppmerksomheten mot de spesifikke utfordringene ved offentlige persondatasystemer. Utvalget evaluerte eksisterende praksis og foreslo tiltak for å styrke personvernet i offentlige registre og databaser. Disse to utredningene la grunnlaget for at departementet utarbeidet Ot prp nr 2 (1977–78) om lov om personregistre mm («Personregisterloven»). Loven ble vedtatt av Stortinget den 9. juni 1978.

3. Personregisterloven

3.1. Forskrifter, konsesjoner og iverksettelse

Personregisterloven var vedtatt av Stortinget den 9. juni 1978. Loven var en utpreget fullmaktslov, med vide fullmakter for Regjering og departement (Justisdepartementet) til å fastsette forskrifter. Før loven kunne tre i kraft, måtte det utarbeides forskrifter, og det måtte etableres et Datatilsyn for å håndheve loven.

Av ulike årsaker havnet den vedtatte loven i en skuff i Justisdepartementet, og det skjedde ikke noe med iverksettelse på omtrent ett år. Først ca. ett år etter vedtakelse av loven ble det nedsatt en hurtigarbeidende arbeidsgruppe for å utarbeide forskrifter og etablere Datatilsynet. Arbeidsgruppen hadde ett medlem fra Statens Rasjonaliseringsdirektorat («R-dir» - tilsvarende det som nå er Dig-Dir/DFØ) som prosjektleder, ett medlem fra Sivilavdelingen i Justisdepartementet, og ett medlem fra lovavdelingen i Justisdepartementet. I løpet av 7 måneder skulle arbeidsgruppen utarbeide utkast til forskrifter som skulle ferdigstilles etter en ekstern høringsrunde, slik at de kunne iverksettes sammen med loven pr. 1. januar 1980. Samtidig skulle arbeidsgruppen etablere Datatilsynet, og ansette de første 4–6 medarbeiderne i Datatilsynet, skaffe og utstyre lokaler til Datatilsynet, og drive utstrakt informasjonsvirksomhet om krav til næringsliv og forvaltning i den nye loven.

Opprinnelig gjaldt personregisterloven for personregistre – manuelle og elektroniske. «Personregistre» var definert som registre, fortegnelser m.m. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte person kan finnes igjen. Loven gjaldt også for annen bruk av personopplysninger i visse typer virksomheter, som inkluderte:

- Kreditt- og personopplysningsvirksomhet
- Databehandlingsforetak
- Adresserings- og distribusjonsvirksomhet
- Opinions- og markedsundersøkelser
- Overføring til utlandet
- Fjernsynsovervåkning.

Igangsetting og drift av slike virksomheter krevde konsesjon fra Datatilsynet.

Personregisterloven påla behandlingsansvarlige en rekke plikter for å sikre at personopplysningene ble behandlet i samsvar med loven. Dette inkluderte blant annet:

- Søknad om konsesjon: Virksomheter måtte søke om konsesjon fra Datatilsynet før de kunne opprette nye personregistre. Virksomheter som drev innen ovennevnte virksomhetstyper, måtte søke konsesjon for å kunne drive sin virksomhet. Det ble gitt overgangsregler med utsatt

4 Erik Samuelsen – Statlige databanker og personlighetsvern – Universitetsforlaget 1972

frist for å søke konsesjon for allerede etablerte registre eller virksomheter.
- Sikkerhet: Virksomheter skulle treffe nødvendige sikringstiltak for å sikre ivaretakelse av opplysningenes integritet og at de ikke kom på avveie.
- Innsynsrett: Alle fikk rett til å få opplyst hvilke opplysninger om dem selv som lagres eller bearbeides ved elektroniske hjelpemidler.
- Handlingsplikt etter pålegg fra Datatilsynet: Virksomheter hadde plikt til å innrette seg etter pålegg fra Datatilsynet om retting, sletting eller supplering av feil i register, og om tiltak som er nødvendige for at evt. feil ikke får betydning for den registrerte.

Basert på konsesjonssystemet krevde loven som utgangspunkt at enhver virksomhet som ønsket å føre personregistre, eller drive slik virksomhet som angitt, måtte søke om tillatelse (konsesjon) fra Datatilsynet. Dette systemet skulle sikre at bruken av personopplysninger skjedde i samsvar med lovens bestemmelser, og at nødvendige sikkerhetstiltak var på plass for å beskytte opplysningene mot uautorisert tilgang, endring eller sletting.

Den oppnevnte arbeidsgruppen forsto umiddelbart at det var nødvendig med omfattende unntak fra loven, i form av forskriftsregulering av forskjellige standard typer registre som kunne unntas fra individuell konsesjonsbehandling. Unntakene ble gjort med hjemmel i loven, ved å definere hvilke typer opplysninger registrene kunne inneholde, hvilke formål de kunne brukes til, hvor opplysningene kunne hentes inn, hvem som kunne få tilgang til opplysningene osv.

Forskriften stilte videre krav til hvordan personopplysninger skulle behandles for at det ikke skulle kreves konsesjon. Kravene omfattet:
- Formålsbinding: Opplysningene skulle kun brukes til det formålet de var samlet inn for, og ikke til andre formål uten samtykke fra den registrerte.
- Registeransvarlig: Virksomhetens ledelse var ansvarlig for å følge reglene i forskriften.
- Korrekthet: Opplysningene måtte være nøyaktige og oppdaterte.
- Sikkerhet: Det skulle være tilstrekkelig tekniske og organisatoriske tiltak for å beskytte opplysningene mot uautorisert tilgang og andre sikkerhetstrusler.
- Innsynsrett: Den registrerte hadde rett til innsyn i hvilke opplysninger som var registrert om seg selv, samt informasjon om formålet med behandlingen og hvem som hadde tilgang til opplysningene.
- Utlevering av opplysninger: Personopplysninger måtte ikke leveres ut annet enn i konkret angitte tilfelle.
- Kobling av registre: Hvis et register skulle kobles med andre registre slo konsesjonsplikten i utgangspunktet inn igjen.
- Sletting: Hvis ikke annen lovgivning hindret sletting- kunne som utgangspunkt enhver kreve seg slettet fra registeret.

3.2. Datatilsynets rolle

Datatilsynet ble etablert som et frittstående organ underordnet Kongen og det departement Kongen fastsatt (Justisdepartementet). Datatilsynets ansvar var å overvåke etterlevelsen av Personregisterloven og forskriften. Datatilsynet hadde bl.a. følgende oppgaver:
- Behandling av konsesjonssøknader: Vurdere og godkjenne søknader om tillatelse til å opprette personregistre.
- Kontroll og tilsyn: Utføre tilsyn og kontroller for å sikre at virksomheter fulgte lovens krav.
- Veiledning: Gi råd og veiledning til virksomheter og enkeltpersoner om personvernspørsmål.
- Håndheving: Iverksette nødvendige tiltak ved brudd på loven, inkludert sanksjoner og pålegg.

3.3. Konsekvenser av brudd

Brudd på Personregisterlov – eller forskrift – kunne medføre straffesanksjoner hjemlet i lov og forskrift. Sanksjonene omfattet mulighet for pålegg om å stanse ulovlig behandling av personopplysninger (som kunne pålegges av Datatilsynet), fengselsstraff, bøter og erstatning til de registrerte (som måtte fastsettes av domstolene på vanlig måte). Det er grunn til å merke seg at loven ga grunnlag for personlig straffeansvar for ledelsen av den virksomheten som var ansvarlig for brudd på loven.

4. Behov for endringer – Personopplysningsloven 2000

4.1. Utredning om behovet for endringer

Personregisterloven var krevende å håndheve. På 1980-tallet var Datatilsynet preget av kapasitetsproblemer, med få ansatte og en voksende arbeidsmengde. Dette førte til at undertegnede i 1982 ble engasjert av Justisdepartementet for å utrede forslag til endringer og forenklinger i loven.[5]

Utredningen gjaldt forenkling og tilpasning av personregisterloven, for å bringe bedre overensstemmelse mellom Datatilsynets arbeidsoppgaver og tilgjengelige ressurser, sett på bakgrunn av den teknologiske utvikling.

Datatilsynet hadde på dette tidspunkt 8 ansatte (3 saksbehandlere) inklusive kontorpersonale, og betydelige restanser mht. behandling av konsesjonssøknader for «gamle» registre. Tilsynet hadde ingen med teknisk bakgrunn og ingen til å drive kontrollvirksomhet.

Da det ble ansett som uaktuelt med en betydelig styrking av Datatilsynet ble det mest nærliggende forslaget å fjerne konsesjonsplikten og innføre materielle regler med straffesanksjoner for overtredelse. Et hovedproblem med dette, var å

5 Complex nr. 1/1983 Utredning om endringer i Personregisterloven

innføre straffesanksjonering av vage og skjønnsmessige materielle regler.

Et annet hovedproblem var at den teknologiske utviklingen medførte at «register» - begrepet ikke lenger var hensiktsmessig som grunnbegrep for beskyttelse av personvernet. Personregister var definert som *«... registre, fortegnelser m.m. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte person kan finnes igjen»*. Utredningen konkluderte med at det ville være mer hensiktsmessig å regulere *enhver form for innsamling, lagring og bruk av personopplysninger*. Dette var begrunnet med at moderne teknologi ville kunne brukes til å finne opplysninger frem, uten at opplysningen på forhånd er «lagret systematisk».

Utredningen ble sendt på høring og bearbeidet videre av en Interdepartemental arbeidsgruppe, og var en del av grunnlaget for Ot.prp.nr. 34 (1986-1987) Om endringer i personregisterloven. Noen mindre endringer ble vedtatt i lov av 12. juni 1987, om endringer i personregisterloven. De mer vesentlige forslagene – om å gjøre Datatilsynet til et mer uavhengig forvaltningsorgan, droppe registerbegrepet og fokusere på innsamling, lagring og bruk av personopplysninger, å droppe konsesjonsplikten, å gi flere materielle regler osv., ble imidlertid bare i begrenset grad tatt til følge.

4.2. Overgangen til Personopplysningsloven

EU-kommisjonen la i 1992 fram utkast til direktiv om beskyttelse av personopplysninger. På denne tiden vokste digitaliseringen raskt, og behovet for en mer omfattende lovgivning som bedre kunne ivareta personvernet nasjonalt og på tvers av landegrensene, ble tydelig. Personverndirektivet ble vedtatt i 1995.[6]

Direktivet var en viktig milepæl i utviklingen av personvernlovgivning. Direktivet hadde som mål å harmonisere personvernlovene i EU, slik at personopplysninger kunne flyte fritt innen det indre markedet, samtidig som individers rett til personvern ble sikret. Det etablerte nøkkelprinsipper som regler om eksplisitt samtykke og krav om nærmere angitte behandlingsgrunnlag for lovlig behandling av data, og retten for enkeltpersoner til å få tilgang til og rette opp sine data.

På bakgrunn av direktivet, innspill fra Datatilsynet og det uttrykte behovet for endringer som er redegjort for i pkt. 3.1 over, oppnevnte Justisdepartement i oktober 1995 et utvalg for å utrede behovet for revisjon av personregisterloven. Hovedpunkter i utredningen var:

- Loven skulle ikke lenger bare gjelde for «personregistre», men også for «elektronisk behandling av personopplysninger».
- Det ble lagt større vekt på etterfølgende kontroll på grunnlag av meldinger til Datatilsynet, og konsesjonsordningen ble for en stor del avviklet til fordel for en meldeplikt til Datatilsynet.
- Det ble innført flere materielle regler i selve loven.
- De registrerte fikk flere rettigheter overfor de behandlingsansvarlige:
  - Tilrettelegging for at de registrerte skulle kunne håndheve sine rettigheter (f.eks. informasjon til de registrerte når opplysninger om vedkommende ble innhentet).
  - Nye og utvidede rettigheter for de registrerte (f. eks utvidet innsynsrett, rett til å kreve manuell behandling av automatiserte avgjørelser, og rett til å kreve begrunnelse for beslutninger truffet ved automatiserte avgjørelser).
  - Tilrettelegging for at det kan bli praktisk mulig for den enkelte å benytte seg av sine rettigheter, bl.a. ved at Datatilsynet etablerer en offentlig tilgjengelig oversikt over behandling av personopplysninger.
- Datatilsynet gjøres faglig uavhengig av regjeringen og departementene, og Justisdepartementet skal ikke lenger være klageorgan for avgjørelser i Datatilsynet.
- Det etableres en ny klageinstans – Personvernnemnda – som et frittstående og uavhengig klageorgan, der leder og nestleder ble oppnevnt av Stortinget, mens de øvrige medlemmene ble oppnevnt av Kongen.
- Det ble innført strengere regler om overvåkning, f. eks fjernsynsovervåkning mv.

Overgangen fra forhåndskontroll ved behandling av konsesjoner til etterfølgende kontroll bygget på tre hovedelementer. For det første ble det innført en plikt til å sende melding til Datatilsynet om bestemte typer behandling av personopplysninger. Meldingene skulle innføres i en offentlig tilgjengelig fortegnelse hos Datatilsynet, og skulle gi Datatilsynet informasjon som bl.a. kunne benyttes i kontrolløyemed. For det andre skulle de som behandler personopplysninger kvalitetssikre behandlingen og iverksette internkontroll som skulle dokumentere hvilken behandling av personopplysninger som fant sted, og hvorledes denne behandlingen var hjemlet og sikret på forsvarlig måte. For det tredje skulle Datatilsynet gis kompetanse til å gi pålegg om at lovstridig behandling av personopplysninger skal opphøre, eller eventuelt stille vilkår som måtte oppfylles for at behandlingen skulle være lovlig. Dersom et slikt pålegg ikke ble etterlevet, kunne Datatilsynet ilegge en tvangsmulkt som skulle løpe (akkumuleres) inntil forholdet var rettet.

Personopplysningsloven ble vedtatt 14. april 2000, med utgangspunkt i denne utredningen og Ot. Prp.nr. 92 (1998-1999) «Om lov om

6 EU-direktiv 95/46/EF

behandling av personopplysninger». Loven trådte i kraft fra 1. januar 2001, og gjaldt uten vesentlige endringer frem til den ble avløst av GDPR den 20. juni i 2018.

Personopplysningsloven fra 2000 var vesentlig bedre tilpasset for regulering av behandling av personopplysninger ved hjelp av ny teknologi enn den gamle personregisterloven.

5. Fullharmonisering av personvernlovgivningen i EU

5.1. Innføring av GDPR

Den største milepælen i moderne personvernlovgivning kom med innføringen av «General Data Protection Regulation» (GDPR) i 2018. GDPR er en forordning, som ble innført i Norge gjennom Personopplysningsloven (18. juni 2018 nr. 38). At det er en forordning, innebærer at den skal innføres i det enkelte EU-land (og EØS-land) «som den er». Det er i utgangspunktet ikke nasjonalt rom for valg om hvordan de enkelte reglene skal innføres – ut over de bestemmelsene der forordningen selv gir anvisning på at det foreligger en valgfrihet om hvordan bestemmelsen skal innføres. GDPR angir vel 50 områder der det kan fastsettes nasjonale regler ut over, eller som en presisering av de som direkte fremgår av forordningen. For Norge er disse samlet i den nye Personopplysningsloven, som iverksetter GDPR, og som er publisert sammen med GDPR[7].

GDPR har som hovedformål å beskytte enkeltpersoners rettigheter og friheter ved behandling av personopplysninger, samtidig som den sikrer fri flyt av data innen EU. GDPR gir ytterligere makt til enkeltpersoner, blant annet gjennom retten til innsyn i egne data, retten til å bli «glemt», regler om dataportabilitet, og streng formålsbegrensing for bruk av personopplysninger.

For bedrifter og offentlige organer innebærer GDPR skjerpede krav til dokumentasjon, risikovurderinger, transparens og sikkerhet. Videre har GDPR et strengt regime for overføring av personopplysninger til land utenfor EU, som ikke har en lovgivning om behandling av personopplysningen som tilfredsstiller kravene i GDPR.

GDPR innførte også et betydelig skjerpet sanksjonsnivå for overtredelser, ved at overtredelsesgebyr på det høyeste av inntil 4 % av brutto global omsetning i konsern, eller 20 millioner euro kan ilegges for de groveste overtredelsene. Dette har selvfølgelig medført betydelig økt oppmerksomhet og vilje til etterlevelse fra næringsliv og det offentlige som reglene retter seg mot.

GDPR har også ført til økte rapporteringskrav og en betydelig økning i antall avviksmeldinger. Fra 2017 til 2023 økte antall avviksmeldinger som Datatilsynet mottok med 790 prosent, en vekst som har vært utfordrende å håndtere for et tilsyn med begrensede ressurser. Mye av økningen skyldes naturlig nok den betydelige skjerpelsen av sanksjonsnivåene knyttet til overtredelse av reglene.

5.2. «Brussel-effekten»

GDPR har for Norges vedkommende den effekten at tilsynspraksis og domstolspraksis i hele EU-området får betydning for praktisering av reglene også i Norge.

GDPR har imidlertid også ringvirkninger langt ut over Europa, ved at behandling av personopplysninger som foregår utenfor Europa, langt på vei må følge Europeiske regler. Dette har blitt kalt «Brussel-effekten». Virksomheter som behandler personopplysninger om EU borgere eller som driver virksomhet i EU, må følge lovgivningen her.

Brussel-effekten er prosessen med ensidig regulatorisk globalisering forårsaket av at EU de facto (men ikke nødvendigvis de jure) eksternaliserer sine lover utenfor sine grenser gjennom markedsmekanismer. Samtidig har dette hatt den effekten at en rekke land i verden har laget egen personvernlovgivning som i mange tilfelle følger EUs eksempel.

5.3. Harmonisering av lovgivning og rettspraksis

GDPR bidrar til å harmonisere rettspraksis i Europa ved å sette felles regler og standarder som gjelder i alle EU- og EØS-land. Som en forordning må GDPR implementeres direkte i nasjonal lovgivning uten vesentlige tilpasninger, med unntak av de områdene hvor det er gitt rom for nasjonale tilpasninger. Dette sikrer at det er en ensartet tilnærming til personvern og behandling av personopplysninger på tvers av landene, noe som gir like rettigheter og plikter for både enkeltpersoner og virksomheter i hele EU. Derved gir det også like konkurranseforhold for virksomhetene. Harmoniseringen forenkler også overføringen av personopplysninger mellom landene, da de samme kravene og beskyttelsene gjelder overalt.

EU-domstolen har som hovedoppgave å tolke EU-retten for å sikre at den anvendes på samme måte i alle EU-land, og å avgjøre rettslige tvister mellom nasjonale myndigheter og EU-institusjoner. EU-domstolen er derfor en nøkkelaktør som sikrer at EU-lovgivning tolkes konsekvent og rettferdig på tvers av medlemslandene. Dette inkluderer tolkning og håndheving av GDPR. Nasjonale domstoler kan be EU-domstolen om veiledning i hvordan bestemmelser i GDPR skal forstås og anvendes. EU-domstolens avgjørelser er bindende for alle medlemslandene, noe som sikrer en ensartet forståelse og anvendelse også av personvernreglene.

Gjennom sine avgjørelser påvirker EU-domstolen direkte hvordan nasjonale domstoler og myndigheter tolker og håndhever personvernregler. For eksempel kan den klar-

7 LOV av 15.6.2018 nr. 38

gjøre hvordan bestemte rettigheter, som retten til å bli glemt, skal balanseres mot andre rettigheter, som ytringsfrihet og informasjonsfrihet. Dette bidrar til å sikre en konsistent anvendelse av reglene i hele EU.

EU-domstolen har avsagt flere viktige dommer som har bidratt til å harmonisere personvernlovgivningen i EU. For eksempel har den klargjort hvordan samtykke skal innhentes og dokumenteres, og hvordan personopplysninger skal beskyttes ved overføring til tredjeland.

6. Teknologiske utfordringer og fremtidige reguleringer

6.1. En strøm av reguleringer

Samtidig som GDPR ble forberedt og iverksatt, har det vært en stadig økende utvikling innen teknologi, med vekst i bruken av skytjenester, kunstig intelligens (AI) og store datamengder. Dette har skapt nye utfordringer for personvern. EU har jobbet med å innføre flere reguleringer for å håndtere de komplekse spørsmålene knyttet til dataøkonomien. Blant disse er Open Data Directive, Data Governance Act, Digital Markets Act, Digital Services Act, AI Act og Data Act. Dette er rettsinstrumenter som skal sikre rettferdig fordeling av verdiene i dataøkonomien, fremme bruk av åpne data, og styrke tilliten til datatransaksjoner. Flere av disse rettsinstrumentene krever at det etableres eller utpekes regulatoriske og koordinerende organer på nasjonalt plan. Det vil være viktig å samordne den innsatsen og ressursbruken som skal settes inn for å gjennomføre rettsinstrumentene på en forsvarlig og oversiktlig måte, og for å hindre en fragmentert regulatorisk oppfølging og kontroll.

En særlig utfordring gjelder for teknologisk utvikling er bruken av personopplysninger i de store språkmodellene. Spørsmålet om hvordan persondata og rettighetsbeskyttede data brukes til å trene språkmodeller og andre AI-løsninger er blitt en het debatt.

Videre har globaliseringen av teknologisektoren ført til at store amerikanske aktører, som f.eks. Amazon, Apple, Oracle og Microsoft dominerer markedet for skytjenester, noe som reiser bekymringer knyttet til overføring av data til tredjeland. Videre reiser det bekymringer for amerikansk dominans over sentrale ressurser for digitalisering og utvikling av samfunnskritiske funksjoner i EU.

6.2. Datatilsynets rolle i dagens landskap

I møte med disse utfordringene har Datatilsynet en viktig rolle. Datatilsynet står imidlertid nå som før overfor betydelige kapasitetsutfordringer. Det er et økende behov for rask og effektiv saksbehandling, samtidig som ressurser og teknisk kompetanse i tilsynet er begrenset. For å møte fremtidens krav til personvern må Datatilsynet styrkes både ressursmessig og organisatorisk. Det skal videre utpekes myndigheter for overvåkning og oppfølging av flere av de aktuelle direktivene og forordningene fra EU, og det vil være et sterkt behov for samordning og samarbeid mellom Datatilsynet og eventuelle andre organer som utpekes i henhold til nye direktiver og forordninger.

Evaluering fra DFØ (Direktoratet for forvaltning og økonomistyring) har også påpekt at tilsynet må bli en mer konstruktiv veileder for offentlige og private virksomheter, samtidig som det må utvikle bedre strategisk samarbeid med andre offentlige organer.[8]

6.3. Overregulering og behov for forenklinger

Personvern har gått fra å være et nisjeområde på 1970-tallet til å bli en sentral del av den moderne digitale økonomien. Fra innføringen av den norske personregisterloven til GDPRs strenge krav, har personvernet utviklet seg i takt med den teknologiske utviklingen – om enn noe på etterskudd. Fremover vil det være nødvendig å balansere innovasjon med personvernkrav, særlig i lys av AI, store data og skytjenester. For å sikre at personvernet fortsatt blir ivaretatt, må både lovgivning og tilsynsmyndigheter som Datatilsynet styrkes og tilpasses det digitale landskapet.

Samtidig er det etter min oppfatning helt nødvendig å avverge den nåværende trenden i retning av en overregulering av det digitale området. Slik overregulering hindrer utviklingen og legger en alvorlig demper på innovasjonskraften i næringsliv og offentlig forvaltning.

> Fremover vil det være nødvendig å balansere innovasjon med personvernkrav, særlig i lys av AI, store data og skytjenester.

Ifølge NHO er 99 % av norske bedrifter små og mellomstore bedrifter (SMB) (bedrifter med færre enn 100 ansatte), og mer enn 56 % av alle ansatte i privat sektor arbeider i SMB-bedrifter. Det er åpenbart at slike bedrifter har begrenset med ressurser til omfattende compliance-arbeid og tolkning og tilpasning til omfattende, skjønnsmessige regler som GDPR.

Internasjonalt kan man registrere en økende diskusjon om EU gjennom sin regulerings-iver er i ferd med å kvele innovasjon og utvikling, slik at EU-landene blir hengende etter i den internasjonale teknologiutviklingen og i produktivitetsutviklingen.

I de senere årene har de fleste virksomheter, inkludert amerikanske selskaper, blitt konfrontert med et økende antall krevende europeis-

8 DFØ-rapport 2024:8 Både vaktbikkje og førerhund? En evaluering av Datatilsynet

Illustrasjon: Colourbox.com

ke digitale reguleringer med omfattende ekstraterritoriale effekter. Innflytelsesrike europeiske stemmer spør om ikke dette nå ha gått for langt, og om de omfattende reguleringene ikke undergraver Europas konkurranseevne.

Mario Draghi, tidligere sjef for den europeiske sentralbanken målbar disse bekymringene i en rapport[9] i september 2024. Rapporten var bestilt av kommisjonens leder Ursula von der Leyen. Draghi hevdet at EU-kommisjonens «lovgivningsaktivitet har vokst overdrevet» de siste årene, og at «innovative selskaper som ønsker å skalere opp i Europa blir hindret på alle trinn av inkonsekvente og restriktive reguleringer.»

Ursula von der Leyen tok bl. a tak i dette i sin tale til Europaparlamentets plenarforsamling om det nye kommissærkollegiet og dets program den 27.november 2024[10], der hun bl.a. la vekt på at Europa for å kunne ta igjen innovasjonskraft, må EU gjøre ting enklere for europeiske bedrifter. Bedriftene forteller at reguleringsbyrden veier tungt på dem. Det er for mye rapportering, og for mange overlappende regelverk, som det er for komplekst og kostbart å overholde. Reglene må iflg von der Leyen effektiviseres for å redusere byrden på bedrifter. Og det må være forutsigbart for bedriftene hva som forventes av dem. På denne bakgrunn har von der Leyen bedt en av EUs mest erfarne kommissærer, Valdis Dombrovskis, om å ta ledelsen når det gjelder forenkling og implementering. Han vil også være ansvarlig for å øke Europas økonomi og produktivitet.

Ett av kommisjonens første skritt i det nye mandatet vil iflg. von der Leyen være en ny tverrsektoriell lovgivning. Kommisjonen vil se på ulike sektorer og vurdere den europeiske lovgivningen. EUs indre marked har alltid vært den største motoren for vekst. Den største styrken til det indre markedet er at det erstatter de utallige nasjonale standarder og forretningspraksis med ett enkelt sett med regler. Så EU må ifølge von der Leyen komme tilbake til det som det indre markedet gjør best: å gjøre forretninger enkelt over hele Europa.

Dette er jo lovende ord fra en av Europas mektigste byråkrater – men det gjenstår å se om det kommer konkrete forenklinger ut av dette. Jeg er noe skeptisk når første skritt i forenklingen skal være å etablere ny tverrsektoriell lovgivning!

Arve Føyen, advokat i enkeltmansfirma. Arve Føyen var engasjert som prosjektleder for implementeringen av personregisterloven og etableringen av Datatilsynet i 1979. Ved etableringen av Datatilsynet ble han ansatt som kontorsjef i Datatilsynet fra 1979–1982 under Helge Seip. I 1982 ble han engasjert av Justisdepartementet for å utrede behovet for endringer i personregisterloven. Siden1983 har han arbeidet som advokat med fokus på juridiske problemstillinger med innføring og bruk av ikt, telekommunikasjon, medier og mediedistribusjon, og personvern. Fra 2008 til 2016 var Arve Føyen nestleder i personvernnemnda, oppnevnt av Stortinget. Han arbeider fortsatt som advokat, og er engasjert som eksternt personvernombud i fire forskjellige virksomheter. Arve Føyen var den første formannen i Norsk forening for Jus & EDB da foreningen ble stiftet i 1980.

9 The future of European competitiveness – Part A | A competitiveness strategy for Europe – September 2024

10 *Speech by President von der Leyen at the European Parliament Plenary on the new College of Commissioners and its programme*

Lovgivning og digitalisering

Av Dag Wiese Schartum

Digitaliseringen av juridisk arbeid har allerede pågått i mer enn 50 år, og har blant annet grunnleggende endret måten jurister finner frem til og anvender lover. I denne artikkelen diskuterer jeg hvordan den fortsatte digitaliseringen kan virke inn på hvordan vi i fremtiden utformer og bruker lover.[1]

1 Utgangspunkt i Regjeringens digitaliseringsstrategi

Den 26. september 2024 la Regjeringen Støre frem sin Digitaliseringsstrategi, «Fremtidens digitale Norge», Digitaliseringsstrategi for 2024–2025.[2] Strategien omhandler digitaliseringen av samfunnet bredt, men har én konsekvensrik uttalelse om fremtidens lovgivningspolitikk sett i lys av digitalisering som er utgangspunktet for denne artikkelen. Det heter således at «Regjeringen vil styrke arbeidet med digitaliseringsvennlig regelverk.»[3] Regjeringen fremhever i denne sammenhengen at «vi [må] legge til rette for tverrfaglig samarbeid fra start, *slik at tjenestene og regelverket utvikles samtidig.* (uthevet her). Uttalelsen er gitt med referanse til Digitaliseringsdirektoratets digitaliseringsblogg.[4] Her blir betydningen av tverrfaglig samarbeid ved utvikling av regelverk ut-

Dag Wiese Schartum

dypet.[5] I teksten strategien viser til, fremhever Direktoratet at «jurister, teknologer, informasjonsarkitekter, designere og andre fageksperter må samarbeide, på tvers av forvaltningsnivåer, sektorgrenser og i de enkelte tverrfaglige produktteam.»

Jeg forutsetter at Digitaliseringsstrategiens angivelse av hvordan regelverk skal utvikles omfatter lovgivning. Lover er uttrykk for politiske valg som treffes på bakgrunn av ideologi, uenighet og debatt. Selv om verken Digitaliseringsstrategien eller Digitaliseringsdirektoratet nevner de politiske prosessene lovvedtak er resultatet av, er intensjonen neppe å avpolitisere lov- og forskriftsarbeidet og overlate jobben til ekspertstyre der jurister og teknologer rår grunnen. Uttalelsen må således forstås innenfor et politisk-parlamentarisk regime der ulike typer fagfolk er i dialog med og gir råd til politiske myndigheter.

Uttalelsen i Digitaliseringsstrategien innebærer at en i lovarbeider som har betydning for digitalisering ikke bare bør vurdere rent materielle spørsmål, men også spørsmål om den praktiske og tekniske gjennomføringen. En slik tilnærming er i nær slekt med den gamle diskusjonen om *administrative og økonomiske konsekvenser av lover* (jf. NOU 1973: 52).[6] Denne utredningen bygget blant annet på erkjennelsen av at ulike lovpolitiske valg vil gi ulike administrative konsekvenser når loven blir iverksatt. De antatte administrative effektene av en lov vil derfor kunne få betydning for innholdet og utformingen av loven. Sagt med andre ord: Digitalisering vil kunne få betydning for utforming av lover.

> De antatte administrative effektene av en lov vil derfor kunne få betydning for innholdet og utformingen av loven. Sagt med andre ord: Digitalisering vil kunne få betydning for utforming av lover.

2 Kravene i Utredningsinstruksen

Etter dagens Utredningsinstruks[7] stilles det en rekke krav til utredning av lover og andre tiltak, blant annet vedrørende administrative og økonomiske virkninger av lover. Forutsetningen synes å være at slike ana-

1 Artikkelen er basert på tekst fra forfatterens utgivelse *Lovgivning i et digitalt samfunn. Om å bruke lover for å fremme og temme algoritmene. Boken er publisert som CompLex 1/2025 og er gratis tilgjengelig.*

2 Digitaliseringsstrategien er tilgjengelig fra *https://www.regjeringen.no/no/aktuelt/norge-skal-bli-verdens-mest-digitaliserte-lan/id3055039/*.

3 Se avsnitt 3.1.1 i strategien.

4 Se *https://www.digdir.no/sammenhengende-tjenester/samarbeid-ikke-stafett/3071*.

5 Digitaliseringsdirektoratet er også opptatt av utvikling av tjenester på samme måte, men her begrenser jeg meg til regelverk.

6 NOUen gav i sin tid grunnlag for Regelverksinstruksen, som senere er blitt avløst av Utredningsinstruksen.

7 *Gjeldende instruks* ble fremmet av Finansdepartementet, og er fastsatt ved kongelig resolusjon 18. oktober 2024 med hjemmel i instruksjonsmyndigheten.

lyser bør være knyttet til de seks spørsmålene som offentlige utredninger alltid skal gi svar på:[8]

1. Hva er problemet, og hva vil vi oppnå?
2. Hvilke tiltak er relevante?
3. Hvilke prinsipielle spørsmål reiser tiltakene?
4. Hva er de positive og negative virkningene av tiltakene, hvor varige er de, og hvem blir berørt?
5. Hvilket tiltak anbefales, og hvorfor?
6. Hva er forutsetningene for en vellykket gjennomføring?

Utredningen skal være så omfattende og grundig som nødvendig.[9] Hvor grundig avhenger blant annet av de forventede virkningene av loven. Sentralt i utredninger er valg av tiltak (jf. særlig spørsmålene 2–5, ovenfor). I utgangspunktet kan en rekke virkemidler være aktuelle som tiltak. Instruksen nevner spesielt regulering (herunder lovgivning),[10] økonomiske, pedagogiske og organisatoriske virkemidler, offentlige tilbud av produkter og tjenester, og offentlige anskaffelser. Utredningsinstruksen nevner ikke tekniske tiltak som en egen virkemiddeltype. «Tekniske løsninger» blir bare nevnt som én av flere forutsetninger for vellykket gjennomføring av tiltak.[11] Tiltak i form av *digitalisering* nevnes overraskende nok ikke.

I Utredningsinstruksen blir det understreket at det kan være hensiktsmessig å bruke *kombinasjoner* av virkemidler.[12] Uttalelsene i Regjeringens digitaliseringsstrategi om parallell, tverrfaglig lov- og tjenesteutvikling handler nettopp om å kombinere ulike typer virkemidler; særlig kombinasjon av lovgivning og digitale løsninger. Skal en for eksempel satse på en lov som i stor grad lar seg automatisere, eller bør en gi rom for skjønnsutøvelse og individuell behandling med digitale løsninger som beslutningsstøtte?

Her kommer jeg ikke detaljert inn på i hvilken grad Utredningsinstruksen er egnet som støtte for den politikken nevnte uttalelse i Digitaliseringsstrategien er uttrykk for. Jeg nøyer meg med å fastslå at det synes å være en vesentlig mangel ved Utredningsinstruksen fordi digitalisering ikke blir fremhevet som egen virkemiddeltype. Dette er i klar kontrast til forutsetningene for Digitaliseringsstrategiens uttalelse om parallell, tverrfaglig lov- og tjenesteutvikling.

Utredningsinstruksen er ikke eneste førende dokument med relevans for spørsmålet om forholdet mellom lov- og tjenesteutvikling. Instruksen viser blant annet til *Lovteknikkheftet*. Denne veilederen er ikke oppdatert siden 2000 og forholder seg overhodet ikke til digitalisering. Den kan derfor neppe sies å legge til rette for virkeliggjøring av den delen av Digitaliseringsstrategien jeg her diskuterer. Derimot gjelder Digitaliseringsdirektoratets «*Veileder digitaliseringsvennlig regelverk*» nettopp de spørsmålene strategien aktualiserer. Veilederen innebærer imidlertid ikke i seg selv noen bindende krav til departementer som utarbeider lovforslag. Veilederen viser til Utredningsinstruksen, Lovteknikkheftet og Språkrådets veileder om «*Godt språk i regelverket*». Ingen av de aktuelle dokumentene inneholder forklaringer av sammenhengene mellom de ulike instruksene og veilederne på området.[13]

Det er altså fire dokumenter som er klart relevante for problemstillinger om forholdet mellom digital lov- og tjenesteutvikling, men ingen av dokumentene avklarer den samlede situasjonen. Det er bare Veileder om digitaliseringsvennlig regelverk som behandler spørsmålene på konkret og direkte måte, men dette dokumentet er kun rent veiledende og neppe et tilstrekkelig effektivt virkemiddel for å virkeliggjøre Regjeringens strategi om integrert digital lov- og tjenesteutvikling.

3 Aktiv lovgivningspolitikk vedrørende digitalisering

I Digitaliseringsrundskrivet gir Regjeringen årlig oppdaterte prioriteringer for statens arbeid med digitalisering. I rundskrivet for 2024, heter det blant annet i avsnitt 1.1[14] at:

> *«Relevant regelverk må gjennomgås. […] Det skal ikke lages nye regelverkshindringer, og eksisterende, utilsiktede hindringer skal fjernes. Det enkelte departement er ansvarlig for å gjennomføre de regelverksendringene som er nødvendige for å kunne oppnå gevinster ved digitalisering på eget område, eller bidra til utviklingen av sammenhengende tjenester på tvers av sektorer og forvaltningsnivåer.»*[15]

Den første del av sitatet om regelverkshindringer [for digitalisering], kan ikke tas bokstavelig: Lover og forskrifter vil nettopp ofte ha som formål å legge «hindringer», i betydningen krav til utvikling og bruk av digitale hjelpemidler. Kravene utformes gjerne som påbud, og en sjelden gang som forbud. Ikke sjelden vil imidlertid påbudene være så krevende å etterleve at de hindrer planlagt utforming og bruk av datasystemer. Personvernregelverket og KI-forordningen er sentrale eksempler på «ønskede hindre». Slik sett er

8 Se Utredningsinstruksen, avsnitt 2.1.

9 Se Utredningsinstruksen punkt 2.2. Instruksen opererer med tre trinn: Minimumsanalyser, forenklede analyser og samfunnsøkonomiske analyser.

10 Kapittel 4 i Utredningsinstruksen stiller særskilte krav til lovutredninger, men disse kommer jeg ikke spesielt inn på her.

11 Se Veileder til Utredningsinstruksen, s. 32.

12 Se Veileder til Utredningsinstruksen, s. 26.

13 En gjør også oppmerksom på manglende oppdatering av Lovteknikkheftet og Utredningsinstruksen.

14 Som handler om brukere og tjenesteutvikling.

15 Digitaliseringsrundskrivet 2024, Rundskriv, 09.02.2024

presiseringen senere i sitatet om fjerning av *utilsiktede* hindringer, mer til poenget. Ingen vil uansett forsvare vedtakelse av nye lover med utilsiktede hindringer for digitalisering. Uttalelsen i Digitaliseringsrundskrivet bør trolig leses som en anmodning til forvaltningen om å delta i regelverksarbeid på en måte som vier spørsmål med betydning for digitalisering spesiell oppmerksomhet, slik at det ikke vedtas nye påbud og forbud fordi en mangler oppmerksomhet om hvilke virkninger disse vil ha.

Generelt bør rundskrivet trolig leses som en beskjed til statsforvaltningen om å drive *aktiv lovgivningspolitikk* innen det digitale feltet. Regelverksendringer «som er nødvendige for å kunne oppnå gevinster ved digitalisering» kan sies å handle om å fjerne uønskede hindre, men kan også handle om å gi bestemmelser i lov og forskrift som reduserer rettslig usikkerhet knyttet til digitalisering, og som legger til rette for ønsket og forsvarlig bruk av datasystemer.

Aktiv lovgivningspolitikk vedrørende digitalisering, krever etter min mening større innsats og mer kontinuitet knyttet til dette aspektet ved lovgivningsarbeider. Regjeringen bør selvsagt ikke oversvømme Stortinget med små og hyppige lovsaker. Likevel bør det demokratisk-politiske styringsapparatet mer aktivt påvirke hvordan datasystemer skal brukes og ikke brukes.

Vi er i ferd med å få et gjennomdigitalisert samfunn. Styring av teknologi og teknologibruk kan derfor vanskelig skilles fra samfunnsstyring ellers. Digitaliseringsprosesser og bruk av datasystemer er derfor viktige temaer som politiske myndigheter verken kan eller bør vise tilbakeholdenhet med å styre.

Når det er viktig bør vi fortsatt bruke lovgivning for å gi påbud og forbud. I NOU 2022: 11 uttalte Personvernkommisjonen for eksempel at en nasjonal personvernpolitikk for skole- og barnehagesektoren burde inneholde tiltak for «å støtte norske virksomheter som utvikler løsninger som bygger opp under prinsippene i den nasjonale utdanningspolitikken og barns grunnleggende rettigheter …».[16] Dersom Personvernkommisjonens generelle uttalelse skulle bli omformet til konkret politikk, kunne skolelovgivningen f.eks. fastsette at det i norske skoler skal brukes digitale læremidler som ikke innebærer kommersiell utnyttelse av opplysninger om elever og lærere. I så fall ville lovgiver påbudt eksistensen av datasystemer med visse kjennetegn, men uten å fastsette detaljert hvordan kravet skal oppfylles.

Like viktig som påbud er å bruke lovgivning for å legge til rette for ønsket og hensiktsmessig teknologibruk. Dette kan skje ved bruk av insentiver, for eksempel innen skatte- og avgiftslovgivningen. En aktiv lovgivningspolitikk må dessuten ta sikte på kontinuerlig å avklare rettslig usikkerhet, særlig når dette er viktig for å fremme ønskede digitale reformer og investeringer. Lovgiver kan f.eks. konkret undersøke hva som oppleves som rettslig usikkert om digitalisering innen et bestemt livsområde, og på det grunnlaget vedta lovendringer som avklarer rettsspørsmålene og reduserer rettslig risiko.

4 Digitalt lovpolitisk observatorium

I en demokratisk rettsstat bør forventningen som nevnt være at lovgiver styrer digital teknologi på aktiv måte. Styringen må være basert på god og oppdatert kunnskap om den teknologiske utviklingen, herunder muligheter og mulige uønskede implikasjoner. Dette krever at lovgiver har kontinuerlig oppmerksomhet på spørsmål som gjelder datateknologi. Det er neppe mulig å arbeide tilstrekkelig innsiktsfullt og raskt med lovgivning innenfor det digitale feltet, dersom de ansvarlige departementene ikke har kompetanse eller mangler interesse for spørsmål som gjelder datateknologi og digitalisering innenfor deres ansvarsområde.

Et vesentlig bidrag til å unngå at lovarbeider ikke skal ta for lang tid, kan være at departementene er beredte og komfortable med å gå løs på utredningsoppgaver som har med datateknologi å gjøre. Dette krever en grunnbemanning av folk med kunnskaper om hvordan teknologi virker inn på aktuelle livsområder. Dermed kan en unngå at arbeid med lovgivningsspørsmål knyttet til digital teknologi er noe en skrur på og av, og i stedet er noe som blir gjenstand for *kontinuerlig* og mer eller mindre intens oppmerksomhet og innsats.

Det svenske IT-rättsliga observatoriet er eksempel på organisering av lovarbeid som kan bidra til rask respons på teknologisk endring. Observatoriet var et rådgivende organ for den svenske regjeringen i perioden 1994 til 2004. Oppgaven var å gjøre en samlet kartlegging av alle rettslige spørsmål som IT-utviklingen aktualiserte, både problemer og muligheter.[17] Observatoriet skulle «verka genom ett spekulativt, framtidsorienterat övervägande av rättsliga nykonstruktioner». Slik skulle de supplere diskusjoner av gjeldende rett og diskusjoner om behov for rettslig endring, med en *spekulerende og prøvende analyse* av behov for å regulere. Lignende analyser av lovgivningsmessige aspekter ved frembrytende teknologier og nye anvendelser av teknologi, vil kunne redusere norske lovgiveres responstid når behov for lovendring blir tydelig nok. Et viktig grunnlag for slike «spekulative» diskusjoner, vil måtte være kontinuerlig oppdatert kunnskap om viktige diskusjoner internasjonalt om teknologi og reguleringsbehov.

16 Se avsnitt 8.5 i NOUen.

17 Se «Det IT-rättsliga observatoriet», tekst fra IT-propositionen (1995/96: 125), gjengitt på nettside under IT-kommisjonenen.

5 Regulatorisk innovasjon

På lignende måte som det kontinuerlig skjer utvikling av teknologiske produkter, bør lovgivning vedrørende digital teknologi være en løpende prosess der nye versjoner og «modeller» av lover blir utviklet etter hvert som lovgiver vinner innsikt i hvordan behovet for regulering utvikler seg, og hvordan effektene av eksisterende regulering er. Teknologisk innovasjon vil med andre ord ofte kreve *regulatorisk innovasjon*, det vil si at det kan være ønskelig eller til og med nødvendig å utvikle nye og bedre lovgivningsteknikker for å kunne lovgi på tilstrekkelig måte. Utvikling av personvernlovgivning kan tjene som eksempel.

Da Sverige forberedte verdens første nasjonale personvernlov (Datalagen 1973), var det stor usikkerhet om hva som ville være hensiktsmessig reguleringsmåte. Lovgiver uttalte at datalagen var et foreløpig tiltak, og at det ikke var usannsynlig at lovgivningen ville bli utformet på mer detaljert måte.[18] Siden 1973 har Europa sett minst tre lovmodeller for regulering av personvern (se straks nedenfor), og innen hver modell har det vært en rekke versjoner som resultat av mer begrensede lovendringer.

Regulatorisk innovasjon forutsetter ikke nødvendigvis utvikling av nye typer lovgivning. Innovasjon kan også bestå av nye *kombinasjoner* av kjente lovgivningsteknikker. I tilfellet Datalagen 1973 prøvet en seg frem med lovregulering basert på konsesjoner til å etablere personregistre, med kun et lite antall bestemmelser for slike registre i selve loven. I stedet forutsatte loven at detaljerte regler skulle bli gitt av Datainspektionen for det enkelte register. Den norske personregisterloven (1978) og flere andre tidlige personvernlover fulgte samme strategi. Etter hvert ble konsesjonsordningen imidlertid gradvis redusert og til slutt avskaffet. I stedet stilte lovgiver opp en rekke konkrete regler for lovlig behandling av personopplysninger i selve loven. Dessuten ble det lagt til nye regulatoriske elementer; særlig krav til internkontroll og selvregulering, kombinert med avskrekkende høye gebyrer for overtredelse av bestemmelsene.

I dag fremstår ikke lovgivningen om personvern som spesielt innovativ. Dersom vi ser etter innovative *elementer* i dagens regulering, er det imidlertid enkelte elementer som kan trekkes frem. Et eksempel er kravene til innbygging i teknologien av rettsprinsipper og konkrete lovbestemmelser (*by design*).[19] Et annet aktuelt eksempel på regulatorisk innovasjon, er «regulatoriske sandkasser», dvs. ordninger der myndigheter tilbyr et sikkert miljø for utvikling og testing av nye og innovative teknologier som er i tråd med lovgivningen.[20] På den måten kan teknologimiljøer lære noe om hva som kan være lovgivningsmessige utfordringer knyttet til teknologien som testes ut. Myndigheten kan på sin side påvirke teknologiutviklingen i retning av løsninger som klart kan anses som rettslig akseptable. Myndigheten kan også fange opp trekk ved teknologiutviklingen som kan gi grunn til videre regulatoriske initiativ.

Et tredje og siste eksempel på det som i dag kan sies å være innovativ lovregulering, er bestemmelsene i artikkel 80 i personvernforordningen som gir visse ideelle organisasjoner og sammenslutninger rett til å tre inn i registrerte personers sted og utøve rettigheter på deres vegne, på grunnlag av samtykke fra de registrerte. Samme artikkel åpner også for at medlemslandene kan tillate ideelle organisasjoner og opptre uten samtykke fra registrerte personer, dvs. på eget initiativ og som selvstendig aktør. Det innovative her er ikke fullmaktsforholdet i seg selv, men det at en aktivt trekker ideelle organisasjoner inn i gjennomføringen av lovgivningen.

Det er selvsagt ikke mulig å bare bestemme seg for at lovgivning skal være innovativ – innovasjon avhenger mer av evne enn av vilje. På den annen side er det mulig å legge til rette for prosesser som skal stimulere til nytenkning om hvordan lovgivning om digital teknologi kan eller bør være.

6 Forsøkslovgivning

I 2021 etablerte Datatilsynet en «regulatorisk sandkasse» for kunstig intelligens. Målet var å stimulere til innovasjon og utvikling av etiske og ansvarlige KI-løsninger. Prosjekter som får plass i sandkassen, får gjennomdiskutert sine løsninger og hjelp til å følge personvernregelverket. En lignende ordning med «AI regulatory sandboxes» er del av EUs KI-forordning, se artikkel 57–61. Slike sandkasser tilbyr kontrollerte miljøer for å legge til rette for utvikling, testing og validering av KI-systemer. Disse åpner imidlertid bare for forsøksvirksomhet innenfor de angitte områdene. Jeg tror det kan være grunn til å vurdere et *nasjonalt* lovgrunnlag for en *generell* forsøksvirksomhet innen det digitale feltet.

Innen offentlig forvaltning gjelder lov om forsøk i offentlig for-

18 Se Peter Seipel, Legal Controls of the Storage and Use of Personal Data. An Appraisal of the Swedish Approach, i Hafli 1977, En komparativ studie av datalover, Institutt for Privatrett, Avdeling for edb-spørsmål, Universitetet i Oslo, Skriftserien for jus og edb, Oslo 1977, s. 54.

19 Regulatoriske elementer av denne typen utviklet seg med utgangspunkt i diskusjoner om Privacy Enhancing Technologies på 1990-tallet, og ble introdusert i personvernforordningen artikkel 25 i 2016.

20 Artiklene 57–59 i KI-forordningen inneholder regler om slike sandkasser for kunstig intelligens. I Norge har Datatilsynet hatt en regulatorisk sandkasse for kunstig intelligens og personvern med basis i personopplysningsloven.

valtning (forsøksloven).[21] Loven gjør det mulig for statlig, fylkeskommunal og kommunal forvaltning å søke Kongen om forsøk med sikte på å forbedre virksomheten, spesielt offentlig tjenesteyting, ressursutnyttelse og demokratiske styringsformer.[22] Loven åpner blant annet for forsøk der det godkjennes avvik fra gjeldende lover og forskrifter om hvordan staten, fylkeskommunene eller kommunene skal organisere sin virksomhet og løse sine oppgaver.[23] Det kan ikke gis unntak for bestemmelser i forvaltningsloven, andre rettssikkerhetsbestemmelser og personvernforordningen.[24] Godkjennelser er normalt begrenset til inntil 4 år ad gangen. Det er stilt krav til å utarbeide nærmere regler for gjennomføringen,[25] men det er ikke stilt krav i loven om evaluering og rapportering av forsøket.

Digitalisering av offentlig forvaltning vil lett kunne skape behov for avvik fra regler om hvordan offentlige myndigheter skal organisere sin virksomhet og løse sine oppgaver. I ett perspektiv har deler av digitaliseringen preg av å være forsøksvirksomhet. Årsaken er blant annet at forvaltningen bruker teknologi for å endre arbeidsmåter og for eksempel grunnleggende endrer relasjonen mellom kunder og næringsdrivende, eventuelt mellom myndigheter og innbyggere. For eksempel ønsker en å utvikle løsninger som i stor grad er selvbetjente.

Jeg mener lovgiver bør vurdere om det er hensiktsmessig å utvide eller supplere forsøksloven, ved å gi lovhjemmel for forsøk som innebærer innovativ digitalisering. En revidert forsøkslov bør ikke være strengt begrenset til offentlig forvaltning, men bør for eksempel åpne for forsøk som vedrører relasjonen mellom offentlig og privat sektor. Forsøksvirksomheten bør heller ikke bare være knyttet til en bestemt type digital teknologi (jf. sandkassene for KI), men bør også omfatte konvensjonelle, regelbaserte løsninger.

Alle vesentlige aspekter ved forsøksvirksomhet bør være gjenstand for vurdering, ikke bare spørsmål om personvern.[26] Blant annet bør spørsmål om effektivitet; hensynet til personer som ikke eller i begrenset grad kan gjøre bruk av digitale systemer; annen diskriminering; og virkninger for offentlighet og rettssikkerhet, vurderes som ledd i forsøksvirksomheten. En revidert forsøkslov bør dessuten stille krav til metode og grundighet av vurderingene i forsøket, og det bør stilles krav til rapportering og tilrettelegging for offentlig diskusjon.

En revidert forsøkslov som tydelig innbefatter digitalisering, vil kunne gi innovative løsninger som er lovlige eller som gir resultater som viser at de *bør være* lovlige. Slik kan forsøksvirksomheten stimulere til digitalisering som er utprøvet og funnet forsvarlig.

7 Lovutviklingsverktøy og KI-genererte lover

Det er viktig med digitale hjelpemidler som gir støtte til anvendelse av lovgivningen. Imidlertid er det også grunn til å gå *til kilden* ved å bruke digital teknologi til å bedre kvaliteten av lovgivningen. Målet med *lovgivningsverktøy* må være å unngå at lovgiver etterlater seg inkonsistenser og uklarheter som gir unødvendige tolkningsproblemer. Et videre mål bør være at lovgiver i større grad kan tydeliggjøre intenderte sammenhenger mellom lover; både «vertikalt» (f.eks. mellom forordninger og norsk, nasjonal lovgivning, og mellom lover og forskrifter), og «horisontalt» (mellom lover innen ulike, tilknyttede rettsområder).

Lovgivningsverktøy kan primært gi *beslutningsstøtte*. Formålet bør altså være å understøtte manuelle, kognitive prosesser, herunder samarbeid mellom personer som deltar i lovarbeid. Da brukes teknologien for at mennesker skal prestere bedre, ikke for å automatisere lovgivningsprosessen.

Lovutviklingsverktøy basert på konvensjonell teknologi har vært diskutert i 20 år eller mer.[27] I dag er det også mulig å tenke seg at maskinlæring kan brukes til automatisk å foreslå lovbestemmelser, basert på gjeldende lover og forskrifter mv. Dette vil trolig være praktisk for visse typer bestemmelser vi har mange av i vår lovgivning, for eksempel bestemmelser om geografisk virkeområde, taushetsplikt, innsynsrett mv. Resultatet vil da bli forslag til lovbestemmelser som låner struktur og innhold fra eksisterende bestemmelser av samme eller lignende type. Dersom lovgiver f.eks. ønsker å legaldefinere begrepet «motorvei», kan en maskinlæringsrutine tenkes å foreslå definisjoner av begrepet på grunnlag av annen lovgivning og andre relevante kilder. Slike forslag vil selvsagt kreve vurdering og videre bearbeiding av mennesker, og vil således kun saksforberedende funksjon.

Daniel Lovric ser også for seg at KI-systemer kan bli satt til å stille lovgivere spørsmål om et saksområde som skal være gjenstand for regulering. På basis av svarene kan systemet så gi et røft forslag til lovtekst som lovutviklere kan arbeide

21 Lov av 26. juni 1992 nr. 87.
22 Se §§ 1 og 2.
23 Jf. § 3 første ledd bokstav a.
24 Jf. § 4 og personopplysningsloven § 2 fjerde ledd.
25 Se § 5 første ledd.
26 Jf. artikkel 35 i personvernforordningen om vurdering av personvernkonsekvenser (DPIA).
27 Se f.eks. Dag Wiese Schartum, IT-støtte for arbeid med lovsaker, CompLex 4/08, Senter for rettsinformatikk 2008 og Ed Hicks, Implementing Legislation Systems – Considerations and Options, paper for CALC 2011, Hydrabad, India, 2011-02-11.

videre med.[28] Et vesentlig poeng ved en slik anvendelse vil være at KI-systemet kan brukes til å identifisere hensyn og interessekonflikter mv., f.eks. basert på analyse av politiske dokumenter, nyhetsoppslag og annet relevant materiale.

Beslutningsstøtte anvendt i lovarbeider kan også tenkes gjennomført ved å sette maskinen til å estimere om et lovforslag kan sies å være i samsvar med bestemte *politiske og rettslige prinsipper*, for eksempel vedrørende kontradiksjon, klarspråk, forsvarlig saksutredning mv. Det er tenkelig å bruke maskinlæringsmodeller for å analysere og gi indikasjoner på i hvilken grad lovgivningen, generelt eller innenfor et gitt domene, er i samsvar med slike bestemte prinsipper eller ikke. Grunnlaget for denne typen analyser kan blant annet være domsavgjørelser, autorative uttalelser i fra internasjonale politiske organer og akademisk litteratur.

En ytterligere mulighet er å bruke lovutviklingsverktøy til å analysere og karakterisere gjeldende lovgivning som ledd i interessekamp og krav om lovendring, utenfor og parallelt med den formelle lovgivningsprosessen. Verktøy basert på maskinlæring er særpreget ved at slike systemer kan gi ulike resultater, avhengig av den underliggende modellen, datagrunnlaget og hvordan systemet videreutvikler modellen basert på dataene. Ulike spørsmålsformuleringer og oppfølgingsspørsmål til svar som systemet gir, vil derfor kunne gi ytterligere resultater og videre innsikt. På basis av svar fra systemet kan brukeren dessuten gå ned i primærdata systemet har anvendt og gjøre videre analyser – både manuelle og automatiserte. Det er derfor neppe slik at denne type verktøy nødvendigvis vil ensrette og innskrenke meningsutveksling og meningsdannelse. Likevel kan ulik tilgang til verktøyene, og manglende kritisk bruk av dem, gi slike negative effekter.

I helt spesielle tilfeller er det mulig å tenke seg *automatisert lovgivning*, dvs. at maskiner programmeres til å treffe *politiske avgjørelser*. Peter Wahlgren bruker automatisk endring av fartsgrenser ved endrede kjøreforhold, og betalingssatser på bomveier som eksempel på at automatisk endrede regler ikke er en helt fremmed tanke i et moderne samfunn.[29] En kunne f.eks. også tenke seg en «politisk regel» i et lovutviklingsverktøy som sier at dersom konsumprisindeksen, i henhold til visse parametere, endrer seg over en viss grense, skal grunnbeløpet i Folketrygden («G») endres forholdsmessig gjennom et automatisk lovvedtak. Slike automatiske lovvedtak måtte imidlertid være basert på et ordinært lovvedtak, og ville måtte være en «forlengelse» av et ordinært lovvedtak. En slik ordning kan kanskje ses som «delegasjon» fra lovgiver til et maskinelt system om å utføre regelendringer innenfor visse, snevre, politisk angitte rammer.

For å ta stilling til om og hvordan IT-verktøy eventuelt kan brukes i lovutviklingsprosesser, trenger vi å forstå disse prosessene på sammenhengende og detaljert måte. Jo mer vi nedfeller slike forståelser i IT-verktøy, jo mer vil verktøyet legge til rette for eller kreve at bestemte fremgangsmåter og metoder blir fulgt. Slike verktøy vil derfor ikke bare handle om praktiske tilrettelegging, men også ha *normerende* og styrende effekter. Dersom verktøyet f. eks. har funksjoner for å gjøre enkle dataanalyser og -modellering, kan dette øke sannsynligheten for at lovgiver legger til rette for gjenbruk av opplysninger. Lovgivningsverktøy vil derfor ikke være nøytrale, og bør utformes med bevissthet om mulig innvirkning på politiske og faglige vurderinger.

8 Automatiseringsvennlig lovgivning

I en klassisk artikkel fra 1977 om «Automatiseringsvennlig lovgivning» stiller Jon Bing spørsmålet om «Hvilke krav [man kan] eller bør stille til lover, forskrifter mv. som skal legges til grunn for et datamaskinassistert forvaltningssystem?» Spørsmålet er med andre ord hvordan lover bør være for å legge til rette for automatisert bruk? Bing refererte bl.a. til den tyske forfatteren Herbert Fiedler. Fiedler drøftet slike spørsmål allerede tidlig i 1970-årene, og omtalte de første arbeidene med å gjøre lovgivning «computer-conscious» i Vest-Tyskland mot slutten av 1950-årene.[30] Spørsmålet om lovgiver bør tilpasse loven til den etterfølgende digitale implementeringen av rettsreglene, er altså en gammel; trolig nesten like gammel som de første anvendelser av datamaskiner i offentlig forvaltning.

Kort sagt er en lov automatiseringsvennlig når den er lett å programmere, dvs. når loven lar seg fortolke som et sett av operasjoner som datamaskiner kan utføre, og de opplysninger en trenger for å anvende loven på konkrete saker foreligger som maskinlesbare data. Spørsmålet om en lov er automatiseringsvennlig eller ikke, har ikke ja eller nei som eneste mulige svar. Det dreier seg snarere om et kontinuum fra lover som overhodet ikke lar seg uttrykke ved hjelp av pro-

28 Se Daniel Lovric, The Future of Legislative Drafting: a Strategic Approach, paper for CIAJ Legislative Drafting Conference, 8–9 September 2022, Ottawa, s. 6.

29 Se Peter Wahlgren, From Lex Scripta to Law 4.0. On Legislation of the Future, Scandinavian studies in law, no. 65, 2018, s. 164.

30 Se Fiedler 1973 s. 8. Dette handlet om helt enkle tilpasninger. Beløp i skattelovgivningen ble endret slik at de var delelige på 12. Dermed ble det lettere å beregne beløp per måned.

grammeringsspråk, til lover som lett lar seg programmere.[31]

Et digitalt samfunn forutsetter ikke lovgivning som lar seg automatisere. Spørsmålet om lovgivningen skal være automatiseringsvennlig eller ikke, og i hvilken grad, avhenger av politisk prioriteringer og valg. Motivet for å gjøre det enkelt å automatisere anvendelsen av lover, er ofte de store effektiviseringsgevinster en kan oppnå ved å erstatte mennesker med maskiner ved behandling av mange, likeartede enkeltsaker. I stedet for å gjøre mennesker i enkeltsaksbehandling overflødig, kan et alternativt politisk valg imidlertid være å bruke digitale hjelpemidler for å forbedre menneskers innsats, for eksempel finne og analysere rettskilder og opplysninger om relevante faktiske forhold mv. Regjeringen Støres digitaliseringsstrategi og målsettingen om at Norge i 2030 skal være verdens mest digitaliserte land,[32] innebærer altså ikke nødvendigvis at Norge skal få verdens mest automatiserte rettsliv. Digitalisering kan i stedet handle om å gi bedre støtte til alle personer som trenger å forholde seg til, forstå og anvende lovgivningen.

Selv om automatiseringsvennlig lovgivning er mulig innen rettsområder med behov for standardisert massesaksbehandling, er det åpenbart en rekke lovområder der slik lovgivning ikke er formålstjenlig eller mulig. For det første kan de politiske prosessene som leder frem til lovvedtak gjøre det ytterst vanskelig å oppnå resultater som er automatiseringsvennlige. Dette gjelder særlig når prosessene forutsetter kompromisser for å oppnå enighet,

Illustrasjon: Colourbox.com

noe som blant annet er typisk for tilblivelsen av lovgivning i EU. En annen viktig årsak er at en rekke lover regulerer individuelle forhold med unikt innhold der det mangler informasjonsgrunnlag og behandlingsmåter som kan standardiseres og programmeres. En tredje årsak er at mye lovgivning forutsetter direkte og konkret interaksjon mellom mennesker. Derfor kan for eksempel avtaleloven vanskelig gjøres automatiseringsvennlig.

9 Lover sett som spesifikasjoner av informasjonssystemer

Ikke sjelden kan lover ses som implisitte spesifikasjoner av datasystemer. Loven fastsetter for eksempel hvilken informasjon som må behandles, og gir regler om hvordan informasjonsbehandlingen skal skje. Implisitt angir loven derfor hvilken funksjonalitet og hvilke kvaliteter de digitale hjelpemidlene som brukes for å sette loven ut i livet bør ha.

En kan spørre seg om ikke lovarbeidet bør være en *eksplisitt* bestilling av den programvaren som er nødvendig for å gjennomføre loven på forsvarlig måte. Ikke sjelden trer lover først i kraft når nødvendige forskrifter foreligger. På lignende måte kan en tenke seg at ikrafttredelse avhenger av at lov og forskrift også er implementert i rettslige beslutningssystemer som offentlige myndigheter utvikler for å automatisere anvendelsen av loven.

Argumentet om at det bør foreligge et egnet datasystem som understøtter riktig etterlevelse av loven, er også gyldig i et innbyggerperspektiv. Det er mulig å se loven som spesifikasjon av datasystemer som enkeltpersoner og næringsliv skal kunne benytte for å etterleve loven på forsvarlig måte. Lovgiver kan således velge å iverksette loven til en tid det er mulig for programvareleverandører å utvikle adekvate systemløsninger. Slik kan lovgivningspolitikk og næringslivspolitikk knyttes sammen ved at lovgivning i større grad blir grunnlag for produkter fra progamvareutviklere.

Ovenfor nevnte datasystemer kunne tilbys på kommersiell basis eller som et forsterket uttrykk for offentlighetsprinsippet.[33] Like selvfølgelig som at *lovtekster* er offentlige tilgjengelige,[34] bør det være at *datasystemer for etterlevelse av loven* er offentlig tilgjengelige, jf.

31 Rules as Code kan stå som representant for lett programmerbare regler (jf. «*Better rules» initiativet hos regjeringen i New Zeeland*). I ytterste fall innebærer denne tilnærmingen at en programmerer rettsreglene som del av lovforberedelsen, slik at det blir helt klart hvordan loven faktisk skal forstås.

32 Digitaliseringsstrategien, avsnitt 1.

33 Jf. Grunnloven § 100 femte ledd.

34 Jf. publicatio legis prinsippet.

«systemoffentlighet».[35] En slik styrking av innbyggernes mulighet til å etterleve loven, bør i utgangspunktet være basert på et rettssikkerhetskrav om datasystemer med *likeverdig funksjonalitet*. Særlig er det viktig at den automatiserte rettsanvendelsen i systemløsninger innbyggerne tilbys har likeverdig kvalitet med systemløsninger offentlig forvaltning anvender. Dersom myndighetene har systemer for automatisert anvendelse av loven, bør innbyggerne ha likeverdige muligheter. Da kan de for eksempel simulere mulige effekter for deres rettsstilling av eksisterende lovgivning.[36] Noe annet kan hevdes å gi et problematisk skjevt styrkeforhold.

10 Tiden det tar

Den tid det tar fra et lovarbeid begynner til det foreligger datasystemer som understøtter etterlevelse av loven, blir lett uforholdsmessig lang. Ikke minst tar det lang tid dersom loven først må vedtas før forskriftsarbeidet kan ta til, og systemutviklingen først begynner når loven med forskrifter er vedtatt. Ikke sjelden fremheves det at lovgivningsprosessen er for tidkrevende og treg i et digitalt samfunn som er merket av hurtig omstilling. Også systemutvikling er imidlertid arbeidskrevende og langvarige prosesser. Problemet er derfor *den samlet tid* det tar fra lovinitiativ til operative systemløsninger.

Etter min mening er tidsaspektet så kritisk for effektiv etterlevelse av lover at en bør vurdere å etablere en lovgivningsmodell som integrerer lovutvikling og tilknyttet systemutvikling. Muligheten er altså å la lov- og forskriftsutvikling og systemutvikling skje i parallell. På den måten kan arbeidet med selve regelverket nyte godt av de analyser som skjer som ledd i utviklingen av datasystemer som skal understøtte loven. Da kan politiske myndigheter få større innsikt i de tekniske, praktiske og økonomiske følgene av lovbestemmelser de ønsker å foreslå. Slik kan det også bli klart om og i hvilken grad anvendelsen av rettsreglene de foreslår kan automatiseres, herunder om det finnes tilgjengelige data som kan brukes i automatiserte rutiner. Dessuten kan lovgiver være den som reelt sett bestemmer hvor automatisert anvendelsen av lovgivningen skal være (ikke systemutviklere som finner mer eller mindre oppfinnsomme måter å automatisere på etter at en lite automatiseringsvennlig lov er vedtatt).

11 Avslutning

Lovgivning er en viktig del av demokratiet. Endrer vi måten vi utformer og bruker lover på, endrer vi også et av de mest sentrale styringsmidlene samfunnet rår over. I kontrast til Regjeringens målsetting om at Norge skal være verdens mest digitaliserte land i 2030, mener jeg det ikke kan være noen målsetting at Norge om fem år skal ha verdens mest digitaliserte lovgivningsprosess. Digitalisering kan ikke være mål i seg selv, men kan være et middel for å oppnå bedre lovgivning og styrke demokratiet og rettsstaten.

Det er ikke én oppskrift vi må følge dersom vi ønsker å digitalisere lovstaten. Muligheter for digitalt baserte endringsprosesser er mange. Vi må velge og forme digitale rutiner både ut ifra hensyn til tradisjon og fornyelse. Skal vi gjøre det, trenger vi diskusjon om muligheter og veivalg. Jeg håper at jeg med denne artikkelen, og det bakenforliggende arbeidet om *Lovgivning i et digitalt samfunn*, kan bidra til uenighet og debatt!

Dag Wiese Schartum, Senter for rettsinformatikk, UiO.

35 Se Dag Wiese Schartum, Systemrettssikkerhet, i Rättsinformation under 2000-talet: nuläge i Sverige och Europa, trender och policy: delbetänkande / av IT-kommissionen. SOU 2001: 71 - Stockholm: Fritzes, 2001. Stockholm, s. 60–73.

36 Noen forskjeller i funksjoner knyttet til sikkerhet og kontroll med forsettlige lovbrudd vil trolig være nødvendig.

Schjødt

Halvor Manshaus

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

Ny EU-dom åpner døren på vidt gap for gruppesøksmål

1. Innledning

Sammenlignet med andre jurisdiksjoner har EU relativt strenge regler knyttet opp mot personvern og databeskyttelse, der personvernet har fått en fremtredende plass. Utgangspunktet er at personopplysninger fritt kan overføres internt innen EU/EØS-området, mens det som hovedregel er forbudt å overføre slike opplysninger ut av dette området. Dette kan innebære åpenbare utfordringer for den som ønsker å overføre personopplysninger ut av EU. EU-kommisjonen kan imidlertid gi en form for godkjenning av spesifiserte mottakerland utenfor området gjennom såkalte adekvansbeslutninger[1]. I praksis innebærer dette både generell godkjenning av overføring til alle virksomheter i enkelte land (som Sveits, Storbritannia, mv.) samt spesifikk godkjenning av konkrete områder og sektorer i andre land (slik som virksomheter som er underlagt den kanadiske personvernlovgivningen for privat sektor, virksomheter i USA som er ført opp på en egen liste over godkjente enheter er unntatt fra forbudet, mv.). Det kan altså overføres personopplysninger fra EU/EØS-området til godkjente virksomheter i mottakerlandet som om det var en virksomhet innenfor EU/EØS. Slike godkjente virksomheter i mottakerlandet må følge EU-kravene knyttet til behandling av personopplysninger.

Gjennom avgjørelsene i Schrems I (C-362/14, avsagt 6. oktober 2015) og II (C-311/18, avsagt 16. juli 2020) har EU-domstolen gjort det klart at overføring av personopplysninger til USA krever tilstrekkelige sikkerhetsmekanismer. Domstolen slo fast at beskyttelsesnivået for personopplysninger i denne jurisdiksjonen var utilstrekkelig. Konsekvensen av dette var at det ikke forelå grunnlag for å gi unntak under adekvansbeslutning for overføring av personopplysninger til USA. Tidligere adekvansbeslutninger for USA ble kjent ugyldige. Schrems II medførte store utfordringer for virksomheter innen EU/EØS som hadde behov for å overføre personopplysninger til USA. Etterfølgende forhandlinger mellom EU-kommisjonen og USA førte etter hvert til at USA måtte styrke personvernet og skjerpe reglene for håndtering av personopplysninger. Blant annet skal slike opplysninger nå behandles i tråd med et nytt regelverk (EU-U.S Data Privacy Framework), samtidig som det skal tilbys uavhengige og gratis klageorganer. På denne bakgrunn ble ny adekvansbeslutning for USA fattet av EU-kommisjonen den 10. juli 2023.[2]

En nylig avsagt dom fra EUs General Court i sak T-354/22 *Bindl v. EU-kommisjonen* belyser problemene som kan oppstå når personopplysninger overføres til et mottakerland utenfor EU/EØS. Saken gir viktige avklaringer om overføring av data, institusjoners ansvar og individers rettigheter. En privatperson hadde i denne saken utfordret selve *EU-kommisjonens* behandling av hans personopplysninger. Den aktuelle overføringen fant riktignok sted i perioden etter Schrems II og før adekvansbeslutningen 10. juli 2023, der det altså ikke forelå noe gyldig adekvansgrunnlag for USA. Avgjørelsen er likevel relevant også etter den siste adekvansbeslutningen som har vært omdiskutert siden den ble fattet. Personverngruppen NOYB har dessuten nylig påpekt at Trump-administrasjonen allerede har gjennomført tiltak som svekker beskyttelsesnivået i USA og uthuler forutsetningene for adekvansbeslutningen. Det er ikke utenkelig at også denne

1 Se oversikt på Datatilsynets nettside: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/omrader-med-tilstrekkelig-beskyttelsesniva/

2 https://noyb.eu/en/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal

beslutningen vil kunne bli kjent ugyldig.

2. Bindl-saken

Saken ble anlagt av en tysk statsborger, Thomas Bindl, som flere ganger i perioden 2021 og 2022 besøkte nettsiden til Conference on the Future of Europe (CFE). Under et slikt besøk 30. mars 2022 registrerte Bindl seg på CFE-nettsiden og til en konferanse kalt «GoGreen» via sin Facebook-konto.

EU-kommisjonen ved generaldirektoratet for kommunikasjon var behandlingsansvarlig for personopplysninger som ble behandlet i forbindelse med denne nettsiden. Bindl tok kontakt med EU-kommisjonen og hevdet at Amazon Web Services var blitt aktivert i bakgrunnen da han skulle logge seg på CFE-nettsiden. Han ba om å få opplyst hva slags personopplysninger tilknyttet ham som var blitt overført og hvilket rettslig grunnlag som forelå for en overføring til Amazon, som er et foretak registrert i USA.

EU-kommisjonen svarte på henvendelsen og oversendte samtidig en elektronisk lenke som genererte en oversikt over alle personopplysninger tilknyttet Bindl som var blitt behandlet i forbindelse med besøkene på det aktuelle nettstedet. Det ble samtidig opplyst at det ikke hadde skjedd noen overføring til land utenfor EU/EØS, og at hans opplysninger ble behandlet og lagret av CFE-nettsiden. Denne siste funksjonen ble håndtert av et Amazon-selskap registrert i Luxembourg (Amazon Web Services EMEA SARL). Det ble presisert i svaret at det var inngått en kontrakt med dette europeiske datterselskapet som presiserte at det ikke skulle skje overføringer til andre selskaper i Amazon-gruppen i USA, og at overføringer ut av EU/EØS-området ikke var tillatt.

Bindl fulgte opp med ytterligere spørsmål. Han viste til at en tilkobling til Microsoft hadde skjedd da han brukte sin Facebook-konto for å registrere seg på CFE-nettsiden. Han ba videre om oversikt over alle personopplysninger delt med tredjeparter, herunder Facebook, samt rettslig grunnlag for all deling og overføring av personopplysninger. Deretter ble saken etter noen purringer fra Bindl fremmet av ham som en klagesak til EU-domstolen. Bindl krevde annullering av selve dataoverføringene, fastsettelsesdom for at EU-kommisjonen ikke hadde fulgt opp forespørselen om innsyn og € 1 200 i erstatning for ikke-materiell skade, fordelt på € 800 for brudd på hans rett til informasjon og € 400 som kompensasjon for ulovlig overføring av personopplysninger. Det er verdt å merke seg at kravet ikke var forankret i GDPR (forordning (EU) 2016/679), men hovedsakelig i forordning (EU) 2018/1725[3] som gjelder EU-institusjoners behandling av personopplysninger. Forordningene er på sentrale områder sammenfallende, og det står i fortalepunkt 5 i forordning (EU) 2018/1725 at EU-domstolen skal tolke forordningen homogent med GDPR så langt det passer. Det innebærer også at rettspraksis under forordning (EU) 2018/1725 er relevant for virksomheter underlagt GDPR.

Retten la til grunn at de to første kravene måtte avvises, men valgte å behandle deler av kravet om erstatning.

Kravet om annullering av dataoverføringer gjaldt tre konkrete overføringer. Den første overføringen fant sted 30. mars 2022, hvor Bindl hevdet at det skjedde en overføring til Amazon Cloud Front. Den andre overføringen skal ha skjedd da Bindl registrerte seg via sin Facebook konto som omtalt ovenfor, og der personopplysninger skal ha blitt overført til Meta Platforms Inc. Den tredje overføringen skal ha skjedd 8. juni 2022, da opplysninger etter et besøk til CFE-nettsiden medførte at personopplysninger ble overført til Amazon CloudFront server i Newark, USA. Kravet om annullering ble avvist ettersom overføringene ikke utgjorde en «bindende juridisk handling» som kunne utfordres i henhold til artikkel 263 TEUF. Domstolen slo i avsnitt 33 i avgjørelsen fast at dette var tekniske dataoverføringer som ikke hadde direkte rettslige konsekvenser:

> *«In the present case, assuming that the transfers at issue are established, it must be noted that they are physical, not legal, acts. The transfers at issue, as described in the application, are IT operations migrating data from one terminal or server to another that result from interactions between the applicant and the Commission's IT systems or services on his visits to the CFE website or the EU Login service. However, the transfers at issue are not acts of the Commission that have binding legal effects, that is to say, they are not intended to regulate a legal situation and, as is apparent from their very nature, the Commission did not have any intention of conferring such effects on them.»*

Med dette som utgangspunkt konkluderte retten med at overføringene ikke hadde noen slik rettslig virkning at disse kunne medføre noen endring i hans rettslige status eller posisjon. Retten viste her til tidligere avgjørelser i blant annet sakene C-351/15 og C-911-19 som allerede har slått fast dette prinsippet.

Når det gjaldt kravet om fastsettelsesdom for manglende oppfølgning fra EU-kommisjonen, ble det

3 Full tittel: «Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC»

vist til at EU-kommisjonen hadde fulgt opp forespørselen etter at kravet var blitt fremmet for retten. Det hadde ingen betydning at innholdet i EU-kommisjonens svar ikke samsvarte med Bindls posisjon. Retten uttaler om dette i avsnitt 42:

> *«The fact that the position adopted by the institution has not satisfied the applicant is of no relevance in this respect because Article 265 TFEU refers to failure to act in the sense of failure to take a decision or to define a position, not the adoption of a measure different from that desired or considered necessary by the applicant...[.]»*

Det gjenværende spørsmålet ble dermed om det forelå grunnlag for kravet om erstatning.

Artikkel 65 i forordning (EU) 2018/1725 slår fast at enkeltpersoner som lider materiell eller ikke-materiell skade på grunn av et brudd på forordningen har rett til erstatning fra det aktuelle EU-organet. Retten viser i avsnitt 48 og 49 til tre kumulative vilkår som må være oppfylt for å konstatere ansvar utenfor kontrakt i denne situasjonen: Et tilstrekkelig alvorlig brudd på EU-retten, faktisk og sikker skade samt direkte årsakssammenheng mellom regelbruddet og skaden. Et tilstrekkelig alvorlig brudd oppstår når en EU-institusjon åpenbart og grovt overskrider sin kompetanse. Kravet til at skaden må være faktisk og sikker, innebærer at hypotetisk eller ubestemt skade ikke er tilstrekkelig for erstatning. Kravet til årsakssammenhengen innebærer i praksis at institusjonens handlinger er den direkte og avgjørende årsaken til skaden.

Retten drøftet først kravet på € 800 som var basert på at EU-kommisjonen ikke svarte på Bindls henvendelse i tide og at det angivelig ble gitt feil opplysninger om overføringene. Anførselen fra Bindl var at dette gjorde det umulig for ham å utøve noen kontroll over egne personopplysninger, som forårsaket en ikke-materiell skade.

Retten anerkjente at EU-kommisjonen opptrådte i strid med artikkel 14(4) i forordning (EU) 2018/1725 ved å overstige svarfristen på én måned med omtrent to måneder. Imidlertid konkluderte retten med at Bindl ikke hadde bevist faktisk og sikker ikke-materiell skade. Han hadde allerede mottatt et delvis svar på en tidligere, vesentlig lik forespørsel i desember 2021. Dette reduserte den faktiske virkningen av forsinkelsen. Ettersom klageren ikke klarte å bevise skade som direkte følge av forsinkelsen, var det allerede her klart at samtlige tre vilkår for erstatning ikke var til stede. Retten avviste følgelig denne delen av erstatningskravet.

Det neste spørsmålet var kravet på € 400 for ikke-materiell skade forårsaket av overføringen av personopplysninger til USA ved tre separate anledninger som beskrevet ovenfor. Kravet var bygget på at overføringen til USA var forbudt og manglet rettslig hjemmel. Retten går her gjennom en rekke punkter der begreper knyttet til overføring av personopplysninger klargjøres, og viser i avsnitt 99–100 til at USA ikke lenger var omfattet av noen gyldig adekvansbeslutning:

> *«In that regard, it should be noted that both of the Commission's adequacy decisions concerning the United States have been declared invalid […] It follows that, at the time of the transfers at issue, no adequacy decision, within the meaning of Article 47 of Regulation 2018/1725, existed with regard to the United States.»*

Fraværet av en adekvansbeslutning for USA på det aktuelle tidspunktet etter Schrems II-dommen plasserte derfor ytterligere samsvarsbyrder på EU-kommisjonen som den behandlingsansvarlige. Dette innebærer tekniske og organisatoriske tiltak for å beskytte dataoverføringer, inkludert overføringer som ble utført under standard kontraktklausuler. Det er verdt å merke seg hvor grundig domstolen her går til verks, spesielt ved gjennomgangen av kontrakten som regulerer håndtering av data mellom CFE-nettstedet og Amazon. Det som kommer frem gjennom denne drøftelsen er at avtalen med Amazon viser at en rekke ulike lokasjoner benyttes til håndtering av personopplysninger fra nettstedet. Enkelte av disse er gjennom selskaper eid av Amazon, mens enkelte lokasjoner driftes av tredjeparter som underleverandører. Dette oppsummeres i avsnitt 116:

> *«In the sixth place, as regards the infrastructure of Amazon CloudFront's edge locations network, it is apparent from the case file that this is provided by a number of undertakings, some of which belong to the Amazon group while others are third companies, the list of which can be viewed on Amazon Web Services' website, according to the geographic area concerned. In the case of the geographic area 'North America (United States, Mexico, Canada), Europe and Israel', the relevant undertakings are established in the EU Member States as well as outside the European Union, in particular in the United States, Israel, Mexico, Switzerland or the United Kingdom. Each undertaking uses servers in the country in which it is established and, consequently, the geographic location of the servers involved in the delivery of the Amazon CloudFront service also depends on the location of the undertakings concerned.»*

Etter å ha slått fast hvordan den tekniske overføringen av personopplysninger var lagt opp, drøftes de tre ulike datoene der overføringene skal ha skjedd. Det er et poeng å merke seg at opplysningene som overføres ikke kan karakteriseres som spesielt sensitive. Det skal ha vært snakk om Bindls IP-adresse, samt standard opplysninger som nettstedet henter fra nettleseren og brukerens datamaskin. Likevel går altså domstolen

meget grundig gjennom alle leddene i denne operasjonen.

Når det gjaldt overføringen som skjedde 30. mars 2022 konkluderer domstolen med at de aktuelle opplysningene ble overført fra CFE-nettstedet via Amazon CloudFront til en server i München, Tyskland. Denne serveren var del av nettverket som omtalt i avsnitt 116 sitert ovenfor. Det var altså klart at det ikke forelå noen overføring ut av EU/EØS-området. Spørsmålet var da om Bindls anførsel om at dette likevel var krenkende kunne føre frem. Det ble hevdet at eierselskapet Amazon vil måtte følge opp utleveringspålegg fra myndigheter i USA, også for informasjon som ligger tilgjengelig på selskapets nettverk i Europa – herunder serverparken i München. Det var ikke godtgjort at noen slik utlevering hadde funnet sted, slik at domstolen måtte vurdere om den teoretiske muligheten i seg selv var tilstrekkelig grunnlag. Anførselen førte ikke frem, og domstolen konstaterer i avsnitt 135 at muligheten for at et land utenfor EU krever eller får tilgang til personopplysningene ikke i seg selv er tilstrekkelig til å konstatere brudd på regelverket.

> *«As it is,* ***the mere risk of access*** *to personal data by a third country* ***cannot amount to a transfer of data****, within the meaning of Article 46 of Regulation 2018/1725, as interpreted in paragraph 93 above, since it has not been demonstrated that the applicant's personal data were transmitted or otherwise made available to a recipient established in a third country. In other words,* ***the risk of an infringement of Article 46 cannot be treated as being akin to a direct infringement of that provision.****» (min utheving)*

Den neste overføringen, som fant sted 8. juni 2022 innebar derimot en overføring av Bindls personopplysninger til USA. På dette tidspunktet var Bindl selv i München, og besøkte CFE-nettsiden en rekke ganger. Disse besøkene ble ikke håndtert av en enkelt Amazon CloudFront server. Bindls IP-adresse ble registrert på flere Amazon-servere rundt om i Europa og USA. Den store geografiske spredningen gjorde det klart at Bindl ikke var fysisk tilstede i disse områdene, men hele tiden befant seg fysisk i München.

07:13 München, Tyskland
11.13 London, Storbritannia
12:56 Hillsboro, USA
13:05 Newark, USA
19.12 Frankfurt am Main, Tyskland

CFE-nettsiden hadde denne dagen 4548 sidevisninger fordelt på 18 ulike IP-adresser. Retten kommenterer ikke misforholdet mellom antall unike sidevisninger og IP-adresser, men påpeker at det kun var IP-adressen til Bindl som koblet seg opp mot servere utenfor EU. Normalt fungerer denne typen servere etter et såkalt proximity-prinsipp der brukeren dirigeres til nærmeste server. I praksis beregnes dette basert på en beregning av forventet treghet i selve overføringshastigheten gjennom nettverket (latency). Det var på det rene at det ikke var noen tekniske problemer med nettsiden eller serverne som skulle medføre at IP-adressen til Bindl dukket opp hos de ulike serverne. Det kan fremstå som om Bindl har benyttet en VPN-tjeneste, som i praksis vil innebære at brukeren får tilordnet en IP fra en lokal server med en annen geografisk plassering enn der brukeren fysisk befinner seg. Dette blir imidlertid en spekulasjon, og domstolen nøyer i avsnitt 157 seg med å konstatere at Bindl ser ut til å ha manipulert sitt digitale fotavtrykk og at dette medførte overføringen av IP-adressen til USA:

> *«Accordingly, the connections that were established from the applicant's IP address to servers located in the United States, when he was in Germany, cannot be attributable to the normal operation of the Amazon CloudFront service; rather, they were attributable to a technical adjustment made by the applicant to change his apparent location, by presenting himself in the digital sphere as though he were, on the same day, in various places near Munich, London, Hillsboro, Newark and Frankfurt am Main, one after the other.»*

Overføringen skjedde altså ikke som en konsekvens av noen feil eller unnlatelse fra EU-kommisjonens side, men skyldtes Bindls egen handling som var den direkte og umiddelbare årsaken. Det forelå dermed ikke tilstrekkelig årsakssammenheng med overføringen av personopplysningen, Bindls IP-adresse til server utenfor EU/EØS. Vilkåret om årsakssammenheng var dermed ikke oppfylt, og denne delen av erstatningskravet ble altså ikke tatt til følge.

Til slutt så domstolen på den siste overføringen, som fant sted 30. mars 2022. Det var da Bindl registrerte seg på «GoGreen»-konferansen. Han ble formidlet fra CFE-nettsiden videre til EU-login, en nettside som håndterte selve registreringen av Bindl. EU-login åpner for at brukere blant annet kan registrere seg ved bruk av eksisterende kontoer på ulike sosiale plattformer. Bindl valgte altså å registrere seg via Facebook, og han hevdet at dette medførte at hans IP-adresse samtidig ble overført til Facebook og eierselskapet Meta i USA. Selv om han kun hadde akseptert «nødvendige» cookies, mente Bindl at hans epostadresse, profilbilde, samt for- og etternavn var blitt overført til Meta-servere i USA. EU-kommisjonen viste på sin side til at EU-login ga flere muligheter for å registrere seg, slik at brukeren selv kunne velge fremgangsmåte. Det ble også fremhevet at de aktuelle personopplysningene aldri ble samlet inn av EU-kommisjonen, som da heller

ikke kunne anses å stå for selve overføringen.

Domstolen gjorde igjen en detaljert gjennomgang av faktum. Blant annet ble de underliggende tekniske datatransaksjonene mellom tjenestefunksjonene for registrering gjenstand for en grundig analyse. Deretter vises det til at det rent faktisk har skjedd en overføring av personopplysninger til USA uten et adekvansgrunnlag, og derfra er veien kort til å konstatere ansvarsgrunnlaget i form av et tilstrekkelig alvorlig brudd på EU-retten. Som det fremgår av avsnitt 191 legger domstolen vekt på at EU-kommisjonen ikke har implementert noen mekanismer for å sikre håndtering av personopplysninger på riktig måte.

> *«In the present case, the Commission has neither demonstrated nor claimed that there was an appropriate safeguard, in particular a standard data protection clause or contractual clause adopted in accordance with the conditions laid down in Article 48(2) and (3) of Regulation 2018/1725 (see paragraphs 102 to 104 above). By contrast, it has been demonstrated that the displaying of the 'Sign in with Facebook' hyperlink on the EU Login website is entirely governed by the general terms and conditions of the Facebook platform [].»*

EU-kommisjonen hadde altså selv skapt omstendighetene som medførte at overføringen fant sted, uten at det forelå noen sikkerhetsforanstaltninger eller adekvansbeslutning. Det neste skrittet ble deretter å se om kravene til skade og årsakssammenheng var oppfylt for den aktuelle overføringen til USA. Her legger domstolen til grunn en lav terskel for konstatering av skade, og uttaler at begrepet omfatter *«[n]ot only 'material damage' but also 'non-material damage' suffered as a result of an infringement of that regulation gives rise to a right to compensation, without any reference being made to any threshold of seriousness…»*. I dette tilfellet fant

Halvor Manshaus v/AI Midjourney.

domstolen det tilstrekkelig at Bindl som en følge av overføringen hadde mistet kontroll over sine personopplysninger, samt at hans rettigheter var krenket. Det forelå etter dette en direkte årsakssammenheng mellom overføringen og den påførte skaden.

På dette grunnlaget fant domstolen altså at EU-kommisjonen var ansvarlig for overføringen som fant sted 30. mars 2022 og tilkjente Bindl € 400 i erstatning, samt halvparten av kravet for sakskostnader. Bindl hadde tapt saken på de to første kravene, og bare vunnet frem med ett av de tre anførte grunnlagene for erstatning.

Avgjørelsen i T-354/22 *Bindl v. EU-kommisjonen* markerer en viktig utvikling innen personvernretten i EU. Den understreker at EU-institusjoner må ta ansvar for eventuelle dataoverføringer og at individer kan kreve erstatning for ikke-materiell skade. Denne saken er så langt jeg har kunnet bringe på det rene det

> I dette tilfellet var beløpet beskjedent, men automatisert behandling og overføring av personopplysninger vil kunne innebære at et stort antall enkeltpersoner rammes – og vil ha krav på erstatning.

første eksempelet på erstatning for overføring av personopplysninger til et land utenfor EU/EØS som ikke er forhåndsgodkjent og uten at det foreligger tilstrekkelig overføringsgrunnlag. I dette tilfellet var beløpet beskjedent, men automatisert behandling og overføring av personopplysninger vil kunne innebære at et stort antall enkeltpersoner rammes – og vil ha krav på erstatning. I jurisdiksjoner som åpner for gruppesøksmål vil slike krav

kunne kumuleres og få store konsekvenser for den ansvarlige. I Norge har vi regler for dette i tvistelovens kapittel 35 om gruppesøksmål.

Dommen reiser også spørsmål om hvordan Kommisjonen og andre institusjoner vil tilpasse sine praksiser i lys av de strenge kravene til personvern. Det er verdt å presisere at dommen ikke direkte tar stilling til bruken av Amazon CloudFront og distribusjonen av servere som lå i denne løsningen, men utelukkende vurderer EU-kommisjonens ansvar utenfor kontrakt. Dette fremgår uttrykkelig av avsnitt 144:

> *«[i]n the context of the present claim for damages, the Court is not directly examining the lawfulness of the Commission's decision to use the Amazon CloudFront service for the distribution of CFE website content; rather, it is verifying the conditions for establishing the Commission's non-contractual liability with regard to the disputed transfer at the time of the visits to the CFE website on 8 June 2022.»*

Avgjørelsen sender et tydelig signal om at ingen er unntatt fra EUs strenge personvernregler, selv ikke EU-institusjonene selv. Reglene her gjelder også offentlige virksomheter og ideelle organisasjoner, uten at det er åpenbart at disse lever opp til de strenge kravene som legges til grunn her. Bruken av tredjepartstjenester for å verifisere epostadresse eller identitet ved registrering og pålogging er allerede godt utbredt inne EU/EØS.

Et annet aspekt ved denne saken er at rettspraksis innenfor EU-retten på mange fronter ser ut til å bli drevet fremover av enkeltpersoner som ønsker å prøve utvalgte spørsmål for retten. I dette tilfellet synes det klart at Bindl fremprovoserer det aktuelle tapet av kontroll over IP-adressen sin. Vi ser her at det også legges til grunn en ekstremt lav terskel for hva som kan utgjøre skade i forordningens forstand. Dersom en person er *«in a position of some uncertainty as regards the processing of his personal data, in particular of his IP address»*, så er dette altså tilstrekkelig til å utløse et krav på erstatning. I dette tilfellet ble det sendt informasjon til Facebook/Meta som inneholdt for- og etternavn, profilbilde og epostadresse. Jeg mener det er grunn til å stille spørsmål ved om dette i realiteten er en overføring i lovens forstand, og spesielt ved måten det har skjedd på i dette tilfellet. Årsaken til at tredjeparten Facebook benyttes ved denne type registrering er normalt for å verifisere brukerens epostadresse. Det må legges til grunn at Facebook allerede satt inne med alle brukeropplysningene, og at formålet altså var å sjekke at denne brukeren – med den aktuelle IP-adressen, er den samme som tidligere registrert hos Facebook. Det er altså koblingen mellom IP-adresse og brukerens registrerte informasjon som er poenget, og selve overføringen har mer en karakter av å bekrefte eksisterende opplysninger enn å overføre ny informasjon. Dette innebærer også at det i realiteten er snakk om et meget begrenset «kontrolltap». Vi vet at IP-adresse generelt sett er ansett som en personopplysning, men kanskje settes terskelen i laveste laget i dette tilfellet. Domstolen bekrefter for øvrig status i EU-retten per i dag at selv dynamiske IP-adresser utgjør personopplysninger: *«Even 'dynamic' IP addresses – which by nature change over time – correspond to a precise identity at a given point in time, which, in this case, coincides with the point in time at which the visit to the CFE website took place»*. I Bindl-saken hadde brukeren tilsynelatende bevisst forsøkt å fremkalle overføringer utenfor EU, som fremgår blant annet fra hendelsesforløpet 8. juni 2022. En konkret vurdering av hele hendelsesforløpet og klagene til Bindl vitner samtidig om at han fortløpende logget og utøvde en sterk grad av kontroll over nettopp hvor og hvordan hans opplysninger ble behandlet og overført. Dette virker vanskelig å forene med erstatning for at han skal ha mistet kontroll over egen IP-adresse. Det er i alle fall klart at kombinasjonen av en lav terskel for hva som utgjør en relevant overføring av personopplysning og kravet til skade på nivået *«[s]ome uncertainty as regards the processing of his personal data…»* vil kunne åpne opp for en rekke gruppesøksmål som omtalt ovenfor.

Dommen er altså avsagt av General Court, og kan således ankes til neste instans. Det er grunn til å ønske en slik anke velkommen, og at vi i neste instans fikk en tilnærming som i større grad hensyntar at denne type «minimums-skade» ikke nødvendigvis bør utløse et umiddelbart krav på erstatning. I rettens vektlegging av skade, kunne det også være naturlig å se hen til hvorvidt saksøker selv har fremkalt situasjonen hvor det oppstår «kontrolltap» over sine personopplysninger – og i hvilken grad det skal tillegges noen vekt.

Halvor Manshaus, leder IP/Mediagruppen i Advokatfirmaet Schjødt AS, Oslo og fast spaltist i Lov & Data.

CompLex 1/25 – Lovgivning i et digitalt samfunn

Om å bruke lover for å fremme og temme algoritmene

Forfatter: Dag Wiese Schartum

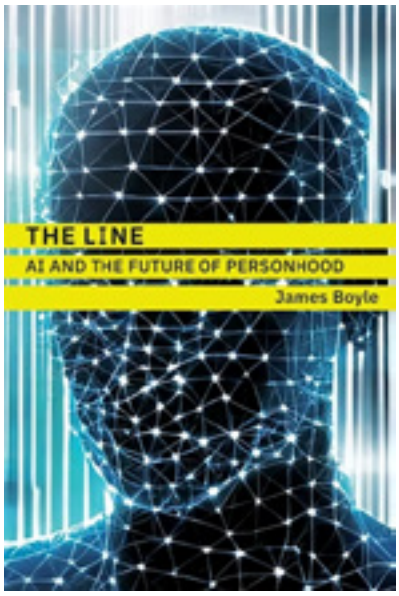
Oslo: Universitetet i Oslo, Juridisk fakultet, Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk 2025, 1/2025. ISSN 2703-8777 Complex (online)

Denne boken inneholder en rekke analyser og anbefalinger i møtet mellom lovgivning og datasystemer. Formålet er å legge til rette for bedre lovstyring av det digitale samfunnet

Les hele utgivelsen på CompLex1/25 (pdf)

The Line

AI and the Future of Personhood



By James Boyle
ISBN: 9780262049160
Pub date: October 22, 2024
Publisher: The MIT Press

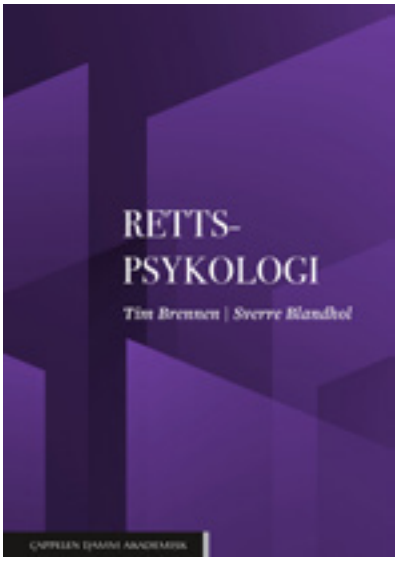
How AI will challenge our ideas about personhood.

Chatbots like ChatGPT have challenged human exceptionalism: we are no longer the only beings capable of generating language and ideas fluently. But is ChatGPT conscious? Or is it merely engaging in sophisticated mimicry? And what happens in the future if the claims to consciousness are more credible? In *The Line*, James Boyle explores what these changes might do to our concept of personhood, to "the line" we believe separates our species from the rest of the world but that also separates "persons" with legal rights from objects.

The personhood wars—over the rights of corporations and animals, over the question of when life begins and ends—have always been contentious. We've even denied the personhood of members of our own species. How will those old fights affect the new ones, and vice versa? Boyle pursues these questions across a dizzying array of fields. He discusses moral philosophy and science fiction, transgenic species, nonhuman animals, the surprising history of corporate personality, and AI itself. Engaging with empathy and anthropomorphism, courtroom battles on behalf of chimps, and doom-laden projections about the threat of AI, *The Line* offers fascinating and thoughtful answers to questions about our future that will arrive sooner than we think.

The book description is from MIT Press: https://mitpress.mit.edu/9780262049160/the-line/

Rettspsykologi



Tim Brennen og Sverre Blandhol
Oslo: Cappelen Damm Akademisk 2025, 414 s. Heftet, Bokmål
ISBN: 9788202774356

Rettspsykologi er en bok for alle som jobber med rett og rettspleie og ønsker kunnskap om hva psykologisk forskning kan fortelle om hvordan denne rettspleien foregår. I boken behandles blant annet temaer som

- forholdet mellom troverdighet, pålitelighet og korrekthet
- hukommelsens grunnleggende trekk og hukommelsessyndene
- falske minner og myten om fortrengning
- løgndeteksjon og den resultatløse jakten på metoder for å avsløre løgn
- suggestibilitet og falske tilståelser
- avhørsmetoder med innsikt fra sosialpsykologi og kognitiv psykologi
- juridisk tenkemåte slik den faktisk foregår
- bekreftelsesskjevhet i forberedelse med og gjennomføring av saker
- fortellinger og bevisbedømmelse
- betydningen av dommernes følelser
- forankring ved utmåling av straff og erstatning

I denne boken beskrives grunnleggende psykologiske temaer som persepsjon og oppmerksomhet, hukommelsesrelaterte problemstillinger, løgndeteksjon, hvordan avhør og vitnekonfrontasjoner bør gjennomføres og hvordan dommere og andre jurister kommer frem til sine standpunkter og noen av de viktigste feilkildene i den anledning.

Omtalen er hentet fra Cappelen Damm: Rettspsykologi av Tim Brennen - Juridiske fag | Cappelen Damm Utdanning

---

LEGORA

Leya, den ledende AI-plattformen for advokater blir, Legora – Lanserer Agentic Research og nye produktoppdateringer

Leya, den ledende AI-plattformen for advokater, har lansert sin nye merkevare og navn, Legora. Selskapet har samtidig gitt ut store produktoppdateringer som vil styrke produktivitet og effektivitet for alle plattformens brukere. De nye oppdateringene inkluderer markedsledende verktøy for agentic research. I tillegg lanseres en ny utvidelse for Microsoft Word, fanebasert analyseverktøy for store dokumenter, og forbedringer for samarbeid rundt informasjonsinnhenting og arbeidsutførelse.

Legora ble grunnlagt i 2023 og ledes av CEO og tidligere deltaker i Y Combinator, Max Junestrand. Legora, som på latinsk betyr «å føre

ting sammen» er en AI-drevet plattform som skaper sømløst samarbeid mellom advokater og kunstig intelligens. Plattformen er i bruk i mer enn 15 land av over 200 selskaper.

«Legoras nye merkevare og produktforbedringer er en milepæl i vår utvikling og viser ikke bare hvor mye vi har vokst, men også vår forpliktelse til å levere det første virkelig AI-drevne samarbeidsverktøyet for advokater,» sier Junestrand. «Når vi nå går inn i vår neste fase er vi dedikert til innovasjon i samarbeid med våre kunder, for å bruke kunstig intelligens til å gi advokater et fortrinn i et stadig mer konkurransedrevet marked.»

Legoras AI-verktøy gjør at advokater kan jobbe raskere og mer presist i alle oppgaver, som frigjør tid til å fokusere på de mest kompliserte oppgavene og viktig strategiarbeid. Med den nye merkevaren kommer tre nye funksjoner som integreres sømløst i Legoras plattform og styrker effektiviteten ved å gi advokatfirmaer muligheten til å samarbeide som et lag når de gjennomgår, produserer og leverer tjenester i samtid. Produktoppdateringene inkluderer:

- **Ny søkeagent**: En avansert agent for informasjonsinnhenting. Agenten formulerer smarte søk samtidig som den beholder så mye av det opprinnelige spørsmålet som mulig.
- **Microsoftutvidelse**: Brukere kan stille spørsmål om innhold i et dokument, anvende brukermanualer i Word og til og med be Legora gjøre endringer basert på kommentarer og endringsforslag. Alt integrert som en utvidelse i Microsoft Word.
- **Forbedret samarbeid**: Brukere av Legora kan nå arbiede sømløst sammen på prosjekter og enkeltdokumenter med fanebasert analyse. Legora integrerer med kundens eksisterende teknologi og prosjektstruktur.

Legora har hentet mer enn $35 million er fra investorer som Benchmark, Redpoint, SV Angel, Y Combinator med flere. *WIRED* kåret Legora til en av Stockholms heteste startups i 2024.

«Som et moderne advokatfirma må vi ligge i forkant når det gjelder AI-utvikling. Vi har lansert et strategisk AI-initativ på Lindahl som kommer til å forandre måten vi jobber på. Det er virkelig inspirerende å tenke på unge advoktater som begynner hos oss og hvordan de kommer til å mestre disse systemene for å hjelpe våre klienter på et høyere nivå enn noen gang tidligere,» sier Monica Lagercrantz, managing partner i Lindahl.

Av Max Junestrand, CEO, Legora

Om Legora

Legora (tidligere Leya) er den første virkelig kollaborative AI-plattformen for advokater. Med kontorer i Stockholm og London styrker Legora eksepsjonelle advokater ved å la dem bruke hele sin ekspertise. Plattformen er i bruk i mer enn 15 land og av over 200 kunder. wLegora samarbeider med sine kunder for å forbedre effektivitet, presisjon, og gi mer tid til å løse kompliserte problemer og viktig strategisk arbeid.

Gorrissen Federspiel

Tue Goldschmieding

Nyt om persondataret i Danmark

Utilsigtede modtagere omfattet af indsigtsretten

Det danske datatilsyn (»Datatilsynet«) har den 26. september 2024 truffet afgørelse i to sager under journalnummeret 2023-32-0023 vedrørende den registreredes indsigtsret.

Sagerne udsprang af et brud på persondatasikkerheden hos Skattestyrelsen, hvor der ved en fejl i forbindelse med en aktindsigtsanmodning var videregivet en række personoplysninger til ansøgeren om aktindsigt. To berørte borgere fremsatte herefter anmodning om indsigt i identiteten af den pågældende der havde fået utilsigtet adgang, hvilket dog blev afvist af Udviklings- og Forenklingsstyrelsen.

Efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) art. 15, stk. 1, har en registreret ret til at modtage bekræftelse på, om personoplysninger vedrørende denne behandles, adgang til disse personoplysninger, samt de i litra a-h nævnte forhold, herunder de modtagere eller kategorier af modtager, som personoplysningerne er eller vil blive videregivet til efter litra c.

Sagerne rejste spørgsmål af principiel betydning for indsigtsretten, idet indsigt i modtagerens identitet blev afvist under henvisning til, at Udviklings- og Forenklingsstyrelsen fandt identitetsoplysningerne omfattet af den særlige tavshedspligt i henhold til den danske skatteforvaltningslov § 17, stk. 1, jf. lovbekendtgørelse nr. 1053 af 20. september 2024, og dermed undtaget retten til indsigt efter den danske databeskyttelseslov § 22, stk. 3, jf. lovbekendtgørelse nr. 289 af 8. marts 2024. Der var derfor grundlag for at vurdere, hvorvidt også utilsigtede modtagere af personoplysninger omfattes af indsigtsretten, og i bekræftende fald om en revisors identitetsoplysninger omfattes af tavshedspligten i skatteforvaltningslovens § 17, stk. 1, og dermed kan undtages efter databeskyttelseslovens § 22, stk. 3. Henset til sagens principielle genstandsfelt, blev spørgsmålet forelagt det danske Dataråd.

Datatilsynet fandt herefter, at der vedrørende identiteten af en revisor, dvs. navn og kontaktoplysninger, ikke i alle tilfælde kan være tale om oplysninger, som omfattes af ovennævnte tavshedspligt. Dette var af hensyn til, at dette er oplysninger, som kan være offentligt kendte eller tilgængelige, eller efter almindelig opfattelse er ufortrolige; om end konteksten hvori oplysningerne indgår kunne føre til et andet resultat. For så vidt angik identitetsoplysningerne på revisorens klient, på hvis vegne revisorens havde foretaget aktindsigtsanmodningen, fandt Datatilsynet dog modsat at der var tale om tavshedsbelagte oplysninger undtaget indsigtsretten efter GDPR art. 15.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/okt/borgere-havde-ret-til-indsigt-i-navn-paa-utilsigtet-modtager

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/sep/borgere-havde-ret-til-indsigt-i-navn-paa-utilsigtet-modtager

Databehandling udover det nødvendige ved app til udbetaling af pant

Det danske datatilsyn (»Datatilsynet«) har i en afgørelse af 26. september 2024 udtalt alvorlig kritik af Dansk Retursystems pant-app samt udstedt en advarsel og et påbud om, at selskabet bringer databehandlingen i overensstemmelse med GDPR. Sagen er offentliggjort under journalnummeret 2023-431-0013.

Sagen udsprang af Datatilsynets undersøgelse af Dansk Retursystems app »Pant«, hvis formål var at udbetale pant via direkte pengeoverførsler. Genstanden var appens databehandling, som i relation hertil indeholdt en tredjepartskomponent, der indhentede brugerens kontooplysninger for at kunne udbetale penge til den korrekte konto. Tredjepartsløsningen indsamlede dog yderligere oplysninger såsom saldi, identitetsoplysninger og transaktionshistorik, hvilke dog ikke blev videregivet til Dansk Retursystem.

Datatilsynet anerkendte indledningsvist, at udviklingen af it-løsninger ofte sker ved brug kodebiblioteker, API'er og andre dataintegrationer, der ikke nødvendigvis hidrører fra den dataansvarliges egen organisation. Tilsynet understregede imidlertid, at anvendelsen af en tredjepartsløs-

ning ikke fritager en dataansvarlig fra forpligtelsen til selvstændigt at vurdere, hvorvidt databehandlingen er i tråd med GDPR, herunder om databeskyttelsen er tilstrækkeligt implementeret gennem design efter art. 25.

Datatilsynet udtalte, at en dataansvarlig i sådant tilfælde bør foretage en risikovurdering af anvendt tredjepartssoftware, og hvor denne tredjepart ikke tilbyder en mulighed for at tilpasse eller begrænse behandlingen af personoplysninger til hvad der er i overensstemmelse med bl.a. de grundlæggende principper i GDPR, vil løsningen ikke lovligt kunne anvendes. Konkret fandt Datatilsynet, at databehandlingen var sket i strid med GDPR art. 5 og art. 25, idet behandlingen klart gik ud over det nødvendige i forhold til formålet, samt at indsamlingen var sket på uklar vis ved at angive i brugerbetingelserne, at der i visse brugstilfælde kunne indhentes og behandles flere data end dem, som benyttes til formålet.

Afslutningsvist udtalte Datatilsynet, at principperne som fastlagt i afgørelsen fremover vil være retningsgivende for sanktionsvalget i lignende sager, og særligt for lignende offentlige og private institutionelle aktører af tjenester, som på tilsvarende vis opererer på et område med et begrænset udvalg af udbydere.

Læs Datatilsynets pressemeddelelse her. https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/okt/alvorlig-kritik-paabud-og-advarsel-i-sag-om-pant-app

Læs Datatilsynet afgørelse her. https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/sep/alvorlig-kritik-paabud-og-advarsel-i-sag-om-pant-app

Datatilsynet godkendte Helsingør Kommunes behandling af ulovligt tilvejebragte oplysninger

Det danske Datatilsyn (»Datatilsynet«) har den 13. september 2024 truffet afgørelse i en sag med journalnummer 2024-32-0482 om Helsingør Kommunes behandling af oplysninger, som var ulovligt tilvejebragt.

En borger klagede til Datatilsynet over, at Helsingør Kommune havde valgt på trods af klagers indsigelser at anvende oplysninger fra aflytninger af faren til klagers barn, i form af skjulte mikrofoner og transskriberinger heraf. Aflytningerne havde resulteret i en straffedom for ulovlig aflytning. Kommunen havde oprindeligt afvist at anvende oplysningerne, men omgjorde beslutningen efter henvendelse fra Familieretshuset, der udtrykte bekymring af hensyn til barnets bedste. Det var kommunens vurdering som dataansvarlig, at behandlingen af oplysningerne tjente et sagligt og nødvendigt formål.

Det følger af Datatilsynets praksis, at behandling af ulovligt tilvejebragte oplysninger, kan være i strid med princippet om rimelighed i henhold til GDPR art. 5, stk. 1, litra a. Dette beror på en konkret vurdering i den enkelte sag. Datatilsynet fandt dog, efter at have forelagt sagen i Datarådet, at behandlingen konkret var rimelig, herunder henset til formålet med kommunens behandling af oplysningerne, der navnlig var at afdække, om der var behov for at træffe foranstaltninger med henblik på at sikre barnets tarv.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/okt/helsingoer-kommunes-behandling-af-ulovligt-tilvejebragte-oplysninger-var-i-overensstemmelse-med-databeskyttelsesreglerne

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/sep/helsingoer-kommunes-behandling-af-ulovligt-tilvejebragte-oplysninger-var-i-overensstemmelse-med-databeskyttelsesreglerne

Datatilsynet gennemførte tilsyn med behandlingssikkerheden i 48 kommuner

Det danske Datatilsyn (»Datatilsynet«) har den 15. oktober 2024 udgivet en vejledning på baggrund af et tilsyn iværksat 7. maj 2024 hos 48 kommuner. Tilsynet baserede sig på kommunernes egen-evaluering i forhold til grundlæggende behandlingssikkerhed.

I tilsynet med kommunernes modenhed indgik de tekniske minimumskrav for statslige myndigheder, som Datatilsynet vurderede, repræsenterer *best practice* og i mange tilfælde allerede følger af gældende praksis fra Datatilsynet og andre relevante myndigheder.

Datatilsynets offentliggjorte vejledning vedrører fem udvalgte indsatsområder, hvor kommunerne konkret bør sætte ind for at leve op til reglerne. Det gælder *i)* procedurer for sletning, *ii)* foranstaltninger mod utilsigtet deling, *iii)* rettighedsstyring, *iv)* konsekvensanalyse og *v)* domænesikkerhed.

Det bør desuden fremhæves, at alle kommuner yderligere har modtaget en individuel rapport med konkrete anbefalinger, som de skal arbejde videre med for at styrke behandlingssikkerheden.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/okt/datatilsynet-har-afsluttet-skriftlige-tilsyn-med-behandlingssikkerheden-i-48-kommuner

Læs Datatilsynets vejledning her: https://www.datatilsynet.dk/Media/638645884892374561/Tilsyn%20med%20kommunernes%20modenhed%20i%20forhold%20til%20grundl%C3%A6ggende%20behandlingssikkerhed%202024.pdf

Boliglag.dk får kritik for manglende lovligt behandlingsgrundlag ved sin behandling af oplysninger om boligejere

Det danske Datatilsyn (»Datatilsynet«) har den 16. oktober 2024 truf-

fet afgørelse i en sag med journalnummer 2024-431-0033 om boligsiden Boliglag.dk's manglende behandlingsgrundlag ved behandling af oplysninger om boligejere.

Datatilsynet havde indledt sagen af egen drift efter en række modtagne klager. I undersøgelsen af sagen fandt Datatilsynet, at det på hjemmesiden var muligt at tilgå oplysninger om bl.a. navn, køn og alder på nuværende og tidligere ejere af boliger samt boligernes salgshistorik og salgsværdi. Oplysningerne kunne fremsøges enten ved at søge på en bestemt adresse eller ved at søge direkte på en fysisk persons navn.

Datatilsynet fandt efter en konkret vurdering, at der var grundlag for at udtale kritik i sagen, da behandlingen af personoplysninger ikke kunne ske inden for rammerne af interesseafvejningsreglen i GDPR art. 6, stk. 1, litra f). Dette var på trods af, at det efter Datatilsynets vurdering normalt vil være tilladt for en dataansvarlig at behandle personoplysninger, som er indhentet fra et eller flere offentligt tilgængelige registre, og som allerede er offentliggjort.

Datatilsynet udtalte, at formålet om at skabe større gennemsigtighed på boligmarkedet og fremme adgangen til offentligt tilgængelige boligdata på en nem og overskuelig måde uden betaling til brug for bolighandel m.v. er sagligt og relevant. Dog fandt de, at dette formål kunne forfølges lovligt på en mindre indgribende måde end det hændte.

Datatilsynet lagde i den henseende vægt på, at de registrerede ikke med rimelighed kunne forvente en så omfattende samkøring og offentliggørelse af deres personoplysninger, som hjemmesiden foranledigede. Det var desuden særligt indgribende, at oplysningerne kunne fremsøges ved en søgning på den enkelte persons navn.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/okt/boliglagdk-faar-kritik-for-ulovlig-behandling-af-oplysninger-om-boligejere

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/okt/boliglagdk-faar-kritik-for-ulovlig-behandling-af-oplysninger-om-boligejere

Datatilsynet har offentliggjort et afsluttende brev i forbindelse med deres tilsyn med en række frie grundskoler

Det danske Datatilsyn (»Datatilsynet«) har den 30. september 2024 offentliggjort et afsluttende brev under journalnummeret 2024-41-0093 i forbindelse med deres tilsyn af 25 udvalgte frie grundskoler. Tilsynets fokus var behandling og hjemmel til videregivelse af personoplysninger samt håndtering af anmodninger om indsigt og sletning.

Formålet med tilsynet var bl.a. et indblik i skolernes »modenhedsniveau« i forhold til efterlevelse af reglerne om hjemmel til videregivelse og håndtering af rettighedsanmodninger.

Datatilsynet fandt, at et større antal af skolernes privatlivspolitikker indeholdt et afsnit, der ikke længere var i overensstemmelse med de gældende databeskyttelsesregler. Afsnittet omhandlede skolens ret til opkrævning af gebyrer for administrative omkostninger ved indsigtsanmodninger. Datatilsynet opfordrede derfor skolerne til at fjerne afsnittet fra deres privatlivspolitikker. Datatilsynet fandt derudover, at der var behov for nærmere vejledning angående hjemmel til videregivelse og håndtering af rettighedsanmodninger.

På denne baggrund samlede Datatilsynet sine generelle observationer og bemærkninger baseret på svar fra skolerne i deres afsluttende brev. I det afsluttende brev indgik bl.a. observationer vedrørende manglende identifikation af specifik hjemmel til behandling af personoplysninger og vejledning om behandling af personoplysninger på baggrund af samtykke, jf. GDPR art. 6, stk. 1, litra a.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/okt/datatilsynet-har-undersoegt-de-frie-grundskolers-behandling-af-personoplysninger

Læs Datatilsynets afsluttende brev her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/sep/datatilsynet-har-undersoegt-de-frie-grundskolers-behandling-af-personoplysninger

Indhentelse af kopi af pas og straffeattester ved rekruttering af medarbejdere var lovlig henset til Parken Services A/S' særlige risikoprofil

Det danske Datatilsyn (»Datatilsynet«) har den 5. september 2024 truffet afgørelse i en sag om procedurerne for indhentelse af oplysninger i forbindelse med rekruttering af medarbejdere hos Parken Services A/S (»Parken«). Sagen blev afgjort under journalnummeret 2023-431-0025.

Datatilsynet blev efter en konkret henvendelse bekendt med, at Parken indhenter kopi af pas og straffeattester i forbindelse med rekruttering af medarbejdere. I den forbindelse ønskede Datatilsynet at undersøge Parkens overholdelse af princippet om dataminimering i GDPR art. 5, stk. 1, litra c), samt hvilken behandlingshjemmel Parkens behandling af personoplysninger henføres under.

Overordnet fandt Datatilsynet, at behandlingen af personoplysningerne efter en konkret vurdering skete inden for rammerne af databeskyttelsesreglerne.

Vedrørende indhentelsen af kopi af pas fandt Datatilsynet, at der på baggrund af de særlige omstændigheder omkring Parkens rekrutteringsprocedure, herunder det meget store antal personer, som Parken beskæftiger, ikke var grundlag for at tilsidesætte Parkens vurdering i rela-

tion til spørgsmålet om dataminimering eller behandlingshjemmel.

Datatilsynet fandt tilsvarende vedrørende spørgsmålet om indhentelse af straffeattester, at Parkens indhentelse af straffeattester, der for løsarbejdere var på ansøgningstidspunktet og for fastansatte var ved beslutningen om ansættelse af den pågældende ansøger, skete inden for rammerne af GDPR.

Der blev i den forbindelse lagt særlig vægt på, at *i)* Parken havde vurderet nødvendigheden af indhentelsen ved forskellige stillingskategorier, *ii)* indhentelsen skete på det senest mulige tidspunkt i forhold til rekrutteringsproceduren, og *iii)* der knyttede sig en helt særlig risikoprofil til Parken på baggrund af en myndighedsvurderet alvorlig og sandsynlig terrorrisiko, som desuden var bekræftet af politiet.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/okt/parken-services-as%E2%80%99-behandling-af-personoplysninger-ved-rekruttering

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/sep/parken-services-as%E2%80%99-behandling-af-personoplysninger-ved-rekruttering

Brøndby Kommune får alvorlig kritik for manglende sikkerhedsforanstaltninger

Den 7. oktober 2024 udtalte det danske Datatilsyn (»Datatilsynet«) alvorlig kritik af Brøndby Kommune for ikke at have truffet tilstrækkelige foranstaltninger til at sikre et passende sikkerhedsniveau af deres IT-systemer. Kritikken omfattede manglende kontrol af adgangsrettigheder og manglende brug af 'Multi-Factor Authentication' (MFA). Sagen blev behandlet under journalnummer 2023-423-0016.

Datatilsynet fandt indledningsvist, at kommunen ikke udførte tilstrækkelig kontrol med adgangsrettigheder. Selvom kommunen havde retningslinjer for interne brugeres adgang, kunne den ikke dokumentere at disse reelt blev fulgt. Kommunens kontrol bestod af stikprøver af 10 brugere udført én gang årligt, i 2020 og 2021. Samtidig manglede kommunen en formaliseret proces til at sikre, at rettigheder for eksterne brugere blev nedlagt rettidigt.

Datatilsynet konkluderede herefter, at kommunen ikke levede op til GDPR art. 5, stk. 1, litra f, og art. 32, stk. 1. Bestemmelserne kræver, at adgangen til personoplysninger kun gives til brugere med et sagligt behov, og at adgangsrettigheder begrænses til de oplysninger, der er nødvendige for brugerens opgaver. Datatilsynet understregede, at kontrollens hyppighed bør tilpasses de problemer, som kontrollerne afslører.

Datatilsynet fandt for det andet en manglende implementering af MFA på de tre undersøgte IT-systemer, selvom systemerne behandlede særligt beskyttelsesværdige personoplysninger. Systemerne havde direkte adgang fra internettet, hvilket øgede sikkerhedsrisikoen. Datatilsynets fremhævede, at det først var efter tilsynets varsling, at Brøndby kommune valgte at implementere en to-faktor-login.

Datatilsynet udtalte, at kravet om passende sikkerhed indebærer, at kommuner og andre dataansvarlige skal implementere verifikationsforanstaltninger som MFA ved oprettelse af fjernadgange til systemer med følsomme eller fortrolige personoplysninger og/eller oplysninger om mange registrerede.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/nov/broendby-kommune-faar-alvorlig-kritik-for-manglende-sikkerhedsforanstaltninger

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/okt/broendby-kommune-faar-alvorlig-kritik-for-manglende-sikkerhedsforanstaltninger

Mangel på passende sikkerhedsprocedurer i Kerteminde Kommune

Det danske Datatilsyn (»Datatilsynet«) har udtalt kritik af Kerteminde Kommune for kommunens manglende implementering af passende sikkerhedsforanstaltninger ved behandling af personoplysninger. Sagen er offentliggjort under journalnummeret 2023-423-0019.

Datatilsynet udførte et tilsynsbesøg hos Kerteminde Kommune i efteråret 2023. Datatilsynet vurderede en række forhold, herunder logning og logauditering.

Angående logning og logauditering drejede tilsynsbesøget sig om, hvorvidt Kerteminde Kommune havde indført passende sikkerhedsforanstaltninger i relation til dets medarbejderes færden i kommunens systemer, som påkrævet under GDPR art. 32, stk. 1. Datatilsynet fandt, at kommunen ikke havde faste procedurer for løbende logkontrol af medarbejderne, men kommunen udførte alene en kontrol, hvis der var konkret mistanke om misbrug. Kerteminde Kommune har efterfølgende oplyst, at kommunen vil starte en proces op, der skal sikre løbende kontrol.

Datatilsynet bemærkede generelt, at det er et absolut minimumskrav, at der gennemføres en stikprøveudtagning hvert halve år af systemer, der behandler fortrolige og/eller følsomme oplysninger eller har adgangsrettigheder af en bred karakter. I den forbindelse kan dataansvarlige etablere et alarmsystem ved mistænkelig aktivitet. Hertil skal den dataansvarlige sikre en effektiv implementering af logkontrol, hvilket kan sikres ved at kombinere effektiv kontrol med behørig orientering til medarbejderne om logkontrol. En restriktiv rolle- og adgangsstyring for den dataansvarliges it-systemer er ikke en effektiv foranstaltning, der kan kontrollere om medarbej-

derne har tilgået personoplysninger på et usagligt grundlag. Der var alene grundlag for kritik vedrørende tilsynets behandling af kommunens logning og logauditering.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/nov/kerteminde-kommune-faar-kritik-for-deres-sikkerhedsprocedurer

Læs Datatilsynet afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/feb/kerteminde-kommune-faar-kritik-for-deres-sikkerhedsprocedurer

Forbedret vejledningsindsats ved brud på persondatasikkerhed

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 26. november 2024 at Datatilsynet har forbedret og udvidet sin vejledning til organisationer ved brud på persondatasikkerheden.

Når en sag afsluttes hos Datatilsynet, oversendes en række links til anmelderen om relevante vejledninger; dels udarbejdet af Datatilsynet, dels materialer, der stammer andetsteds fra. Disse vejledninger udvælges automatisk, men gennemgås manuelt for at tilpasse vejledningerne til den konkrete hændelse. Denne målrettede vejledningsindsats er styrket yderligere ved et nyt tiltag, hvor Datatilsynet fremover vil henvise til et GDPR-univers for små foreninger, når de anmelder et brud på persondatasikkerheden.

Denne øgede indsats skal øge kendskabet til vejledningerne og reducere sandsynligheden for brud på persondatasikkerhed.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/nov/datatilsynet-styrker-vejledningsindsatsen-yderligere-ved-brud-paa-persondatasikkerheden

Lyngby-Taarbæk Kommune politianmeldt af Datatilsynet

Det danske Datatilsyn (»Datatilsynet«) har i en pressemeddelelse af 27. november 2024 offentliggjort, at de har politianmeldt Lyngby-Taarbæk Kommune og indstillet kommunen til en bøde på 350.000-400.000 kr. for brud på forpligtelsen til at gennemføre passende sikkerhedsforanstaltninger som dataansvarlig. Sagen er fortsat under behandling.

Politianmeldelsen udsprang af, at Lyngby-Taarbæk Kommune anmeldte en række brud på persondatasikkerheden om uautoriseret adgang til personoplysninger. Anmeldelserne drejede sig om manglende retningslinjer og procedure for nedlæggelse af brugeradgang og fravær af regelmæssig kontrol med dette, da tidligere medarbejdere fortsat havde adgang til it-systemet KMD-Nexus. Dette it-system indeholdt fortrolige og følsomme personoplysninger om et stort antal borgere på omsorgsområdet i kommunen. Endvidere drejede anmeldelserne sig om misbrug af loginoplysninger til en række Microsoft Office-tjenester, der var uvedkommende for en medarbejder i kommunen.

Til sidst undersøgte Datatilsynet om kommunen havde implementeret effektiv sikring af fjernadgangsforbindelser til it-systemet og Office-tjenesterne. Dette var ikke tilfældet, og Datatilsynet fandt, at der var en øget risiko forbundet hermed, da disse systemer og tjenester kan tilgås direkte fra internettet.

Datatilsynet indstillede til bøden i medfør af GDPR art. 83, stk. 2, hvor Datatilsynet lagde vægt på sagens grovhed. Kommunen havde i flere tilfælde og over en længere periode undladt at implementere grundlæggende sikkerhedsforanstaltninger, passende retningslinjer og procedurer til trods for, at kommunen blev gjort opmærksom herpå.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/nov/datatilsynet-anmelder-lyngby-taarbaek-kommune-til-politiet

God praksis for styring af datakvalitet

Det danske Finanstilsyn (»Finanstilsynet«) har den 8. oktober 2024 offentliggjort et notat vedrørende god praksis for kreditinstitutternes styring af datakvalitet. Notatet omhandler datakvalitet på alle risikoområder, og retter sig mod de kreditinstitutter, der skal efterleve kravene til styring af datakvalitet i § 8, stk. 11, § 19, stk. 1, nr. 5, samt bilag 7, nr. 9, i bekendtgørelse nr. 1103 af 30 juni 2022 om ledelse og styring af pengeinstitutter m.fl. (»ledelsesbekendtgørelsen for pengeinstitutter m.fl.«).

Notatet er udarbejdet på baggrund af en række inspektioner af datakvalitet i de største danske kreditinstitutter, som Finanstilsynet har gennemført i 2023 og 2024. Her fandt Finanstilsynet, at styringen af datakvalitet var påvirket af fejl, mangler og forsinkelser i kreditinstitutternes løbende dataindberetninger og dataleverancer. Herudover fandt Finanstilsynet, at der var mangel på systematik og ensartethed i kontrollen af data.

Det anbefales, at der udarbejdes metoder og retningslinjer for at følge god praksis inden for datakvalitet. Kreditinstitutterne kan her lade sig vejlede af 'Principles for effective risk data aggregation and risk reporting', 2013, Bank for International Settlements (»BCBS 239«).

Ydermere anbefales det af Finanstilsynet, at der etableres klare retningslinjer for roller og ansvar, fastlægges forretningsgange og metoder for styring af datakvalitet af især kritiske dataelementer samt udarbejdes et datakatalog for metadata.

Læs Finanstilsynets pressemeddelelse her: https://www.finanstilsynet.dk/nyheder-og-presse/nyheder-og-pres-

Illustrasjon: Colourbox.com

semeddelelser/2024/okt/god_praksis_styring_datakvalitet_081024
Læs Finanstilsynets notat om god praksis her: https://www.finanstilsynet.dk/Media/638639668063564514/God-praksis-notat%20om%20kreditinstitutters%20styring%20af%20datakvalitet%20(002).pdf

Et risikopræget 2025 for den finansielle sektor

Det danske Finanstilsyn (»Finanstilsynet«) har den 18. december 2024 udgivet sit halvårlige notat vedrørende risikobilledet i det finansielle system. Notatet indeholder *(i)* en redegørelse af en række makrofinansielle risici, *(ii)* indsatser Finanstilsynet agter at iværksætte i 2025 på baggrund heraf, samt *(iii)* tre risikoscenarier og de finansielle konsekvenser heraf.

Finanstilsynet har identificeret en række risici for den finansielle sektor. Det angår en række makrofinansielle forhold, herunder risici vedrørende inflationen og renteniveau, geopolitisk indvirkning på aktiekurser, trusler og stigende tilfælde af cyberangreb, samt et øget antal af IT-driftshændelser, der potentielt kan medføre angreb i forsyningskæden, hvilket kan lede til en bredere påvirkning af den finansielle sektor.

Finanstilsynet fører en risikobaseret tilsynsvirksomhed, hvor ovennævnte risici har dannet grundlag for Finanstilsynets indsats i 2025. For det første, vil Finanstilsynet påbegynde en indsats til at sikre en robust finansiel sektor. Dette indebærer et fokus på udlån på private og konjunkturfølsomme erhverv, undersøgelser af belåningsstandarder ved boliglån samt af udenlandske aktører på markedet for erhvervsejendomme. Endvidere indebærer det en overvågning af implementeringen og overholdelsen af en række regulatoriske forhold og udarbejdelse af vejledninger til den finansielle sektor. Herudover vil Finanstilsynet også påbegynde indsatser, der skal sikre en ordentlig finansiel sektor. Dette skal sikres gennem en undersøgelse af prissætning for pensionsselskaber, fokus på hvidvaskregulering og svindel.

Til sidst vil Finanstilsynet også have fokus på bæredygtighedsrapportering.

Som nævnt har Finanstilsynet udarbejdet tre forskellige risikoscenarier med samfundsøkonomiske konsekvenser, der tager udgangspunkt i individuelle og systematiske risici. Dette er *i)* en hård recession, *ii)* en krise på de finansielle markeder, og *iii)* hackerangreb, der skaber markante driftsforstyrrelser.

Læs Finanstilsynets pressemeddelelse her: https://www.finanstilsynet.dk/nyheder-og-presse/nyheder-og-pressemeddelelser/2024/dec/risikobillede_h2_181224

Læs Finanstilsynets notat om risikobilledet her: https://www.finanstilsynet.dk/Media/638701032455799341/Hjemmesidenotat_E24.pdf

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

Delphi

Sophie Wichmann

Tre bolag får reprimand av IMY efter att ha delat personuppgifter via Meta-pixeln

Integritetsskyddsmyndigheten (IMY) har utdelat en reprimand till Kry International AB (”Kry”), Apotea Sverige AB (Apotea”), Länsförsäkringar AB och ytterligare 27 bolag inom Länsförsäkringsgruppen efter att bolagen brutit mot dataskyddsförordningen.

Verksamheterna hade av misstag läckt personuppgifter till Meta, som äger bland annat Facebook och Instagram. I samtliga fall uppgav bolagen att den felaktiga överföringen orsakats av att en delfunktion i analysverktyget Meta-pixeln aktiverats utan deras kännedom. Informationen användes till annonsering och marknadsföring och innehöll till exempel mejladresser och telefonnummer. Länsförsäkringar upptäckte läckan efter knappt tre månader men för Kry och Apotea tog det närmare två år.

Den personuppgiftsansvarige ska enligt artikel 32.1 i dataskyddsförordningen vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen. Bolagen uppgav i samband med tillsynen att de visserligen haft rutiner för att följa upp sin behandling av personuppgifter, men att de inte följts.

I besluten konstaterade IMY att en grundläggande förutsättning för att bolagen ska kunna uppfylla sina skyldigheter enligt dataskyddsförordningen är att de är medvetna om vilken behandling som sker under deras ansvar. Bolagen kände inte till incidenterna förrän en utomstående uppmärksammat dem. IMY konstaterade därför att bolagen saknat kontroll och förmåga att identifiera oavsiktlig behandling av personuppgifter.

Särskilda kategorier av personuppgifter, till exempel uppgifter om hälsa, är förbjudna att behandla om inte undantag föreligger enligt artikel 9.2 i dataskyddsförordningen. I sin bedömning konstaterade IMY att de aktuella överföringarna inte hade omfattat särskilda kategorier av personuppgifter. Avseende Kry hade överföringen inte omfattat några uppgifter om relationen mellan användaren och slutanvändaren eller några uppgifter om vad bokningen gällt. Det hade således inte gått att utläsa om slutanvändaren varit patient och inte heller om mötet utgjort ett vårdbesök, eller vilka hälsobesvär det i så fall skulle gälla. Avseende Apotea hade endast produkternas interna produkt-id och inga uppgifter om t.ex. namnet på produkten överförts till Meta. Det framgick alltså inte av uppgifterna som fördes över till Meta om en kund hade köpt en vara av integritetskänslig natur, t.ex. läkemedel eller medicintekniska produkter.

Illustrasjon: Colourbox.com

I samtliga fall uttalade dock IMY att kunderna, med hänsyn till sammanhanget personuppgifterna behandlades i, haft en berättigad förväntan på att deras uppgifter hanteras med hög grad av konfidentialitet.

Mot bakgrund av att bolagen på förhand hade begränsat behandlingen på ett sådant sätt att känsliga personuppgifter inte kunnat överföras till Meta, bedömde IMY att överträdelserna var av mindre allvarlig art och bolagen undgick sanktionsavgift.

Besluten visar på vikten av att ha lämpliga tekniska och organisatoriska åtgärder på plats för att ha kontroll över verksamhetens personuppgiftsflöden och upptäcka eventuella personuppgiftsincidenter.

Sophie Wichmann, Thesis Trainee, Advokatfirman Delphi

Gorrissen Federspiel

Tue Goldschmieding

Forvekslingsrisiko mellem ordmærket »KynoRehab« og forretningskendetegnet »CPH Kyno«

Østre Landsret har den 3. oktober 2024 afsagt kendelse i kæresagen mellem den kæ-rende, KynoRehab ApS (»KynoRehab«), og den indkærede, som drev virksomhed under navnet »CPH Kyno«, i en sag om brud på den danske varemærkelovs § 4, stk. 2, nr. 2, jf. lovbekendtgørelse nr. 88 af 29. januar 2019, om forvekslingsrisiko med et beskyttet varemærke, samt den danske markedsføringslovs § 3 og § 22, jf. lovbekendtgørelse nr. 1420 af 2. december 2024, om henholdsvis god markedsføringsskik og om identiske eller forvekslelige forretningskendetegn. Afgørelsen blev afsagt under sagsnummeret BS-3677/2024-OLR.

KynoRehab, indehaveren af det registrerede ordmærke »KynoRehab«, påstod som kærende, at virksomhedsdrift under navnet »CPH Kyno« medførte en forvekslingsrisiko efter varemærkelovens § 4, stk. 2, nr. 2, og subsidiært, at det udgjorde en overtrædelse af markedsføringslovens § 3 og § 22. Begge parter drev virksomhed med »terapi og justeringer af hunde«.

Indledningsvist konstaterede Landsretten, at »CPH Kyno« ikke havde opnået varemærkeretlig beskyttelse. Landsretten fandt derefter, at de respektive mærkers bestanddele »Rehab« og »CPH« måtte anses for henholdsvis beskrivende for de udbudte ydelser eller en stedsangivelse. Bestanddelen »Kyno« var altså den relevante del til brug for forvekslingsvurderingen efter varemærkelovens § 4, stk. 2, nr. 2.

Landsretten lagde herefter vægt på det faktum, at »kyno« betød hund på græsk, hvilket ikke kunne anses for kendeligt for en betydelig del af den danske befolkning, og at der ikke var oplysninger om brug af ordet som betegnelse for lignende ydelser hos andre erhvervsdrivende i landet. Landsretten fandt, at ordet »kyno« havde tilstrækkeligt særpræg, samt at forretningskendetegnet »CPH Kyno« derfor medførte en forvekslingsrisiko efter varemærkelovens § 4, stk. 2, nr. 2.

Østre Landsret stadfæstede herefter forbuddet mod, at indkærede gjorde erhvervsmæssig brug af navnet »CPH Kyno«.

Læs dommen fra Østre Landsret her: https://domsdatabasen.dk/#sag/6379/7654

Brug af kagefotos i YouTube-video ikke omfattet af parodiundtagelsen til ophavsretten

Østre Landsret har den 13. november 2024 afsagt dom i sag BS-50776/2023-OLR om krænkelse af ophavs- og persondataretten ved en DJ's *(i)* brug af en bloggers kagefotos i en video på videoplatformen YouTube samt *(ii)* omtale af bloggerens navn, bopælsområde og visning af portrætbillede i en live-stream på streamingplatformen Twitch.

Angående brugen af bloggerens fotos konstaterede retten, at disse var omfattet af den danske ophavsretslov § 70, jf. lovbekendtgørelse nr. 1093 af 20. august 2023, om naboretlig beskyttelse af fotografiske billeder. Retten tog derved navnlig stilling til, om brugen var omfattet af parodiundtagelsen. Retten udtalte, at den nye bestemmelse om parodi, karikatur eller pastiche i ophavsretslovens § 24 b udgjorde en kodificering af gældende ret vedrørende parodiundtagelsen til dansk ophavsret. Retten afviste, at DJ'ens brug af billederne var omfattet af denne undtagelse, idet brugen ikke vakte en forestilling om de eksisterende værker. Brugen udgjorde derfor en krænkelse af bloggerens ophavsret efter ophavsretslovens § 70.

Retten behandlede ligeledes, om DJ'ens brug af bloggerens navn, bopælsområde og portrætbillede på en livestream på mediet Twitch udgjorde en krænkelse af GDPR, idet der var tale om personoplysninger efter GDPR art. 4, nr. 1. Retten udtalte, at brugen var sket som led i markedsføring, hvorfor DJ'en var dataansvarlig, jf. art. 4, nr. 7, og følgelig ikke kunne anses for en privat aktivitet uden for GDPR, jf. art. 2, stk. 2, litra c. Retten fandt, at DJ'en havde krænket bloggerens rettigheder ved ikke at foretage en lovlig, rimelig og gennemsigtig behandling i GDPR art. 5, stk. 1, litra a, hvorfor der ikke var det fornødne lovlige behandlingsgrundlag, jf. GDPR art. 5, stk. 2, jf. art. 6.

Retten udtalte derefter, at der ligeledes forelå en krænkelse af bloggerens ret til eget navn og billede efter det ulovbestemte princip i dansk ret, idet DJ'ens omtale af bloggeren ikke var nødvendigt for at rejse en offentlig debat om parodisk brug af ophavsretligt beskyttede billeder, og der derved ikke var en rimelig begrundelse for brugen.

Endelig konstaterede retten, at DJ'en var underlagt princippet i lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«) § 3 om god markedsføringsskik, idet omtalen af bloggeren var sket i markedsføringsmæssig henseende. Retten fandt, at DJ'ens brug havde afstedkommet en række negative kommentarer om bloggerens person, og at dette må have været klart påregneligt for DJ'en. Der forelå derfor en krænkelse af god markedsføringsskik efter markedsføringslovens § 3.

Læs dommen fra Østre Landsret her: https://domsdatabasen.dk/#sag/6644/7981

Sø- og Handelsretten afviser krænkelse i sag mellem Bayer A/S og tre udbydere af generiske lægemidler

Sø- og Handelsretten har den 9. oktober 2024 afsagt kendelse i sagerne BS-17450/2024-SHR, BS-19709/2024-SHR og BS-9717/2024-SHR om midlertidigt forbud og påbud baseret på en påstået krænkelse af et patent mellem patentindehaveren Bayer A/S (»Bayer«) og de tre udbydere af generiske lægemidler Stada Nordic ApS, Glenmark Pharmaceuticals Nordic AB og Sandoz A/S (de »sagsøgte«).

Bayer var indehaver af stridspatentet og markedsførte lægemidlet »Xarelto« baseret på dette patent. De sagsøgte var hver udbydere af generiske lægemidler af »Xarelto«. Krænkelsesvurderingen skulle for hver af de sagsøgte foretages baseret på stridspatentets kravtræk 1.5 om lægemidlets halveringstid, og for Stada Nordic ApS's produkt skulle der ligeledes foretages en vurdering efter kravtræk 1.1 om hurtig frigivelse.

Patentets kravtræk 1.5 gav retten anledning til at foretage en nærmere fortolkning af formuleringerne »halveringstid på 10 timer eller mindre« og »human patient« jf. patentkravslæren i den danske patentlovs § 39, jf. lovbekendtgørelse nr. 90 af 29. januar 2019. Retten konstaterede, at begreberne ikke var nærmere defineret i patentkravenes ordlyd, og foretog derefter en fortolkning af begreberne med henblik på at afklare, hvordan en fagmand ville forstå begreberne på patents prioritetstidspunkt. Rettens fortolkning var baseret på ekspertvidnernes udsagn, patentbeskrivelsen samt Bayers korrespondance med The European Patent Office (EPO) ved registreringen af patentet, samt en efterfølgende ugyldighedssag ved EPO's Technical Board of Appeal.

Retten sammenlignede herefter fortolkningen af stridspatentets kravtræk 1.5 med stridsprodukternes produktresumeer. Retten konkluderede herefter, at Bayer ikke havde sandsynliggjort eller godtgjort, at de sagsøgte krænkede stridspatentet, idet det ikke var sandsynliggjort, at halveringstiden var 10 timer eller mindre. Der var således ikke grundlag for at fremme anmodningen om midlertidige forbud og påbud. Sagen er kæret af Bayer til Østre Landsret.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-17450-2024-SHR-BS-19709-2024-SHR-BS-9717-2024-S.2553.aspx

Gannis populære Buckle Ballerina var beskyttet efter markedsføringsloven, men ikke efter ophavsretsloven

Sø- og Handelsretten afsagde den 1. november 2024 kendelse om den immaterialretlige beskyttelse af det danske modebrand Ganni A/S' (»Ganni«) skomodeller »Buckle Ballerina« og »Buckle Sandal«. Kendelsen, som er kæret til Østre Landsret, er offentliggjort under sagsnummeret BS-32550/2024-SHR.

Sagens omdrejningspunkt var et af Ganni påstået forbud mod, at modeforhandleren Lulu's Fashion Lounge, LLC (»Lulu's Fashion Lounge«) forhandlede mv. Steve Madden LTDs (»Steve Madden«) skomodeller »Graya Ballerina« og »Sandria Sandal«, som ifølge Ganni krænkede Gannis rettigheder til Buckle Ballerina og Buckle Sandal.

Retten afviste indledningsvist Gannis påstand med henvisning til, at det ikke var godtgjort, at Buckle Ballerina opfyldte originalitetskravet, påkrævet for beskyttelse efter den danske ophavsretslov, jf. lovbekendtgørelse nr. 1093 af 20. august 2023. Retten lagde i vurderingen vægt på, at *i)* skoen fremstod som en sammensætning af kendte designelementer, *ii)* de valg, der var truffet i designprocessen, måtte anses for sædvanlige i modeverdenen, og *iii)* der ikke ud fra en samlet betragtning var en sådan nyskabelse, at skoen som intellektuel frembringelse burde nyde ophavsretlig beskyttelse.

Imidlertid fandt retten, at skomodellen besad fornøden kommerciel adskillelsesevne i form af sit særpræg og sin position på markedet, til at nyde beskyttelse efter den danske markedsføringslov, jf. lovbekendtgørelse nr. 1420 af 2. december 2024. Følgelig fandt retten kriterierne for udstedelse af et midlertidigt forbud og påbud for opfyldt for så vidt angik Gannis Buckle Ballerina-skomodel.

Hvad angik Gannis Buckle Sandal fandt retten ikke, at Steve Maddens pendant hertil, skomodellen Sandria Sandal, udgjorde en nærgående efterligning i strid med hverken ophavsrets-, markedsføringsloven eller designlovgivningen. I det lys blev forbuddet rettet mod Lulu's Fashion Lounges markedsføring mv. af denne skomodel afvist.

Det bemærkes, at Ganni i en ellers tilsvarende sag trykt i Lov og Data for 4. kvartal 2024, fik medhold i august 2024 mod selvsamme producent Steve Madden, offentliggjort under sagsnummeret BS-25562/2024-SHR, hvor Sø- og Handelsretten nåede frem til, at

Buckle Ballerina nød såvel ophavsretlig som markedsføringsretlig beskyttelse. Denne afgørelse er tilsvarende kæret.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-32550-2024-SHR.2557.aspx

Læs kendelsen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/media/-300011/files/Kendelse_BS-32550-2024-SHR.pdf

Byggekoncerns anvendelse af navne- og figurmærker udgjorde ikke brud på forligs- og sameksistensaftale

I en dom af 8. november 2024 tog Sø- og Handelsretten stilling til, om Byggmax Group AB (»Byggmax«) havde misligholdt en forligs- og sameksistensaftale (»aftalen«) indgået med Bygma Gruppen A/S (»Bygma«). Spørgsmålet var navnlig, om et senere, dvs. efter aftalens indgåelse, erhvervet datterselskabs BygMax A/S' (»BygMax«) anvendelse af egne kendetegn, virksomhedsnavn og figurmærker var i strid med aftalen. Dommen, som er anket til Østre Landsret, blev afsagt med sagsnummeret BS-29312/2023-SHR.

Idet der til støtte for Bygmas påstande om misligholdelse alene var gjort gældende, at parternes aftale var misligholdt, forelå der ikke en tvist om overtrædelse af varemærkelovgivningen. Retten vurderede derfor kun, om der forelå et brud på selve aftalen. Grundlæggende skulle det herefter klarlægges, om aftalen regulerede brugen af mærket »BYGMAX« og et bestemt figurmærke, og om BygMax' anvendelse heraf stred mod aftalen. Retten fandt ikke, at Byggmax-koncernens anvendelse af mærket »BYGMAX« samt det pågældende figurmærke var omfattet af aftalen, og der forelå ikke sikre holdepunkter for en fravigelse af ordlyden. Byggmax havde således ikke misligholdt aftalen.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-29312-2023-SHR.2559.aspx

Læs dommen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-29312-2023-SHR.pdf

Ikke godtgjort, at en medarbejder uberettiget havde videregivet forretningshemmeligheder angående en licensaftale

Sø- og Handelsretten har den 18. november 2024 afsagt kendelse i sagen BS-20425/2024-SHR, om et midlertidigt forbud mod fortsat markedsføring af et parallelimporteret lægemiddel. Sagsøgeren 2care4 Generics ApS (»2care4 Generics«) påstod, at sagsøgte Nordic Prime ApS (»Nordic Prime«) uberettiget opnåede markedsføringstilladelse til lægemidlet Ivermectin ved at erhverve forretningshemmeligheder fra en tidligere ansat i 2care4 Generics, som efterfølgende blev ansat i Nordic Prime.

Retten fandt, at oplysninger om en licensaftale mellem sagsøger og et ikke oplyst selskab udgjorde forretningshemmeligheder efter den danske lov om forretningshemmeligheder § 2, nr. 1, litra a), jf. lovbekendtgørelse nr. 309 af 25. april 2018, da oplysningerne ikke kunne anses for almindeligt kendt eller umiddelbart tilgængelige for personer i de kredse, der normalt beskæftiger sig med den pågældende type oplysninger.

Retten fandt det dog ikke tilstrækkeligt godtgjort eller sandsynliggjort, at den tidligere ansatte havde videregivet oplysningerne om licensaftalen til Nordic Prime. Retten fandt i stedet, at Nordic Prime havde erhvervet forretningshemmeligheden som en lovlig handling ved uafhængig opdagelse på baggrund af egen research, kompetencer og erfaring i henhold til lov om forretningshemmeligheder § 3 stk. 1. Anmodningen om midlertidigt forbud mod fortsat markedsføring af lægemidlet blev derfor afvist.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-20425-2024-SHR.2563.aspx

Læs kendelsen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/media/-300011/files/Kendelse__BS-20425-2024-SHR.pdf

Vurderingen af en overdragelse af ophavsrettigheder til edb-programmer efter dagældende ophavsretslov skal afgøres efter aftalen

Sø- og Handelsretten afsagde den 18. november 2024 dom i sag BS-17826/2022-SHR mellem Thubalka A/S (»Thubalka«) og sagsøgte A vedrørende ophavsrettigheder til tre forskellige edb-programmer udviklet til at styre klokkespil. Thubalka påstod bl.a. A tilpligtet at anerkende, at enerettighederne til edb-programmerne tilkom Thubalka.

Det første edb-program, »Microsoft DOS-programmet«, var udviklet af A som led i hans ansættelse hos virksomheden Jansson Gruppen A/S (»Jansson«). Forholdet blev behandlet efter den danske ophavsretslovs § 1, jf. lovbekendtgørelse nr. 1093 af 20. august 2023, idet programmet var udviklet forud for 1989-ophavsretslovens § 42 b, nu videreført i § 59, der regulerede ophavsretten til et edb-program frembragt af en arbejdstager som led i ansættelsesforholdet. Retten fastslog herefter, at efter § 1 beholder ophaveren til et edb-program ophavsrettighederne hertil, medmindre andet er aftalt. I vurderingen heraf fandt retten, at ophavsretten ikke kunne anses for overdraget af A, idet der bl.a. blev lagt vægt på, at det ikke var en nødvendighed for Jansson at have ophavsrettighederne til programmet, at der ikke forelå en aftale mellem Jansson og Thubalka om overdragelse af ophavsrettighederne til Thubalka, og at A var ansat som

elektriker og ikke programmør hos Jansson.

Angående de øvrige edb-programmer, »VB6-version 2009« og »VB-version 2018«, var spørgsmålet, om A havde frembragt disse som arbejdstager under sin senere ansættelse hos Thubalka eller efter Thubalkas anvisninger, jf. ophavsretslovens § 59. I tråd med ovenstående, fandt retten dog tilsvarende, at ophavsrettighederne tilkom A, da de ikke kunne anses for frembragt af A som ansat. Med hensyn til VB6-version 2009 blev det bl.a. tillagt betydning, at programmet var udviklet i A's fritid og at der ikke på udviklingstidspunktet forelå en skriftlig ansættelsesaftale. Ved udviklingen af VB-version 2018, var A gået på efterløn, og der var også for dette program ikke indgået en skriftlig aftale mellem parterne om udviklingen af programmet.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-17826-2022-SHR.2558.aspx

Læs dommen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-17826-2022-SHR.pdf

Forbudsretlig passivitet ved to års forløb mellem begæring om forbud og patentudstedelse.

Sø- og Handelsretten har den 20. november 2024 afsagt kendelse i sagen BS-18183/2024-SHR, om midlertidige forbud og påbud vedrørende en række trykmålere. Sagsøger MKS Instruments Inc. (»MKS«) påstod, at trykmålerne, som blev fremstillet af sagsøgte Sens4 ApS (»Sens4«), var i strid med patentet som blev udstedt den 6. april 2022, og der derfor skulle nedlægges midlertidige forbud og påbud.

Retten forholdt sig ikke til, hvorvidt trykmålerne var i strid med patentet, men vurderede alene, hvorvidt der forelå forbudsretlig passivitet. Retten fandt, at MKS den 7. juni 2019 via en tredjepart købte to trykmålere af Sens4, som herefter blev analyseret og undersøgt. MKS var således ifølge retten bekendt med, at trykmålerne indeholdt den omstridte tekniske løsning, på tidspunktet for stridspatenets udstedelse i 2022.

Forbudsbegæringen blev indgivet af MKS den 9. april 2024, to år efter patentet blev udstedt. Et forbud eller påbud kan dog kun meddeles hvis en række kriterier i den danske retsplejelovs § 413 opfyldes, jf. lovbekendtgørelse nr. 1160 af 5. november 2024. Ét af kriterierne er herefter, at det godtgøres eller sandsynliggøres, at partens mulighed for at opnå sin ret vil forspildes, hvis parten henvises til at afvente tvistens retlige afgørelse, jf. retsplejelovens § 413, stk. 1, nr. 3.

Retten fandt, henset til tidsperioden mellem patentets udstedelse og forbudsbegæringen, at MKS ikke ville forspilde sin ret ved at være henvist til at forfølge den ved almindelig rettergang. Retten konkluderede derfor, at der forelå forbudsretlig passivitet, hvorfor Sens4 blev frifundet og anmodningen om forbud og påbud blev afvist.

Læs pressemeddelelsen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-18183-2024-SHR.2560.aspx

Læs kendelsen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/media/-300011/files/Kendelse_BS-18183-2024-SHR.pdf

Ophavsrettigheder til spotlampe og montagevejledning

Sø- og Handelsretten afsagde i sag BS-39050/2024-SHR af 18. december 2024 kendelse om den ophavsretlige beskyttelse af en spotlampe og en dertilhørende montagevejledning. Sagen var anlagt af belysningsleverandøren Teamtronic A/S (»Teamtronic«) mod sagsøgte LYS. A/S og A (»sagsøgte«). A var stifter og ejer af virksomheden LYS. A/S og havde tidligere været ansat som hhv. salgschef og direktør i Teamtronic.

Indledningsvist afviste retten sagsøgers påstand om et brud på den danske lov om forretningshemmeligheder, jf. lov nr. 309 af 25. april 2018, som følge af A's tidligere ansættelse. Vedrørende det ophavsretlige ben af sagen fandt retten, at montagevejledningen til den omstridte spotlampe var beskyttet efter den danske ophavsretslov § 1, jf. lovbekendtgørelse nr. 1093 af 20. august 2023, da den var frembragt ved en tilstrækkeligt selvstændig intellektuel indsats til at kunne anses som et værk i ophavsretlig henseende. Teamtronics eneret var herefter krænket, fordi sagsøgte havde solgt vejledningen i tillæg til spotlampen, hvorfor der kunne udstedes forbud herimod.

I relation til selve spotlampen, fandt retten det dog ikke godtgjort, at lampen besad en sådan fornøden originalitet i forhold til lignende spotlamper, at den var ophavsretligt beskyttet. Manglende ophavsretlig beskyttelse udelukker dog ikke, at slavisk kopiering kan være i strid med princippet om god markedsføringsskik efter den danske markedsføringslovs § 3, jf. lovbekendtgørelse nr. 1420 af 2. december 2024. Retten fandt således, at sagsøgte havde handlet i strid med god markedsføringsskik ved salg af den omtvistede lampe til Teamtronics tidligere største kunde, hvorfor der kunne nedlægges midlertidigt forbud. Der blev lagt vægt på, at A havde udnyttet sin viden om Teamtronics kundeaftaler, samt at lampen var produceret af Teamtronics underleverandør, som havde assisteret med udviklingen af den originale spotlampe.

Læs kendelsen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/media/-300011/files/Kendelse_ekstraheret_BS-39050-2024-SHR.pdf?rev1

Forbud mod fremtidig anvendelse af et selskabsnavn grundet forvekslingsrisiko

I en kendelse af 20. december 2024 har Sø- og Handelsretten truffet afgørelse i forbudssagen BS-47557/2024-SHR mellem Lissy Boesen Design ApS (»Lissy Boesen Design«) og Casa-Form ApS (tidligere Boesen Design ApS) (»Casa-Form«) angående ophavs-, brugs- og varemærkeretten til en række legeskulpturer.

Sagens kerne var, hvorvidt Lissy Boesen Design som selskab havde opnået den omhandlede ophavsret til legeskulpturerne ved overdragelse eller tildeling af eksklusiv brugsret, idet ophavsretten som udgangspunkt tilfaldt den stiftende direktør som oprindelig ophavsperson efter § 1 i den danske ophavsretslov, jf. lovbekendtgørelse nr. 1093 af 20. august 2023. I mangel af at der bestod en skriftlig aftale mellem parterne eller en vurderingsberetning med ophavsretten anført som aktiv, fandt retten det dog ikke godtgjort, at Lissy Boesen Design havde den ret, som de ved søgsmålet søgte beskyttet, hvorfor deres påstand måtte afvises.

Retten fandt imidlertid, at der bestod en betydelig forvekslingsrisiko mellem Lissy Boesen Design og Casa-Forms tidligere selskabsnavn, Boesen Design. Denne risiko var sagsøger beskyttet imod i medfør af den danske markedsføringslovs § 22, jf. lovbekendtgørelse nr. 1420 af 2. december 2024, den danske varemærkelovs § 4, jf. lovbekendtgørelse nr. 88 af 29. januar 2019, og den danske selskabslovs § 2, jf. lovbekendtgørelse nr. 1168 af 1. september 2023. Det var uden betydning, at selskabsnavnet efter forbudssagens anlæg var ændret til Casa-Form. Retten nedlagde herefter forbud mod fremtidig brug af Boesen Design, idet retten bemærkede at selskabsnavnet ville kunne ændres tilbage igen.

Læs kendelsen fra Sø- og Handelsretten her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-47557-2024-SHR.2568.aspx

Illustrasjon: Colourbox.com

Overtrædelse af forbud mod at opfordre børn til køb på sociale medier

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) har i en afgørelse af den 8. oktober 2024 i sagerne 24/06341, 24/06340 og 24/06342 vurderet, at flere influenter har overtrådt forbuddet mod direkte at opfordre børn til køb af produkter i henhold til den danske markedsføringslovs § 9, jf. lovbekendtgørelse nr. 1420 af 2. december 2024.

Forbrugerombudsmanden vurderede, at influenterne gennem deres opslag på sociale medier lagde pres på børnene ved at tilskynde dem til hurtige køb, idet de direkte linkede til produkter og bl.a. skrev »en ting du gerne må gøre for mig er at købe [x].« Forbrugerombudsmanden lagde i sin vurdering særligt vægt på, at influenterne generelt har en stor gennemslagskraft og påvirkningsmulighed over for børn og unge, særligt i skolestartsalderen. Derudover blev det fremhævet, at influenter, der driver erhvervsvirksomhed på sociale medier, skal overholde de særlige regler for markedsføring, der er rettet mod børn og unge.

Læs afgørelsen fra Forbrugerombudsmanden her: https://forbrugerombudsmanden.dk/find-sager/sager/markedsfoeringsloven/sager-efter-markedsfoeringsloven/boernog-unge/2406341-2406340-og-2406342-influenter-opfordrede-boern-til-koeb-i-opslag-paa-sociale-medier

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

Bird & Bird

Gunnar Hjalt

Verkligt bruk av EU-varumärke påverkar förväxlingsrisk även då tidsfristen för verkligt bruk ännu inte inträffat

Patent- och marknadsöverdomstolen (PMÖD) har kommit fram till att tre klädkedjors användning av beteckningen ATG i vissa utföranden, i samband med varuslaget kläder, inte inneburit intrång i det registrerade EU-varumärket nr 017942626 ATG, registrerat bland annat för varuslaget kläder. Vid tidpunkten för talans väckande var det aktuella EU-varumärket ATG yngre än fem år och alltså inte möjligt att angripa på grunden bristande användning. Detta påverkade inte att skyddet ändå blev urholkat av domstol.

PMÖD konstaterade initialt att EU-varumärket ATG kunde anses ha normal särskiljningsförmåga och att det förelåg varuslagsidentitet och hög märkeslikhet i förhållande till en viss cirkelfigur ATG (fig).

Däremot ansåg domstolen att vid beaktande av användningen av kännetecknen i den faktiska inköpssituationen kunde inte genomsnittskonsumenten uppfatta klädkollektionen som härrörande från innehavaren av EU-varumärket. Utgångspunkten här var inköpssituationen för genomsnittskonsumenter av svarandens produkter, vilken enligt domstolen var besök i en fysisk butik eller besök på en hemsida där det nästan uteslutande såldes kläder. Domstolen tog ingen hänsyn till att innehavaren av EU-varumärket ATG ännu hade tid till förfogande att starta försäljning av kläder märkta ATG i fysiska butiker eller på en hemsida. Möjligen hade det betydelse i målet att käranden i sina andra- och tredjehandsgrunder åberopat att vissa varumärken var föremål för hög kännedom och utökat skydd i Sverige och inom EU. Domstolen hade också bekräftat att kärandens varumärken ATG var kända för spel- och vadhållningstjänster, inom omsättningskretsen i Sverige.

Det synes vara en nackdel för en innehavare av ett känt varumärke att försöka bredda varumärket till nya produktområden. Den femåriga fristen att påbörja verkligt bruk kan under vissa omständigheter bli förkortad.

Se avgörandet i dess helhet här:
https://www.domstol.se/globalassets/filer/domstol/patentochmarknadsoverdomstolen/avgoranden/2024/pmt-2942-23.pdf

Gunnar Hjalt, Senior Counsel, Bird & Bird Advokat.


simonsen vogtwiig

Rune Ljostad og Henning Wahlberg

Hvordan utmåles vederlag for inngrep i databasevernet? Ny dom fra Borgarting lagmannsrett

Borgarting lagmannsrett avsa 11. november 2024 dom i sak mellom Konstali Helsenor AS (Helsenor) og Start Medical AS (Start Medical), samt to personer tilknyttet Start Medical. Det var tidligere avsagt deldom der det ble konstatert ansvarsgrunnlag, herunder at det forelå inngrep i databasevernet til Helsenor. Denne dommen gjaldt utmåling av kravet.

Sakens bakgrunn er at Helsenor og Start Medical var konkurrenter og drev med utleie av helsevikarer. Helsenor hadde utviklet en applikasjon med store mengder data med opplysninger om helsevikarer. Lagmannsretten hadde i deldommen funnet at Start Medical og de to personene hadde begått inngrep i databasevernet ved at 564 fullstendige vikarprofiler og rundt 19 000 e-postadresser ble trukket ut fra Helsenors database.

Databasevernet følger av åndsverkloven § 24 og innebærer at den som fremstiller en database får enerett til å råde over hele eller vesentlige deler av databasens innhold ved uttrekk eller gjenbruk av databasen. Ved inngrep i databasevernet har den forurettede krav på vederlag og/eller erstatning etter åndsverkloven § 81. Bestemmelsen gir krav på kompensasjon etter flere alternativer, avhengig av hva som er det gunstigste for rettighetshaver, herunder et rimelig vederlag for bruken samt erstatning for skade som ikke ville oppstått ved lisensiering, erstatning for økonomisk tap, eller vinningsavståelse. Det kan også tilkjennes det dobbelte av et rimelig vederlag dersom inngrepet er gjort forsettlig eller uaktsomt.

Helsenor argumenterte for at et rimelig vederlag skulle være 5 % av Start Medicals bruttoomsetning i perioden fra 5. august 2020, som var da dataene ble trukket ut, og frem til 1. november 2023, da dataene ble slettet. Bruttoomsetningen i perioden var ca. 164 millioner kroner, og et vederlag utgjør dermed ca. 8,2 millioner kroner. Videre argumenterte de for at motpartene hadde opptrådt forsettlig eller grovt uaktsomt og at det derfor var grunnlag for det dobbelte av et rimelig vederlag.

Start Medical mente kravet måtte settes vesentlig lavere, og viste til at bransjepraksis fra lisensiering av sammenlignbare databaser tilsier at vederlaget settes lavt. Videre viste de til at vederlaget må gjenspeile omfanget av bruken og at bruken av dataene var svært begrenset, som kun var brukt to ganger til masseutsendelse av e-post. Videre argumenterte de for at dersom vederlaget skulle beregnes som en prosentandel av omsetningen, kan ikke vederlaget utmåles basert på deres *totale* omsetning, men i stedet kun inntekter som står i årsakssammenheng med utnyttelsen.

Retten påpekte at Helsenor ikke hadde noen lisensieringspraksis som kunne tilsi hva et rimelig og markedsmessig vederlag er, og heller ikke fant retten at det forelå relevant og sammenlignbar bransjepraksis. Retten mente imidlertid at det var hensiktsmessig at vederlaget fastsettes som en prosentandel av inntektene som antas generert gjennom bruken av dataene, og viste til at en slik vederlagsmodell er relativt vanlig ved lisensiering. Retten var imidlertid ikke enig med Helsenor at vederlaget skulle baseres på Start Medicals samlede omsetning, fordi det ville innebåret at lisensvederlaget beregnes også på deler av Start Medicals inntekter som ikke har noe å gjøre med inngrepsdataene.

Etter bevisføringen anslo lagmannsretten skjønnsmessig at 65 % av de samlede inntektene i perioden 2020–2023 relaterer seg til helsevikarer som inngikk i inngrepsdataene fra Helsenor. 65 % av den samlede omsetningen i perioden var 105 millioner kroner, som derfor utgjorde beregningsgrunnlaget.

Deretter var spørsmålet hvor høy prosentandel av dette inntekts-

Illustrasjon: Colourbox.com

grunnlaget på 105 millioner kroner som skal utgjøre det rimelige vederlaget. Helsenor anførte at prosentsatsen skulle være 5 %, og viste til at denne satsen gjenfinnes i enkelte rettsavgjørelser om immaterielle rettigheter. Retten mente imidlertid at vederlaget i størst mulig grad må fastsettes på grunnlag av en konkret økonomisk analyse av rettighetenes verdi. Retten viste til at tilgang til helsevikarer er avgjørende for denne typen virksomhet, og at Helsenors database gjør det mulig å raskt finne frem til kandidater. Samtidig viste retten til at tilgang til data om helsevikarer i seg selv ikke er nok til å generere inntekter, og at andre innsatsfaktorer er nødvendig for å skape inntektene, slik som forhandling og avtaleinngåelse med den enkelte helsevikar. Retten påpeker også at Helsenors årsregnskap for perioden viser et årsoverskudd på rundt 5–6 % av den totale omsetningen, som tilsier at dersom Helsenor ikke hadde eid databasen og i stedet lisensiert tilgangen fra andre mot en lisensavgift på 5 % av omsetningen, ville Helsenors årsresultat ligget ned mot null. Retten mener dette indikerer at dataene ikke har en så stor verdi som det 5 % lisensavgift tilsier.

På bakgrunn av dette fastsatte retten skjønnsmessig at det rimelige vederlaget bør settes til 2,5 % av grunnlaget på 105 millioner kroner, altså 2,6 millioner kroner. Retten fant at inngrepet hadde vært dels forsettlig, og dels uaktsomt, og satte derfor vederlaget til det dobbelte av et rimelig vederlag jf. åndsverkloven § 81 andre ledd, totalt 5,2 millioner kroner.

Retten fant også at det forelå inngrep i Helsenors forretningshemmeligheter og brudd på markedsføringsloven § 25 om god forretningsskikk.

Saken er publisert i Lovdata under *LB-2022-91877-2*.

Rune Ljostad, advokat (H) og assosiert partner i Advokatfirmaet Simonsen Vogt Wiig AS og leder firmaets faggruppe for IP. Han har prosedert flere prinsipielle saker innen IP og personvern og Henning Wahlberg, advokat i Advokatfirmaet Simonsen Vogt Wiig AS.

Karolina Lehto

New standard terms and conditions for public ICT procurement contracts (JIT 2025) in Finland

History of standard terms and conditions for ICT procurement in Finland

There is a long tradition for public-sector standard terms and conditions for ICT procurement contracts in Finland. The terms and conditions have been published as recommendations since 1998 and they are widely used, thus forming a de facto market standard for ICT-related public procurement contracts. The terms and conditions have been updated in roughly 10-year intervals.

The General Terms and Conditions of Government Procurement of Information Technology (VYSE 1998) and the related Special Terms and Conditions were published in 1998. VYSE 1998 included Special Terms and Conditions for Procurements of Equipment (VLAE), for Procurements of Standard Software (VVOE), for Procurements of Customised Application Software (VTSE), for Equipment and Software Maintenance Services (VHYE), for Facilities Management Services (VKÄE) and for Consulting Services (VKOE).

VYSE 1998 terms and conditions were updated in a project launched by the Ministry of Finance in 2006. The new Terms and Conditions of Government IT Procurement were adopted as a recommendation on 8 October 2007, and they were named "JIT 2007". New Special Terms and Conditions for Services were introduced. Old VYSE 1998 Special Terms and Conditions for Equipment and Software Maintenance Services (VHYE) and the Special Terms and Conditions for Facilities Management Services (VKÄE) were abolished. As the previous VYSE 1998 had been mainly used by the government sector, JIT 2007 was directed to both government agencies and municipalities.

JIT terms and conditions were updated again in 2015, when Terms and Conditions of Public IT Procurement (JIT 2015) were published as a recommendation of the Advisory Committee on Information Management in Public Administration (JUHTA). JIT 2015 terms and conditions were more clearly than their predecessors directed to the whole public sector, including government agencies, bodies and funds, unincorporated state enterprises as well as municipalities and joint municipal authorities. The JIT 2015 recommendation included the General Terms and Conditions and eight sets of Special Terms and Conditions. Open-source software was emphasized as a relevant option for public sector applications. The previous JIT 2007 project terms were now divided into three appendices: Special Terms and Conditions for the Procurement of Client's Application under Open Source Software Terms (JIT 2015 – Client's Applications Open Source), Special Terms and Conditions for the Procurement of Client's Application under Software Terms Other than Open Source (JIT 2015 – Client's Applications Non-Open), and Special Terms and Conditions for Projects Implemented Using Agile Methods (JIT 2015 – Agile Methods). New Special Terms and Conditions for Services Delivered via a Data Network (JIT 2015 – Services via Network) were also introduced.

In addition to the terms and conditions, JIT 2015 also contained supporting material on open interfaces in information system or service procurement. This appendix was meant to help the contracting authorities to describe their requirements concerning open interfaces in more detail in the invitation to tender and in the agreement.

Later, in June 2018, Special Terms and Conditions for the Processing of Personal Data (JIT 2015

– Personal Data) were added to the JIT 2015 Terms and Conditions, taking into account the requirements of art. 28 of the EU General Data Protection Regulation (EU) 2016/679. Smaller modifications to the other Special Terms and Conditions, based on the GDPR, were made accordingly.

JIT 2025 terms and conditions

On March 8, 2024, the Ministry of Finance established a working group with a mission to update the JIT 2015 terms and conditions by the end of the year 2024. Like the previous JIT working groups, also this working group consisted of representatives widely from both government sector and municipalities as well as from the private sector. The working group's goal was to update the JIT terms to align with the current regulatory framework, particularly from the perspectives of the Finnish Information Management Act, the General Data Protection Regulation (GDPR), and sanctions legislation. Additionally, the terminology of the JIT terms and conditions was to be harmonized with the Finnish General Terms of Public Procurement in Service Contracts (JYSE Services) and in Supply Contracts (JYSE Supplies), when relevant. JYSE terms are directed for public procurement of other than ICT contracts.

The working group held 11 meetings and prepared the modifications to the JIT terms and conditions within the set time-limit. The new JIT 2025 terms and conditions were published on February 7, 2025. They are so far available in Finnish and in Swedish.

JIT 2025 consists of the following terms and conditions[1]:

- General Terms and Conditions
- Special Terms and Conditions for the Procurement of Client's Application under Open Source Software Terms
- Special Terms and Conditions for the Procurement of Client's Application under Software Terms Other than Open Source
- Special Terms and Conditions for Services
- Special Terms and Conditions for Consulting Services
- Special Terms and Conditions for Procurement of Hardware
- Special Terms and Conditions for Services Delivered via a Data Network
- Special Terms and Conditions for Procurement of Expert Work.

Illustrasjon: Colourbox.com

The earlier JIT 2015 Special Terms and Conditions for Projects Implemented Using Agile Methods were no longer much used, and they were therefore replaced by the new Special Terms and Conditions for Procurement of Expert Work. These terms are intended to be used when procuring IT expert services, for example, when acquiring software developers or project managers for the client's project. They are specifically intended for agile client projects where the results of the expert work are not based on solutions under the supplier's intellectual property rights, and the work is primarily carried out in the client's own application environment. The experts may, for example, work in a multi-supplier project. The new Special Terms and Conditions for Procurement of Expert Work are not meant to be used in project contracts where a specific agreed outcome is acquired from the supplier. The Special Terms and Conditions for the Procurement of Client's Application, which include a more waterfall-like project approach, are meant for those situations.

The main updates for the General Terms and Conditions include e.g. updates to the price modifications and billing terms, terms for situations where the supplier or its subcontractor is subject to sanctions, new terms regarding the supplier's duty to present proof on fulfilment of its employer obligations, and clarifications on how to calculate the contract value on which the damages are based on. Also, if the supplier has been found guilty of a prohibited restriction of competi-

1 Translation by author.

tion between undertakings as stipulated in the Competition Act in relation to the procurement contract in question, the supplier must pay penalty fees and damages to the client.

In the General Terms and Conditions and in the Special Terms and Conditions for Services, terms regarding service personnel's security clearances have been updated.

The Special Terms and Conditions for Procurement of Hardware have been updated to correspond better with the JYSE terms for procurements of goods, e.g. new clause setting requirements for the device characteristics has been introduced. Unless otherwise agreed, the device must be suitable for the purpose for which such devices are generally used or suitable for the specific purpose for which the device was intended to be used, if the supplier ought to have been aware of this purpose.

The Special Terms and Conditions for Services Delivered via a Data Network have been largely updated and modernised to be more suitable for procurement of software as a service (SaaS).

The JIT 2015 supporting material for requirements for open interfaces was abolished as outdated.

The JIT 2015 Special Terms and Conditions for the Processing of Personal Data was removed from JIT 2025, and it was replaced by two new documents, the JIT/JYSE Special Terms and Conditions for the Processing of Personal Data and the JIT/JYSE Description of the Processing Activities[2], which are common to both JIT and JYSE terms. These terms and conditions are no longer an attachment of JIT terms, nor JYSE terms, but instead independent documents which can be used in all procurement contracts regardless of whether the scope of procurement is ICT-related or not.

The new JIT 2025 General Terms and Conditions are publicly available on the Ministry of Finance's web pages. They will also be available for public hearing in Finnish and in Swedish later during the year 2025.

Senior legal counsel Karolina Lehto acted as a secretary for the JIT 2025 working group. She was also a member in both JIT 2007 and JIT 2015 working groups.

2 Translation by author.

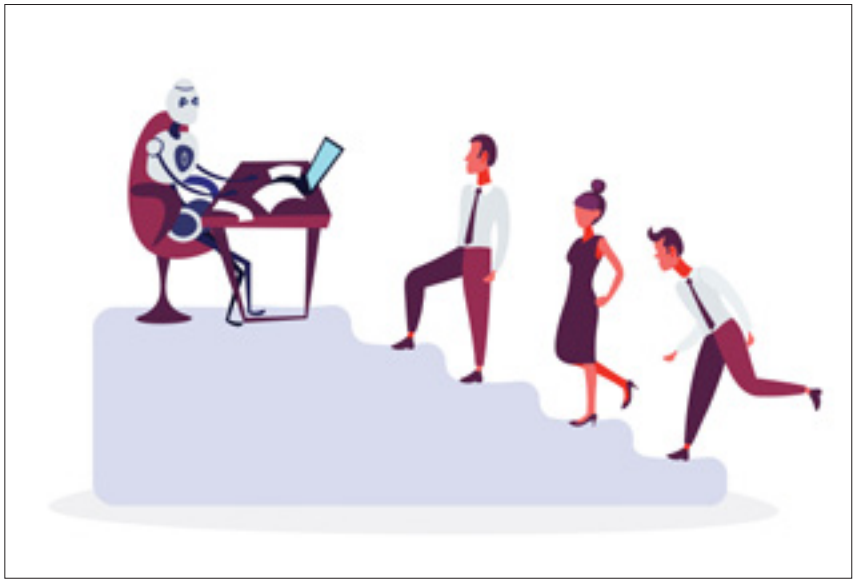
Wikström & PARTNERS

Anton Karlsson

AI för offentlig förvaltning – Riktlinjer för generativ AI

Myndigheten för Digital Förvaltning (”DIGG”) och Integritetsskyddsmyndigheten (”IMY”) har den 21 januari 2025 publicerat Riktlinjer för generativ AI inom offentlig förvaltning[1], som ska ge vägledning om hur generativ AI bör upphandlas och användas inom offentlig förvaltning, där syftet är att främja en säker, effektiv och etisk användning av generativ AI. Målgruppen för riktlinjerna är anställda och personer inom ledningsfunktioner, och särskilt i organisationer som befinner sig i en tidig fas av AI-mognaden. Riktlinjerna omfattar totalt 18 riktlinjer inom områdena Ledning och ansvar, Dataskydd och personuppgiftsbehandling (GDPR), Arbetssätt, Anskaffning, Informationssäkerhet, Upphovsrätt samt Etik.

Inom området Anskaffning har två riktlinjer tagits fram, Ta medvetna beslut om att skaffa generativ AI och Köp generativ AI enligt LOU, inom vilka viktiga frågor som verksamheter inom den offentliga förvaltningen bör beakta vid anskaffning av AI-verktyg lyfts. Det lyfts särskilt att avtalsfrågor och leverantörsvillkor bör studeras noggrant, och att det finns flera aspekter som är viktiga att ha i åtanke vid granskning och förhandling av avtalsvillkor, bland annat villkor avseende rätten till genererat material, ansvarsbegränsningar, behandling av personuppgifter, informationssäkerhet, och tvister och uppsägning.



Illustrasjon: Colourbox.com

Riktlinjerna begränsar sig till vägledning avseende användningen av existerande generativa AI-system, och omfattar inte vägledning avseende utveckling av nya grundmodeller eller finjustering av befintliga grundmodeller. Mot bakgrund av den snabba utvecklingstakten vad avser generativ AI, kommer riktlinjerna utvecklas och uppdateras kontinuerligt.

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

1 *https://www.digg.se/ai-for-offentlig-forvaltning/riktlinjer-for-generativ-ai.*


Selmer
Jennifer Parmlind og Anne-Marit Wang

EUs nye produktansvarsdirektiv: større ansvar for teknologiaktører

Den 8. desember 2024 trådte det nye produktansvarsdirektivet (EU 2024/2853) i kraft, og erstatter det tidligere direktivet fra 1985 (85/374/EEC). Den teknologiske utviklingen har gjort det helt nødvendig å modernisere det over 40 år gamle regelverket. Det nye direktivet utvider blant annet det objektive ansvaret for personskader og skader på eiendom ved å omfatte sikkerhetsmangler i programvare, inkludert AI-systemer. Samtidig innføres det blant annet nye regler som reduserer bevisbyrden for skadelidte i saker som involverer teknologisk og vitenskapelig komplekse produkter. Det nye direktivet innebærer et betydelig større ansvar for produsenter av denne typen produkter.

Direktivet gjelder for produkter som gjøres tilgjengelige på markedet eller tas i bruk etter 9. desember 2026. «Tilgjengelig på markedet» gjelder også produkter som tilbys gratis. Det tidligere direktivet vil fortsatt gjelde for produkter som ble gjort tilgjengelige på markedet eller tatt i bruk før denne datoen.

Direktivet innebærer fullharmonisering, og medlemsstatene kan derfor ikke, med mindre annet angis særlig, innføre verken strengere eller lempeligere regler innenfor de områdene som direktivet behandler. Selv om det ennå er usikkert om og når direktivet vil bli implementert i norsk rett, er det merket som EØS-relevant, noe som indikerer fremtidig innlemmelse.

Artikkelen vil gjennomgå noen utvalgte nyheter i det nye produktansvarsdirektivet som får særlig relevans for teknologiaktører.

1. Utvidelse av produktdefinisjonen

Fysiske personer kan kreve erstatning for skader som forårsakes av *produkter* med sikkerhetsmangler. Det nye direktivet presiserer at programvare, inkludert operativsystemer, firmware, dataprogrammer, applikasjoner og AI-systemer, nå regnes som produkter.[1] Det presiseres i fortalen punkt 13 at dette gjelder uavhengig av hvordan programvaren leveres eller brukes, enten den er lagret på en enhet, tilgjengelig via et kommunikasjonsnettverk eller levert som en tjeneste (SaaS).

Det digitale innholdet i for eksempel en e-bok faller utenfor direktivets virkeområde. Derimot anses digitale produksjonsfiler, som brukes til å fremstille fysiske gjenstander ved å muliggjøre automatisk styring av maskiner eller verktøy, som produkter.[2] I fortalens punkt 16 gis det som eksempel at en CAD-fil med sikkerhetsmangler, som brukes til å lage et 3D-printet produkt som forårsaker skade, kan føre til erstatningsansvar.

Programvare med fri og åpen kildekode (open source) omfattes ikke av direktivet dersom den utvikles eller formidles utenfor en kommersiell kontekst.[3] Dette innebærer at utvikleren av slik ikke-kommersielt distribuert programvare ikke kan holdes ansvarlig ved sikkerhetsmangler. Det følger av fortalens punkt 15 at dersom åpen kildekode senere integreres i et kommersielt produkt, kan produsenten av det endelige produktet imidlertid holdes ansvarlig for eventuelle sikkerhetsmangler som forårsaker skade. Hvordan dette vil påvirke den relativt utbredte bruken av open source vil gjenstå å se.

Videre omfattes nå også digitale tjenester som er integrert i eller tilknyttet et produkt på en måte som er avgjørende for dets funksjonalitet og sikkerhet, som etter fortalens punkt 17 eksempelvis kan være kontinuerlig tilførsel av trafikkdata i navigasjonssystemer eller temperaturkontrolltjenester som overvåker og regulerer temperaturen i et smart kjøleskap.[4] Ansvaret er likevel begrenset til tilfeller der slike tjenester er innenfor produsentens kontroll,

1 Artikkel 4(1).
2 Artikkel 4(1) og 4(2).
3 Artikkel 2(2).
4 Artikkel 4(3) og artikkel 11(2)(a).

det vil si at produsenten enten selv utfører eksempelvis integrering, eller gir samtykke eller tillatelse til at en tredjepart utfører dette.

2. Utvidelse av begrepet sikkerhetsmangler

Et produkt skal anses å ha en sikkerhetsmangel dersom det ikke gir den sikkerheten en person har rett til å forvente, eller som kreves i henhold til EU-retten eller nasjonal lovgivning.[5] Ved vurderingen av om et produkt har en sikkerhetsmangel skal alle relevante faktorer fortsatt tas i betraktning.

Direktivet har flere nye spesifiseringer av faktorer som skal inngå i denne vurderingen.[6] Blant annet skal det tas hensyn til hvordan produktet påvirkes av andre produkter det med rimelighet kan forventes å brukes sammen med, for eksempel innenfor et smart-hjem-system.

Det skal også tas hensyn til produkters evne til å lære eller tilegne seg nye funksjoner. Ifølge fortalens punkt 32 reflekterer dette forbrukernes berettigede forventning om at programvare og underliggende algoritmer er utformet for å forhindre skadelig atferd. En produsent som utvikler et produkt, slik som et AI-system, med potensial for uforutsett atferd, kan derfor forbli ansvarlig for skader som oppstår som følge av dette.

Produsenter er som regel unntatt fra ansvar dersom de kan bevise at det er sannsynlig at sikkerhetsmangelen som forårsaket skaden, ikke eksisterte da produktet ble plassert på markedet eller tatt i bruk.[7] Dagens teknologi gjør det imidlertid mulig for produsenter å utøve kontroll utover dette tidspunktet. Det nye direktivet fastslår derfor at produsenter fortsatt vil være ansvarlige for defekter som oppstår etter dette tidspunktet som følge av programvare eller relaterte tjenester under deres kontroll, enten det gjelder oppdateringer, oppgraderinger eller maskinlæringsalgoritmer.[8] Dersom en produsent, eller en tredjepart i samarbeid med produsenten, leverer en oppdatering som introduserer en sikkerhetsmangel, kan produsenten altså holdes ansvarlige for skader, selv om produktet var trygt ved lansering. Samtidig følger det av fortalen punkt 32 at et produkt kan anses å ha en sikkerhetsmangel hvis det blir ansett for å være sårbart mot cyberangrep. Produsenter av produkter kan altså med dette holdes ansvarlige både for oppdateringer av produktet, og for skader som har oppstått på grunn av manglende nødvendige oppdateringer av produktet. Dette er en betydelig utvidelse av produktansvaret.

Produsentens presentasjon av produktet kan ha betydning for sikkerhetsvurderingen, men det presiseres i fortalens punkt 31 at advarsler alene er ikke tilstrekkelig for å frita produsenten for ansvar. En produsent kan derfor ikke unngå erstatningsansvar kun ved å opplyse om mulige risikoer. En produsent vil fortsatt kunne holdes ansvarlig dersom produktet ikke lever opp til allmenne sikkerhetsforventninger, uavhengig av eventuelle opplysninger om risikoer.

3. Ansvar for nye aktører i leveransekjeden

Som tidligere har produsenten hovedansvaret, men det nye direktivet presiserer samtidig at produsenter av komponenter også kan holdes ansvarlige dersom de har kontroll over integrasjonen av komponenten eller dersom komponenten i seg selv utgjør et produkt.[9]

Begrepet produsent omfatter fortsatt enhver som, direkte eller via en tredjepart, setter sitt navn, varemerke eller kjennetegn på produktet og dermed fremstår som involvert i produksjonen.[10] Dette innebærer at EU-domstolens dom i sak C-157/23 trolig vil forbli relevant også under det nye direktivet. I den aktuelle saken kom EU-domstolen frem til at leverandører med lignende navn som produsenten eller produktet kan holdes ansvarlig, som om de faktisk har produsert produktet. Leverandører kan dermed ikke høres med at de ikke er ansvarlige for sikkerhetsmangler fordi de ikke har vært involvert i produksjonen. Avgjørelsen støtter på denne måten opp under prinsippet om å styrke forbrukervernet, som er en av kongstankene bak direktivet.

Fysiske personers vern styrkes ved at det alltid skal finnes en ansvarlig aktør i EU. Importører, autoriserte representanter for produsenter utenfor EU og tilbydere av distribusjonstjenester (fulfilment service providers) holdes ansvarlige dersom det ikke finnes en importør eller representant i EU.[11] Fortalens punkt 37 understreker at distribusjonstjenester spiller en stadig viktigere rolle i forsyningskjeden ved å muliggjøre import fra tredjeland. De kan utføre oppgaver som minner om importørens, men faller ikke nødvendigvis inn under den tradisjonelle definisjonen. Slik tjenesteytere omfattes dersom de tilbyr minst to av følgende tjenester: lagring, emballering, adressering eller forsendelse av et produkt uten å ha eierskap over det. Posttjenester og godstransporttjenester er unntatt.[12]

Distributørens ansvar trer, som kjent fra tidligere, i kraft dersom ingen av de andre ansvarlige aktørene kan identifiseres. I slike tilfeller blir distributøren ansvarlig dersom den skadelidte ber distributøren om å identifisere en ansvarlig aktør i EU, eller sin egen distributør. Dersom distributøren ikke gir denne informasjonen innen én måned (tidligere rimelig tid), vil ansvaret for

5 Artikkel 7(1).
6 Artikkel 7(2).
7 Artikkel 11(1)(c).
8 Artikkel 11(2).
9 Artikkel 8(1)(a) og 8(1)(b).
10 Artikkel 4(10)(b).
11 Artikkel 8(1)(c).
12 Artikkel 4(13).

produktets sikkerhetsmangler overføres til distributøren.[13] På samme måte kan leverandører av onlineplattformer holdes ansvarlige dersom de presenterer produkter eller muliggjør transaksjoner på en måte som gir inntrykk av at de selv, eller en næringsdrivende under deres kontroll, står bak salget.[14]

En annen nyhet er at dersom et produkt endres vesentlig og deretter gjøres tilgjengelig på markedet eller tas i bruk, skal det anses det som et nytt produkt. Dette omfatter også programvareoppdateringer, oppgraderinger og den kontinuerlige læringen til AI-systemer. Der lovgivningen ikke angir nærmere kriterier, anses endringer som vesentlige dersom de endrer produktets opprinnelige ytelse, formål eller type uten at dette var forutsett i produsentens opprinnelige risikovurdering, eller dersom de endrer risikonivået.[15] Hvis endringen skjer utenfor produsentens kontroll, blir den som har foretatt modifikasjonen ansvarlig.[16] For å sikre en rettferdig risikofordeling i en sirkulær økonomi, kan de som gjør vesentlige endringer fritas dersom de kan bevise at skaden skyldes en del av produktet som ikke ble berørt av endringen.[17]

4. Utvidede erstatningsmuligheter

Som tidligere, kan det kreves erstatning for personskader og skade på eiendom. Direktivet anerkjenner imidlertid nå personskade i form av psykisk skade, forutsatt at den er medisinsk anerkjent og dokumentert.[18] I tillegg omfatter det skade som oppstår ved ødeleggelse eller tap av data, for eksempel sletting av digitale filer som ikke kan gjenopprettes.[19] Denne endringen får konsekvenser for blant annet teknologiselskaper som lagrer eller behandler sensitiv informasjon og data. Data som brukes i kommersiell sammenheng er unntatt fra direktivet, også der privat bruk ikke kan utelukkes. Dette er i tråd med det forrige direktivet der skade på ting brukt i en kommersiell sammenheng ikke erstattes. Det er opp til hvert land å fastsette hvordan erstatningen beregnes.

Videre inneholder det nye direktivet ikke lenger noen fradragsgrenser, noe som altså i utgangspunktet innebærer en rett til å få dekket hele det økonomiske tapet.

5. Lettelser i Bevisbyrde for skadelidte

Direktivet viderefører prinsippet om at aktørene har ansvar uavhengig av skyld (culpa). For å sikre en rettferdig risikofordeling må skadelidte fortsatt bevise skaden, produktets sikkerhetsmangel og årsakssammenhengen mellom disse.

Det har imidlertid vist seg å være utfordrende å bevise at et produkt er defekt, spesielt ettersom den teknologiske utviklingen har gjort innhenting og vurdering av bevis mer komplisert. Direktivet har derfor innført mekanismer som forenkler prosessen med å kreve erstatning, særlig i saker som involverer teknisk komplekse produkter.

Skadelidte har ofte begrenset tilgang til informasjon om hvordan et produkt er konstruert og fungerer, mens produsentene har betydelig kunnskap og kontroll over denne informasjonen. For å balansere dette gir direktivet skadelidte forbedret tilgang til bevismateriale. Skadelidte som har fremlagt tilstrekkelige fakta og bevis for å underbygge rimeligheten av sitt erstatningskrav, kan be om at det utleveres relevant bevismateriale.[20] Domstolen kan også kreve at slik bevisføring presenteres på en lett tilgjengelig og forståelig måte, noe som er særlig viktig i saker med høy teknisk kompleksitet.[21] Dette vil få konsekvenser for produsenter av særlig tekniske produkter, som vil måtte utarbeide dokumentasjon som på en forståelig måte dokumenterer produktets sikkerhet.

Samtidig pålegger direktivet domstolene å begrense bevisinnhentingen til det som er nødvendig og forholdsmessig, blant annet for å unngå omfattende søk som inkluderer irrelevant informasjon.[22] I tillegg må tiltak iverksettes for å beskytte konfidensiell informasjon, inkludert forretningshemmeligheter.[23] Dette kan innebære begrenset tilgang til dokumenter, redigerte versjoner av bevismateriale eller lukkede rettsmøter for å sikre at sensitiv informasjon ikke blir offentliggjort.

For å redusere bevisbyrden for skadelidte etablerer direktivet visse presumsjoner.[24] Dersom saksøkte unnlater å fremlegge bevis, eller hvis produktet ikke oppfyller obligatoriske sikkerhetskrav fastsatt i EU- eller nasjonal lovgivning, skal det anses som sannsynlig at produktet har en sikkerhetsmangel. Det samme gjelder dersom produktet har åpenbare funksjonsfeil under normal eller rimelig forutsigbar bruk. Videre skal det presumeres at det foreligger en årsakssammenheng mellom produktets sikkerhetsmangel og skaden dersom det er fastslått at produktet har en sikkerhetsmangel, og den påførte skaden typisk samsvarer med slike feil.

I særlig teknisk komplekse saker, for eksempel produkter som benytter AI eller avansert maskinlæring, inkludert den så kalte black box-problematikken, gir direktivet domstolen adgang til å legge til grunn en presumsjon om at et produkt har en sikkerhetsmangel og/eller at det foreligger en årsakssammenheng. Dette gjelder der den skadelidte står overfor urimelig store vanskeligheter med å oppfylle bevisbyrden som

13 Artikkel 8(3).
14 Artikkel 8(4).
15 Artikkel 4(18).
16 Artikkel 8(2).
17 Artikkel 11(1)(g).
18 Artikkel 6(1)(a).
19 Artikkel 6(1)(c).
20 Artikkel 9(1).
21 Artikkel 9(6).
22 Artikkel 9(3).
23 Artikkel 9(5).
24 Artikkel 10(2), 10(3) and 10(4).

Illustrasjon: Colourbox.com

følge av sakens tekniske eller vitenskapelige kompleksitet og der den skadeliste i det minste kan vise til at det er sannsynlig at produktet har en sikkerhetsmangel og/eller at det foreligger en årsakssammenheng.

Den saksøkte har mulighet til å motbevise disse presumsjonene. I tillegg har den saksøkte en tilsvarende rett til å få tilgang til relevant informasjon som skadelidte besitter, for å kunne forsvare seg effektivt.[25]

6. Forlenget ansvarsperiode

Direktivet viderefører fristen på ti år for ansvar, regnet fra den dagen produktet ble gjort tilgjengelig på markedet eller tatt i bruk.[26] Dersom produktet gjennomgår en vesentlig endring, løper en ny tiårsperiode.[27] Produsentene og andre som gjør vesentlige endringer kan derfor holdes til ansvar over en lengre periode enn tidligere. Oppdateringer og oppgraderinger som ikke regnes som en vesentlig endring, vil ikke trigge en ny tiårsperiode.

Ved helseproblemer som utvikler seg sakte, er ansvarsperioden utvidet til 25 år.[28]

Jennifer Parmlind, Senior Associate i Advokatfirmaet Selmer, arbeider særlig med teknologi og immaterielle rettigheter.

Anne-Marit Wang, partner i Advokatfirmaet Selmer.

25 Artikkel 9(2).

26 Artikkel 17(1)(a).

27 Artikkel 17(1)(b).

28 Artikkel 17(2).

LOVDATA

Produksjon: Aksell AS