

KOMMUNAL- OG
DISTRIKTSDEPARTEMENTET
Postboks 8112 DEP
0032 OSLO

Deres referanse

Vår referanse
22/05459-3

Dato
10.02.2023

Høringsuttalelse – NOU 2022:11 Ditt personvern – vårt felles ansvar

1. Innledning

Vi viser til høringsbrevet av 11. november 2022, med invitasjon til å komme med høringsuttalelse til Personvernkommisjonens utredning, NOU 2022:11 Ditt personvern – vårt felles ansvar.

Personvernkommisjonen har levert en grundig, god og viktig utredning. Vi håper derfor at NOU-en vil bli fulgt opp med konkrete tiltak som kan styrke personvernet, både for enkeltindividet og for samfunnet i sin helhet.

Datatilsynet syns det er svært positivt at NOU-en setter personvern på dagsordenen og ønsker spesielt å vise til at kommisjonen etterlyser en nasjonal personvernpolitikk. Vi har også merket oss at kommisjonen trekker frem den gjennomgående tendensen til at digitaliseringen skjer på bekostning av personvernet, noe som etter tilsynets oppfatning underbygger viktigheten av et styrket datatilsyn i Norge.

I tillegg til behovet for en nasjonal personvernpolitikk, ønsker vi spesielt å trekke frem tre områder hvor vi mener det er særlig viktig med snarlig oppfølging og handling:

- Personvern i skolene og barnehagene
- Utredning av et forbud mot atferdsbasert markedsføring
- Styrking av Datatilsynet

Godt personvern er viktig i alle sektorer. I dette høringssvaret har vi først og fremst valgt å kommentere de anbefalingene i NOU-en vi mener kan ha størst positiv effekt for personvernet.

Vi tillater oss å peke på at viktige områder innen forsvars- og justissektoren dessverre ikke har blitt innfortolket som en del av Personvernkomisjonens mandat. Dette gjør at vi nå ikke får en nødvendig diskusjon om for eksempel overvåkningstiltak i regi av de hemmelige tjenestene, tilrettelagt innhenting av kommunikasjonsdata, lagring av IP-adresser, overvåking av flypassasjerer og innhenting av personinformasjon fra åpne kilder.

De seneste årene har vi sett en rekke ulike initiativer som har skullet legge til rette for innhenting og lagring av personopplysninger fra digitale kilder i stor skala. Det dreier seg om tiltak som kan virke svært inngripende, og som kan ha stor innvirkning på personvernet til folk flest. Vi har flere ganger pekt på at tiltakene som er foreslått har vært i strid med grunnleggende menneskerettigheter, og at konsekvensene ved å innføre tiltakene er mangelfullt utredet. Internasjonale domstoler har også konkludert med det samme i lignende saker i andre land vi normalt sammenligner oss med.

Vi mener at en analyse av den samlede situasjonen for vårt kollektive personvern blir ufullstendig uten en gjennomgang av de initiativene som er tatt i forsvars- og justissektoren.

2. Datatilsynets merknader

2.1 Hva er personvern, rettslig rammeverk og teknologiske drivkrefter – en nasjonal personvernpolitikk

Utredningens innledende kapittel og første del tegner et bilde av en digitaliseringsprosess som i stor grad har skjedd på bekostning av personvernet. Kommisjonen foreslår en nasjonal personvernpolitikk for å legge føringer for digitaliseringen av samfunnet, i tillegg til det som følger av lovgivningen. En slik politikk vil kreve at personvern i større grad løftes ut av ekspertsirkelene og gjøres til et relevant og viktig spørsmål i samfunnsdebatten, i kommunestyre og på Stortinget. Kommisjonen foreslår at regjeringen legger frem en personvernpolitisk redegjørelse for Stortinget årlig, forankret i gjeldende personvernpolitikk. Vi mener at en nasjonal personvernpolitikk er nødvendig, og vi støtter anbefalingen.

Kommisjonen skriver at en nasjonal personvernpolitikk må se personvernet i et helhetlig perspektiv. Kommisjonen peker også på at det i dag ikke finnes noen offentlig virksomhet med et overordnet ansvar for å vurdere den samlede bruken av personopplysninger i offentlig forvaltning. Dette fører, ifølge kommisjonen, til at det er svært vanskelig å vurdere den samlede effekten av potensielt inngripende tjenester, tiltak eller lovendringer. Dette er utfordringer Datatilsynet har pekt på i flere sammenhenger og vi er enige i at utfordringen fortjener å løftes opp på det rikspolitiske nivået.

Videre peker kommisjonen på at en nasjonal personvernpolitikk må fremme personvernvennlig innovasjon. Datatilsynet har gjennom flere år arbeidet strategisk for dette, blant annet gjennom den regulatoriske sandkassen for kunstig intelligens og med veiledningen vår om programvareutvikling med innebygd personvern.

Vi støtter derfor opp under forslaget. At offentlig sektor bør gå foran, blant annet ved å bruke sin betydelige innkjøpsmakt for å stimulere til fremveksten av personvernvennlige produkter og tjenester, er likeledes et forslag vi stiller oss bak.

I kapittel 5 redegjør kommisjonen for teknologiske utviklingstrekk med betydning for personvernet. Kommisjonen støtter et generelt forbud mot biometrisk fjernidentifikasjon i det offentlige rom, for eksempel ansiktsgjenkjenningsteknologi. Et slikt forbud er tatt inn i forslaget til forordning om harmoniserte regler for kunstig intelligens i EU («AI Act»).

Vi anbefaler et generelt forbud, og vi støtter også Personvernkommisjonens anbefaling om at norske myndigheter bør arbeide opp mot EU for å få gjennomført et forbud.

Vi støtter også den mer generelle anbefalingen i kapittel 5 om at føre-var-prinsippet bør gjelde når «teknologi med særlig høy risiko for personvernet vurderes innført».

2.2 Personvern i den digitale forvaltningen

I kapittel 6 gjennomgår kommisjonen personvernets stilling i den digitale forvaltningen. Datatilsynet mener kommisjonen trekker frem viktige forhold knyttet til digitaliseringen av offentlig sektor og utfordringer dette kan medføre for personvernet.

Vi støtter anbefalingene kommisjonen foreslår. Under vil vi komme med noen utdypende kommentarer.

Offentlige myndigheters behandling av personopplysninger – deling og viderebruk

Kommisjonen gir en grundig gjennomgang av de menneskerettslige og personvernrettslige kravene til offentlige myndigheters behandling av personopplysninger.

Vi mener det er viktig å løfte frem disse overordnede perspektivene i diskusjoner om personvern i det offentlige Norge.

Kommisjonen angir at det er behov for sterkere parlamentarisk kontroll med ny lovgivning som påvirker innbyggernes personvern. Dette forutsetter at Stortinget settes i stand til å gjøre gode vurderinger, blant annet ved at personvernkonsekvensene av lovforslag er synliggjort på en grundigere og mer balansert måte. På den måten vil Stortinget få best mulig forutsetninger for å gjøre gode avveininger og verdivalg. Vi støtter også målsettingen om økt personvernkompetanse i forvaltningen, særlig i forbindelse med regelverksarbeid.

Videre legger kommisjonen til grunn at en ordinær høringsrunde i forbindelse med utarbeidelse av lovgivning ikke er tilstrekkelig til å ivareta rådføringsplikten som fremgår av personvernforordningen artikkel 36 nr. 4. Ikke bare er det et lovfestet krav, det vil også være formålstjenlig og fornuftig å involvere Datatilsynet tidligere i mange regelverksprosesser. Vi er derfor helt enige i anbefalingen om at det bør utredes om rådføringsplikten etterleves i tilstrekkelig grad i dag.

Kommisjonen anbefaler å etablere et frittstående og rådgivende organ som har overordnet ansvar for å se offentlige digitaliseringstiltak og lovgivningen i sammenheng på tvers av sektorer. Vi mener at en slik koordinering vil kunne være et godt tiltak for å sikre helhetlig ivaretagelse av personvernet i offentlig sektor. Vi stiller oss også bak forslaget om større grad av sentraliserte anbefalinger og krav til IKT-sikkerheten i det offentlige.

Kommisjonen anbefaler at man i større grad gjør bruk av muligheten til å lov- eller forskriftsfeste ansvarsforholdene der opplysninger skal deles på tvers av offentlige myndigheter. Datatilsynet deler kommisjonens oppfatning. Økt bruk av lov- og forskriftshjemler for å plassere ansvar vil være et viktig tiltak for å sikre ivaretagelse av de registrertes rettigheter og forhindre ansvarspulverisering.

Vi ser positivt på kommisjonens anbefaling om å utforske hvorvidt tekniske løsninger for deling av informasjon mellom offentlige organer også kan benyttes til å øke graden av samtykkebasert deling. En slik tilnærming vil styrke innbyggernes kontroll over egne personopplysninger. Samtidig vil offentlige myndigheters behov for tilgang til informasjon om den enkelte innbygger ivaretas.

Kommisjonen har pekt på «kun én gang»-prinsippet, som ligger til grunn for digitaliseringen av offentlig sektor. Det er en forventning hos mange innbyggere at personopplysninger man har delt med det offentlige er tilgjengelige for relevante myndigheter. Dette er et viktig hensyn bak dagens digitaliseringsstrategi.

En slik tilnærming forutsetter likevel gode mekanismer for å kunne følge opp opplysningenes korrekthet. Deling og bruk av feilaktige opplysninger kan få alvorlige konsekvenser for enkeltpersoner. Det har vi erfart i vårt tilsynsarbeid, for eksempel gjennom saker der personer feilaktig har blitt registrert som døde i Folkeregisteret.

Vi ser positivt på at kommisjonen har løftet frem underretningsplikten den behandlingsansvarlige har etter personvernforordningen artikkel 19. En riktig praktisert underretningsplikt vil være et viktig virkemiddel for å hindre at ikke-korrekte personopplysninger spres og brukes videre til nye formål.

Automatisering av beslutningsprosesser

Datatilsynet stiller seg bak kommisjonens vurderinger av fordelene og ulempene ved automatiserte beslutningsprosesser og beslutningsstøtteverktøy. Hensynet til likebehandling, transparens, forutberegnelighet og effektivitet kan bli bedre ivaretatt, mens bruk av feilaktig informasjon, feiltolking av lovverket og manglende forvaltningsskjønn i automatiserte prosesser kan få store konsekvenser. Særlig vil menneskelig inngripen være et viktig tiltak for å unngå disse fallgruvne.

Datatilsynet mener det er gode grunner til å følge tett med på utviklingen når stadig mer komplekse avgjørelser forventes å skulle fattes ved hjelp av, eller i sin helhet av, automatiserte beslutningssystemer. Vi støtter kommisjonens anbefaling om størst mulig grad av lovregulering av offentlige automatiseringstiltak.

Profilering

Datatilsynet deler kommisjonens vurdering av at profilering til kontrollformål alltid bør anses som en inngripende behandling av personopplysninger. Selv om profilering av innbyggere kan medvirke til målrettet og effektiv utøvelse av forvaltningens oppgaver, medfører det samtidig en iboende stor risiko for urimelig forskjellsbehandling eller diskriminering. Det er

liten tvil om at dette på lengre sikt kan føre til nedkjølingseffekter i befolkningen, slik også kommisjonen peker på.

2.3 Personvern i justissektoren

Datatilsynet mener kommisjonen trekker frem sentrale utfordringer i justissektoren og støtter i all hovedsak de foreslåtte anbefalingene i utredningens kapittel 7. Vi vil nedenfor kommentere enkelte utfordringer og anbefalinger.

Datatilsynet merker seg at kommisjonen har hatt utfordringer med å få innsikt i politiets metodebruk og verktøy. Kommisjonen ser det som problematisk at det er begrenset offentlig informasjon tilgjengelig om hvilke verktøy politiet anvender i dag eller vurderer å anvende i fremtiden. Dette gjør det vanskelig å vurdere personvernkonsekvenser ved metodebruken. Datatilsynet slutter seg til dette.

Rettslig regulering av personvern i justissektoren – Kriminalomsorgen

Personvernkommisjonen mener Justis- og beredskapsdepartementet i arbeidet med ny lovregulering knyttet til straffegjennomføring bør tydeliggjøre behandlingsansvaret i kriminalomsorgen og anbefaler å legge ansvaret til den virksomheten som utfører den faktiske behandlingen av personopplysninger.

Datatilsynet er enig i at plasseringen av behandlingsansvaret i Kriminalomsorgen har vært uklar. I 2022 gjennomførte vi et tilsyn med kriminalomsorgen ved Kriminalomsorgsdirektoratet (KDI) og tre underliggende enheter. Gjennom tilsynet ble det funnet avvik fra regelverkets krav til ansvars plassering og styringssystem for personvern og informasjonssikkerhet. I løpet av tilsynsperioden utarbeidet KDI en instruks som plasserer behandlingsansvaret hos direktoratet. Datatilsynet mener dette er en god løsning.

Vi støtter derfor *ikke* kommisjonens anbefaling på dette punktet. Kommisjonens anbefaling er heller ikke nærmere begrunnet. I etterkant av det nevnte tilsynet har Datatilsynet også tatt opp behovet for å få på plass nytt regelverk i brev til Justis- og beredskapsdepartementet. Vi mener det er uheldig at dette arbeidet har tatt tid.

Utviklingstrekk som påvirker personvernet – økt internasjonalt samarbeid

Datatilsynet bemerker at Schengen-samarbeidet ikke er omtalt i rapporten. Etter vårt syn er dette temaet helt sentralt når det gjelder personvern innen justissektoren og utlendingsforvaltningen.

Avtalen om Schengen-samarbeidet gir Norge rett og plikt til å anvende hele Schengen-regelverket, herunder bestemmelser om informasjonsutveksling og bruk av felleseuropeiske systemer. Som nasjonal tilsynsmyndighet har Datatilsynet tilsyns- og kontrolloppgaver knyttet til norske myndigheters bruk av de felleseuropeiske informasjonssystemene Schengen informasjonssystem (SIS), Visuminformasjonssystemet VIS og fingeravtrykksregisteret Eurodac.

Videreutviklingen av Schengen-samarbeidet har store personvernmessige konsekvenser. For å styrke Schengen-samarbeidet er det vedtatt en rekke nye rettsakter som vil tre i kraft i tiden fremover. Dette innebærer at det gjøres endringer i eksisterende informasjonssystemer og at det innføres nye informasjonssystemer. En gjennomgående trend er at det legges opp til å behandle flere personopplysninger for flere formål, med en tettere integrasjon mellom systemer. Det åpnes også for tilgang til rettshåndhevende myndigheter for politimessige formål (sekundærbruk). Dette er en utvikling Datatilsynet er opptatt av å følge med på.

Personvernutfordringer i justissektoren – personvern i lovarbeid

Kommisjonen påpeker at det ved innføring av nye tiltak er avgjørende at eventuelle personvernkonsekvenser blir tilstrekkelig belyst og vurdert i forkant. Kommisjonen har observert at lovgivers vurderinger av personvernkonsekvenser kan være begrensede og mangelfulle i forbindelse med lov- og forskriftsforslag. Datatilsynet er av samme oppfatning. Vi viser i den forbindelse til bestemmelsene om forhåndskonsultasjon i personvernforordningen art. 36 nr. 4 og tilsvarende bestemmelse i direktiv (EU) 2016/680 om beskyttelse av fysiske personer ved behandling av personopplysninger for å forebygge, etterforske, avdekke eller straffeforfølge lovbrudd eller gjennomføring av straffereaksjoner, og om fri utveksling av slike opplysninger (LED) artikkel 28 nr. 2.

Vår erfaring så langt er at forhåndskonsultasjon i liten grad har blitt benyttet innen justissektoren og at våre synspunkter i hovedsak innhentes gjennom etterfølgende høringer. Datatilsynet ønsker å bli involvert tidligere i regelverksprosesser.

Vi støtter derfor anbefalingen om at departementene i større grad bør rådføre seg med Datatilsynet i forbindelse med lov- og forskriftsarbeid. Vi vil understreke at vi i kraft av vår ombudsrolle er opptatt av å ivareta personvern hensyn innenfor hele justissektoren, også på områder som er unntatt fra vår tilsynsmyndighet etter politiregisterloven.

Vi har for øvrig merket oss kommisjonens uttalelser i utredningens avsnitt 7.1.2:

«I en god rettsstat må verdier og kryssende hensyn veies mot hverandre. Hvordan og hvor grundig man utfører en slik interesseavveining, på både systemnivå og i hver enkelt sak, sier noe om rettsstatens kvalitet. I merknadene til politiregisterloven § 1 (lovens formål) heter det: «I de tilfellene der hensynet til personvern og hensynet til kriminalitetsbekjempelsen ikke kan forenes, er utgangspunktet at hensynet til personvernet må vike.» Denne betraktningen, om at bekjempelse av kriminalitet har forrang ved en konflikt med personvernet – selv om det i forarbeidene gis anvisning på en forholdsmessighetsvurdering – er kommisjonen ikke enig i. Hvordan ulike interesser vektet, vil være avgjørende for hvilken løsning som velges. Når interesser står mot hverandre, kan ikke utgangspunktet være at personvernet alltid må vike. Dersom personvern krenkelsen som følge av et tiltak er tilstrekkelig alvorlig, må konklusjonen etter Personvernkommisjonens oppfatning være den motsatte; kriminalitetsbekjempelsen skal vike.»

Disse uttalelsene er viktige og klargjørende, og vil kunne bidra til mer nyanserte avveininger i tiden som kommer, både i enkeltsaker og i forbindelse med lovarbeid. Vi vil særlig fremheve

betydningen av at lovgivningen utformes slik at den sikrer en god balanse mellom personvern og kriminalitetsbekjempelse.

Vurdering av personvern i myndighetsutøvelse – implementering av LED i politiregisterloven

Personvernkommisjonen mener det er behov for vurderinger av politiregisterlovens harmonisering med EU-retten og viser til at LED inneholder flere krav som ikke eksplisitt er gjennomført i politiregisterloven. Dette gjelder blant annet bestemmelsene om personvernprinsipper, vurderinger av automatiserte beslutningsprosesser og innebygd personvern. Kommisjonen peker også på at politiets rammer for og adgang til å benytte informasjon fra åpne kilder ikke er utredet og avklart som følge av manglende implementering av LED art. 10 bokstav c.

Datatilsynet støtter kommisjonens anbefaling om at Justis- og beredskapsdepartementet må vurdere om alle bestemmelsene i LED skal implementeres i politiregisterloven. Det vil i den sammenheng også være naturlig å vurdere om det er behov for regulering av utvikling og bruk av kunstig intelligens i justissektoren. Vi vil fremheve behovet for tydeligere rammer for politiets og påtalemyndighetens behandling av personopplysninger. Vi stiller oss positive til å bidra med innspill i et slikt arbeid.

Datatilsynet støtter også kommisjonens vurdering av at politiregisterloven bør forenkles og forbedres.

Tilsyn og kontroll

Datatilsynet mener i likhet med kommisjonen at tilsyn og kontroll er nødvendige kontrollmekanismer for å sikre forsvarlig og lovlig behandling av personopplysninger. Dette gjelder ikke minst innen justissektoren, der det ofte vil gjelde unntak og begrensinger i innbyggernes rett til informasjon og innsyn. Personvernkommisjonen mener at Datatilsynet og politiet bør føre statistikk over antallet personer som årlig benytter seg av retten til å klage inn politiets behandling av personopplysninger. Det vises til at offentliggjøring av slik statistikk kan bidra til å løfte bevisstheten om retten til å klage.

Datatilsynet bemerker at vi mottar få klager på politiets behandling av personopplysninger. Behov for mer informasjon om Datatilsynets rolle er derfor noe vi ser nærmere på. I den forbindelse vil vi også se på tilgjengeliggjøring av statistikk.

2.4 Personvern i skolen og barnehagen

Datatilsynet mener kapittel 8 i utredningen gir en god situasjonsbeskrivelse av barns og unges personvern. Vi er enige med kommisjonen i at det er avgjørende at personvernet ivaretas i barnehagene og i skolene.

I barnehagene og skolene brukes det digitale verktøy for både oppfølgings- og undervisningsformål. Det er gjerne store internasjonale teknologiselskaper som leverer disse verktøyene. Skoleadministrasjonene har liten mulighet til å påvirke den behandlingen av opplysninger som disse digitale verktøyene legger opp til. I tillegg er utdanningssektoren et attraktivt marked, og kommisjonen trekker frem mulighetene for å skape tidlige

forbrukerrelasjoner med elevene. En sentral utfordring er at det er store forskjeller i kommunenes kompetanse til å vurdere disse digitale verktøyene før de kjøpes inn og tas i bruk.

Politiske føringer for personvern i skolen og barnehagen

Datatilsynet støtter kommisjonens anbefaling om sterkere nasjonale føringer for sektoren, og etablering av en nasjonal personvernpolitikk fremstår som nødvendig og hensiktsmessig. Datatilsynet har også erfart at sektoren selv ønsker dette. Etablering og vedlikehold av en nasjonal felles tjenestekatalog er et tiltak som etter vår oppfatning vil kunne gi store personverngevinster, spesielt for små kommuner med begrensede personvernressurser.

Datatilsynet er også enig i at tilstrekkelig kompetanse og ressurser er nødvendig for at kommunene skal kunne ivareta personvernet i sektoren.

Vi støtter derfor anbefalingen om å etablere et nasjonalt kompetansemiljø, som det tidligere Senter for IKT i utdanningen, som ble nedlagt i 2019. Senteret skulle bidra til økt kvalitet i opplæringen med bruk av informasjons- og kommunikasjonsteknologi for barn i barnehagene, elever i grunnopplæringen og studenter i lærer- og barnehagelærerutdanningen.

Kommisjonen påpeker også behovet for tilpassede rutiner og veiledning fra kommunene til skoleledelse og lærere. Vi mener at dette er en nødvendig forutsetning for kommunens ivaretagelse av behandlingsansvaret sitt, og for å sikre praktisk etterlevelse av personvernregelverket i underordnede organer og etater.

Kompetanse og digitale løsninger i skolen

Det er positivt at kommisjonen foreslår at det bør gjennomføres en bred utredning om digitale verktøy som er i bruk i skolen og hvordan de påvirker barns personvern. Vi mener at det er uomtvistet at innsamling av elevers personopplysninger, og etterfølgende profilering og bruk av dataene til kommersielle formål, går på bekostning av elevenes grunnleggende rettigheter. Slike behandlinger utgjør en kontinuerlig krenkelse av elevenes personvern. Konkrete tiltak som for eksempel annonseblokkeringsverktøy på skolens utstyr vil kunne ha en positiv effekt, og etter vår mening bør slike verktøy introduseres og tas i bruk umiddelbart.

Vi mener lovgiver snarest bør ta stilling til om det skal innføres konkrete forbud i lovs form.

Datatilsynet er enig i kommisjonens forslag om sentralisering og samarbeid ved innkjøp og forhandlinger for skole- og barnehagesektoren. Samarbeid med andre land vil kunne gi en bedre posisjon overfor store leverandører.

Barn og unges kunnskap om personvern bør styrkes, og vi gir vår tilslutning til kommisjonens anbefalinger om å styrke opplæringen i undervisningen.

2.5 Forbrukernes personvern

Datatilsynet støtter samtlige av Personvernkommisjonens anbefalinger knyttet til forbrukernes personvern i kapittel 9, og det er positivt at kommisjonen kommenterer forbrukerbegrepet innledningsvis i kapittelet. Vi ønsker samtidig å kommentere enkelte av punktene.

Tilsyn og håndheving

Vi ønsker velkommen Personvernkommisjonens anbefalinger om regulering av, og tilsyn med, informasjonskapsler og liknende sporingsteknologier. Vi viser i den forbindelse til Datatilsynets og Forbrukertilsynets felles høringsuttalelse til forslaget om ny ekomlov.

Lovprosesser i EU

Vi er enige i at regjeringen bør påvirke personvernrelaterte lovprosesser i EU for å sikre interessene til norske forbrukere og virksomheter. Dette fordrer at regjeringen engasjerer seg tidlig nok i prosessene og at Norges handlingsrom til å komme med innspill utnyttes godt.

Atferdsbasert målretting av både kommersielle og ikke-kommersielle budskap kan medføre særlige utfordringer. Illustrerende og reelle eksempler inkluderer politisk mikromålretting, målretting av reklame for ugunstige kredittløsninger mot personer man antar har betalingsproblemer, og målretting av brukerinhold som fremmer spiseforstyrrelser mot tenåringer som har vist interesse for kosthold og trening. Algoritmene og anbefalingssystemene bruker kunstig intelligens. Vi mener derfor at regjeringen bør argumentere for strengere regulering av slike algoritmer i EUs «AI Act». Tilsvarende bør regjeringen engasjere seg i EUs lovforslag om politisk markedsføring, også når det gjelder åpenhet.

Når det gjelder det lovtekniske, mener vi det er viktig med klare regler som levner minst mulig rom for tolkningstvil for å sikre like spilleregler mellom markedsaktørene. Der forbud og begrensninger er aktuelt, bør man unngå at reglene kan fravikes ved samtykke, siden dette kan føre til «dulting» av forbrukere og samtykketretthet. På den annen side bør lovgivningen gi innbyggerne reelle og meningsfulle valgmuligheter der dette er passende.

Atferdsbasert markedsføring

Kommisjonen nevner at forordningen om digitale tjenester («Digital Services Act», DSA) skal bidra til større demokratisk kontroll med internettbaserte tjenester og plattformer. Vi gjør oppmerksom på at ikke alle typer aktører i de digitale økosystemene vil måtte følge kravene i DSA. Regjeringen bør derfor vurdere om enkelte av reglene i DSA kan og bør gjelde mer generelt, for eksempel reglene om markedsføring, manipulerende design og anbefalingsalgoritmer.

Datatilsynet deler for øvrig Personvernkommisjonens syn knyttet til et føre var-prinsipp når det gjelder atferdsbasert markedsføring mot barn. Vi frykter at digitale plattformer vil tillate atferdsbasert markedsføring mot barn under henvisning til at de ikke med rimelig sikkerhet vet hvilke brukere som er mindreårige.

Barn er imidlertid ikke den eneste sårbare gruppen på nett. Vi støtter Personvernkommisjonens flertall i at et generelt forbud mot atferdsbasert markedsføring må utredes.

Atferdsbasert markedsføring kan ha skadevirkninger både for individer og for demokratiet vårt.

Kommisjonens mindretall argumenterer mot utredning fordi et forbud etter mindretallets oppfatning vil være uforholdsmessig når atferdsbasert markedsføring kan gjøres forsvarlig. Datatilsynet er av den oppfatning at denne argumentasjonen ikke står seg, av flere grunner. Vi mener for det første at en utredning må komme før en konklusjon, og ikke omvendt. For det andre vil en utredning gi oss et bedre beslutningsgrunnlag. For det tredje er problemet at store deler av markedet ikke kan eller vil opptre forsvarlig. For det fjerde er en overlappende utredning allerede besluttet av Stortinget, se Sttingsvedtak 196 (2022–2023).

Vi ber om at omfanget av en utredning ikke defineres for snevert – digitale tjenester medfører beslektede utfordringer som kan kreve ulike løsninger. For eksempel bør man ikke begrense seg til atferdsbasert *markedsføring*, selv om dette bør være kjernen i utredningen. Også atferdsbasert målretting av ikke-kommersielt innhold, som rangering og forsterkning av brukerinnhold på sosiale medier, kan innebære inngripende sporing og profilering eller true rettigheter, friheter og demokrati. En fremtidig utredning bør derfor også ta for seg slik målretting av ikke-kommersielt innhold.

Vi mener det er mulig med effektiv regulering, også på nasjonalt nivå. Selv om Norge har begrenset handlingsrom til å særregulere behandling av personopplysninger innenfor rammene av EØS-avtalen, har vi trolig handlingsrom til å regulere en rekke forretningspraksiser og teknologier som forutsetter personopplysninger. Utredningen må ta stilling til hvilken innretning slik regulering kan og bør ha. Mulige handlingsrom kan være:

- Å forby eller begrense visse former for markedsføring, som atferdsbasert markedsføring. Her ligger også en mulighet til å utrede videre hvordan «atferdsbasert markedsføring» bør defineres, altså hvilke praksiser man ønsker å forby.
- Å regulere atferdsbasert målretting av kommersielle og ikke-kommersielle budskap på bestemte samfunnsområder eller i bestemte kommunikasjonskanaler, på samme måte som politisk markedsføring på TV er særregulert.
- Å regulere teknologier som utnytter brukernes underbevissthet for å foreta valg, fange deres oppmerksomhet eller manipulere dem.
- Å regulere enkelte algoritmiske beslutningsprosesser.
- Å regulere i kontekst av diskrimineringslovgivningen.
- Adtech-økosystemet kan føre til at sensitive opplysninger deles med fremmede makter. Norge kan ha handlingsrom til regulering i kontekst av lovgivning om nasjonal sikkerhet.

Særlig om barn og unges personvern

Vi er i likhet med Personvernkommisjonen særlig bekymret for barns og unges personvern på nett. Vi mener det er stort behov for å utrede hvordan barns rettigheter og friheter kan ivaretas på digitale flater. Dette gjelder både når barn selv deler sine personopplysninger, og tilfeller hvor barns personopplysninger blir delt av andre, for eksempel foreldre.

Datatilsynet ser særlig utfordringer knyttet til foreldres og tredjeparters eksponering av barns personopplysninger åpent på nett. Konsekvensene av dette er at foreldre selv gjennom sin digitale atferd risikerer å krenke barns rett til personvern. Det kan for eksempel være foreldre som gjennom egne kanaler deler privat informasjon om barnet på nett i forbindelse med konflikt med barnevernet, eller at foreldre samtykker til at en tredjepart får dele personopplysninger om barnet gjennom sine kanaler.

Reguleringen knyttet til lovligheten av en slik type eksponering er krevende. Det oppstår blant annet et spenningsfelt i forholdet mellom barnets rett til personvern og foreldrenes eller tredjepartens ytringsfrihet. Slike saker reiser også kompliserte spørsmål om foreldres samtykkekompetanse på vegne av barnet.

Vi ser positivt på at det i forslaget til ny barnelov er tatt inn en bestemmelse som vil gi foreldrene en plikt til å ta hensyn til barnets rettigheter når de samtykker på vegne av barn. Det er imidlertid uklart hvordan bestemmelsen i barneloven skal håndheves og virke sammen med øvrig regulering i personvernregelverket. Dette gjelder blant annet spørsmål om behandlingsgrunnlag og den avveiningen som må gjøres mellom ytringsfrihet og personvern i medhold av personopplysningsloven § 3. Vi mener derfor det er behov for en nærmere utredning av hvorvidt lovreguleringen på området ivaretar barnas rett til personvern på en god nok måte.

Datatilsynet støtter videre personvernkommisjonens anbefaling om å forebygge personvernutfordringer i forbindelse med deling av innhold på nett gjennom bevisstgjøring og kompetanseheving. Dette kan for eksempel skje gjennom obligatorisk veiledning på helsestasjon, i barnehage og på skole.

2.6 Regelkompleksitet og nasjonalt handlingsrom

Datatilsynet støtter de fleste av Personvernkommisjonens anbefalinger knyttet til regelkompleksitet og nasjonalt handlingsrom i kapittel 10, men ønsker å knytte særskilte merknader til to av dem.

Ideelle organisasjoners rett til å opptre på vegne av registrerte

Kommisjonen foreslår å gi ideelle organisasjoner rett til å klage til Datatilsynet uten fullmakt fra én eller flere registrerte, slik regelverket krever i dag.

Vi kan ikke se at det er noe dokumentert behov for å endre den ordningen som allerede følger av gjeldende rett. Vi viser til personvernforordningen artikkel 77, som gir enkeltindividet en slik klagerett, og til artikkel 80, som bestemmer at ideelle organisasjoner kan klage på den registrertes vegne. Innføringen av personvernforordningen innebar en betydelig styrking av individets klagerett, samtidig som forordningen presiserte at ideelle organisasjoner også kan representere klager overfor tilsynsmyndighetene. Vi mener denne ordningen virker etter sin hensikt, både nasjonalt og internasjonalt. Forbrukerrådet – som har gjennomført gode utredninger som har avdekket systematiske feil og prinsipielle personvernproblemstillinger, i tillegg til uheldig eller ulovlig forretningspraksis – er et godt eksempel på organisasjoner som bruker dette handlingsrommet allerede.

Dersom det vurderes å gå videre med et slikt forslag, må konsekvensene for Datatilsynet utredes. Vår kapasitet til å behandle slike klagesaker er allerede i dag svært presset. Kommisjonen ser ikke ut til å ha forutsatt dette i kapittel 14.

Tiltak for å forbedre lovtekster uten å gjøre innholdsmessige endringer

Datatilsynet stiller seg spørrende til kommisjonens utgreiing på dette punktet. For eksempel har man i ny ekomlov foreslått å kopiere definisjonen av samtykke i personvernforordningen artikkel 4 nr. 11, i stedet for å henvise til personvernforordningen. Problemet er at samtykke i forordningen også må forsås i lys av fortalen og andre bestemmelser, slik som artikkel 6, 7 og 8. Ved å kopiere definisjonen går dette tapt. Det er videre høyst uklart hva slags informasjonsbestemmelser kommisjonen ser for seg og hvorvidt en justering av dem faktisk vil redusere eller øke graden av klarhet i regelverket.

2.7 Teknologi i personvernets tjeneste

Datatilsynet stiller seg bak anbefalingene kommisjonen gir i kapittel 11, og kommer med innspill til hvordan anbefalingene kan implementeres i avsnittene under.

Personvernkommisjonen mener tilsynsmyndigheter bør gi råd til privatpersoner om hvordan de kan bruke teknologi for å beskytte seg mot ulovlig eller uønsket behandling, og gi konkret anvisning på aktuelle verktøy. Datatilsynet gir allerede i dag privatpersoner veiledning knyttet til enkeltindividets rettigheter og friheter, både via nettsidene, vår veiledningstjeneste og i saksbehandlingen. Slik situasjonen er i dag, har imidlertid ikke Datatilsynet ressurser til å gi konkrete anvisninger på bruk av ulike verktøy.

Personvernkommisjonen mener det bør treffes tiltak for å skape tydeligere plikter til å bygge personvern inn i tekniske og organisatoriske løsninger. Kommisjonen er i tvil om i hvilken grad det er adgang til slik klargjøring innenfor rammene av personvernforordningen. Vi tror at adgangen til å gjøre nasjonale tilpasninger her er begrenset.

Personvernkommisjonen uttaler at det er viktig å konkretisere plikten til å bygge inn personvern på måter som fremmer åpenhet om behandling av personopplysninger. Kommisjonen argumenterer for eksempel for at de registrerte bør gis direkte tilgang til egne personopplysninger, uten å måtte kreve innsyn først.

Vi er enige med kommisjonen på dette punktet, og alle virksomheter som behandler personopplysninger i en viss utstrekning kan med fordel sørge for å få på plass slike løsninger.

Reglene om innebygd personvern, åpenhet og ansvar må gjerne synliggjøres i opplæringsloven og i universitets- og høgskoleloven, slik kommisjonen foreslår. Vi vil i så fall anbefale at det samtidig vurderes inntatt relevante henvisninger til det generelle regelverket i personopplysningsloven og personvernforordningen.

Personvernkommisjonen anbefaler at norske myndigheter stimulerer til utvikling av norsk personvernteologi. Tiltak kan inkludere anskaffelseskrav i offentlig sektor, forskningsmidler for å utvikle personvern fremmende teknologi, og forskjellige

bevilgningsordninger. Datatilsynet har tro på at dette kan fremme både innovasjon og digitalisering innenfor de rammene vi ønsker i Norge og Europa. Vi ser også for oss at Datatilsynet kan spille en viktig rolle i en slik sammenheng, på grunn av erfaringene våre med den regulatoriske sandkassen, som nettopp har som formål å fremme innovasjon og ansvarlig bruk av kunstig intelligens.

2.8 Åpenhet

Kommisjonen mener at åpenhet er spesielt viktig når det skal tas beslutninger som har direkte betydning for innbyggernes plikter, rettigheter, friheter og muligheter. Dette kan for eksempel dreie seg om hvorvidt man får innvilget et lån eller barnetrygd. Kommisjonen anbefaler at full forklarbarhet må være det klare utgangspunktet, og at lavere standarder kun bør aksepteres når effektene antas å være ubetydelige.

I tillegg anbefaler kommisjonen at offentlige myndigheter og andre innflytelsesrike samfunnsaktører kontinuerlig må ha som en av sine viktigste oppgaver å styrke åpenheten knyttet til anvendelse av digital teknologi med direkte betydning for innbyggernes plikter, rettigheter, friheter og muligheter.

Vi støtter begge disse standpunktene, og vi mener at åpenhet blir spesielt viktig i årene som kommer, når samfunnsfunksjoner og tjenester digitaliseres og algoritmer i økende grad brukes til å analysere oss, og til å ta avgjørelser om oss.

2.9 Veiledning, tilsyn, klager og Datatilsynets organisasjon

I utredningens kapittel 13 går kommisjonen blant annet inn på Datatilsynets rolle, oppgaveutføring og budsjett. Vi mener det er positivt at kommisjonen tar opp disse temaene på eget initiativ.

Kommisjonen understreker at et «velfungerende tilsynsorgan er et nødvendig premiss for å sikre innbyggernes personvern», og at tilstrekkelige ressurser er en forutsetning for et velfungerende tilsynsorgan. Vi stiller oss bak kommisjonens uttalelser, og vi viser til omtalen nedenfor i pkt. 2.10, hvor konsekvensene av mangelfulle ressurser i tilsynet er nærmere beskrevet.

Det er også statens rettslige forpliktelse å sikre et slikt velfungerende tilsynsorgan, se personvernforordningen artikkel 52 nr. 4, jf. fortalepunkt 120.

For øvrig hadde vi gjerne sett at Datatilsynets uavhengighet, jf. artikkel 52, var blitt gjort til gjenstand for en noe grundigere omtale. Etter vår mening har tilsynets uavhengighet betydning for flere av spørsmålene kommisjonen tar opp i kapittel 13.

Spesielt om behovet for veiledning

Kommisjonen trekker frem at det er et stort behov for informasjon og veiledning om personvernregelverket. Kommisjonen uttaler at den ser at det kan være uheldig at samme organ både skal gi veiledning, fatte avgjørelser, utføre tilsyn og drive med kontrollvirksomhet.

Vi viser til at Datatilsynets lovpålagte oppgaver er beskrevet i personvernforordningen artikkel 57. Her er det blant annet slått fast at tilsynsmyndigheten skal drive med ulike former for informasjons- og veiledningsarbeid, og at tilsynsmyndigheten også skal føre kontroll med og håndheve anvendelsen av regelverket.

Tilsynet opplever at det er et stort veiledningsbehov både hos virksomheter og enkeltpersoner. På grunn av ressursituasjonen har vi dessverre måttet nedprioritere mange forespørsler om veiledningsmøter. Vi har også begrensede ressurser til å videreutvikle nettsidene våre, selv om de er oppdatert på innhold.

Kommisjonen foreslår at også andre myndigheter enn Datatilsynet bør veilede om «personvernspørsmål som direkte er knyttet til deres myndighetsområde». I så fall er det viktig å sikre at veiledning og tolkning av personvernregelverket er konsekvent på tvers av sektorer, og at det er bevissthet om Datatilsynets rolle som regelverksforvalter og -håndhever på personvernområdet.

Datatilsynets rolle ved utforming av lover og forskrifter

Det er svært positivt at Kommisjonens trekker frem Datatilsynets rolle i forbindelse med forberedelse av nasjonal lovgivning og andre administrative tiltak. Vi er enige i at Datatilsynet bør involveres i flere lov- eller forskriftsprosesser for å sikre at personvern hensyn blir ivaretatt på riktig tidspunkt i prosessen.

Etter vår vurdering er det klart at forordningens artikkel 36 nr. 4 forutsetter en annen type involvering enn alminnelige lov- eller forskriftshøringer. Andre europeiske tilsynsmyndigheter deler denne forståelsen, blant annet myndighetene i Tyskland (BfDi) og Storbritannia (ICO). ICO har i et brev til den skotske regjeringen vist til følgende:

«Consultation is directly with the ICO and is separate from any public consultation, which would not satisfy the [article 36(4)] requirements. Consultation should be undertaken during the formative stages of the developments of policy, to ensure that there is opportunity to give due consideration to input from the ICO before the outputs are finalised».

Vår forståelse er for øvrig at rådføringsplikten i artikkel 36 nr. 4 utløses ved arbeider med lover eller forskrifter som innebærer en *høy risiko* for personvernet, jf. også artikkel 35 nr. 1. Her er det ulike synspunkter blant øvrige europeiske tilsynsmyndigheter. I Tyskland er for eksempel den føderale myndigheten involvert i alle prosesser som berører behandling av personopplysninger. En slik ordning ville neppe være gjennomførbar i Norge, i alle fall ikke med dagens ressursituasjon i Datatilsynet.

Uansett er det klart at økt involvering i arbeidet med å forberede lover og forskrifter, og eventuelt andre administrative tiltak, vil gi behov for økte ressurser til Datatilsynet.

2.10 Økonomiske og administrative konsekvenser

I kapittel 14 er det foreslått en rekke tiltak som krever oppfølging av andre aktører enn Datatilsynet. Datatilsynet mener det er naturlig at det må følge ressurser med tiltakene for at de skal være mulig å gjennomføre i praksis. I dette høringssvaret fokuserer vi på mulige administrative og økonomiske konsekvenser for Datatilsynet.

Kommisjonen anbefaler en generell styrking av Datatilsynet. Vi er selv av den oppfatning at det ikke lenger er samsvar mellom de oppgavene som vi er satt til å løse og de ressursene vi har. Det vi erfarer, etter å ha tilpasset oss ny lovgivning og ny oppgaveløsning, er at vårt mandat og samfunnsoppdrag suksessivt har økt i både omfang og kompleksitet. Statistikken over innkomne saker peker oppover på alle områder. Det er ingenting som tyder på at dette vil endre seg med det første.

Datatilsynet har hatt en stor økning av saker, både i volum og kompleksitet. Vi har blant annet erfart en særlig økning i antall avviksaker og klagesaker og oppgaver som er knyttet til harmonisering og samordning mellom EUs datatilsynsmyndigheter. Mange virksomheter etterlyser nå også flere stedlige tilsyn fra Datatilsynet.

Den lovpålagte behandlingen av klager fra enkeltindivider binder opp svært mye ressurser hos Datatilsynet, og fører i dag til at vi har begrensede muligheter til å prioritere. Ofte må selvinitierte tilsynsaktiviteter vike for klagesakene, selv om førstnevnte kan fremstå som viktigere eller er egnet til å gi større effekt, både for enkeltindivider og for samfunnet.

Internasjonalt arbeid og samordning er også en kjerneoppgave og helt nødvendig ettersom mye av rettsdannelsen skjer i EU. Det er en rekke krav og frister som må overholdes i disse sakene og sakene er ofte komplekse og svært ressurskrevende. Ny lovgiving fra EU berører Datatilsynet og krever ressurser å følge opp.

Det gjeldende personvernregelverket er komplisert og oppleves av mange som vanskelig tilgjengelig. Det er fortsatt begrensede rettskilder, og det er en klar forventning fra både offentlige og private virksomheter at Datatilsynet skal gi informasjon, utvikle veiledningsmaterieell og selvhjelpsverktøy slik at regelverket kan etterleves.

Mangel på ressurser er også noe våre nordiske tilsynskolleger erfarer. Vi ser imidlertid at øvrige skandinaviske tilsyn styrkes for å møte utfordringene. Etter det vi erfarer, har for eksempel IMY, det svenske Datatilsynet, i den svenske regjeringens budsjettforslag 2022 fått en økt ramme på 56 millioner kroner de neste to årene, hvorav 48 millioner i 2023. Til sammenligning var det norske Datatilsynets totale budsjett for 2022 på ca. 71 millioner kroner.

I tillegg til våre eksisterende oppgaver kommer kommisjonen med en rekke forslag som vil kreve ressurser og ha økonomiske konsekvenser for oss. Her er noen eksempler på forslagene som utløser ressursbehov:

- Forslaget om at departementene i større grad skal rådføre seg med Datatilsynet i lov- og forskriftsarbeider.

- Forslaget om utredning av forbud mot atferdsbasert markedsføring – behovet for økte midler til Datatilsynet må vurderes, ettersom et slikt forbud trolig vil medføre ekstra oppgaver.
- Forslaget om å legge ansvar for håndheving av informasjonskapsler og lignende sporingsteknologi til Datatilsynet.
- Forslaget om at flere myndigheter veileder om personvern vil kreve koordineringsarbeid og oppfølging fra Datatilsynet for å sikre enhetlig tolkning av regelverket på tvers av sektorer.

Norge trenger et effektivt og slagkraftig datatilsyn for å hjelpe norske virksomheter i privat og offentlig sektor å ivareta personvernet til innbyggerne. Vi støtter derfor kommisjonens anbefaling om en styrking av tilsynet.

3. Avslutning

Dersom dere har spørsmål eller ønsker at vi utdyper synspunktene, kan dere ta kontakt med direktør Line Coll eller avdelingsdirektør Jørgen Skorstad.

Med vennlig hilsen

Line Coll
direktør

Jørgen Skorstad
avdelingsdirektør

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer