

JUSTIS- OG BEREDSKAPSDEPARTEMENTET
Postboks 8005 Dep.
0030 OSLO

Deres referanse
18/3955

Vår referanse
18/01381-2/CNE

Dato
31.08.2018

Høring - Personvernkommisjon - Innspill til mandat - Justis- og beredskapsdepartementet

1. Innledning

Ifølge høringsbrevet, skal Personvernkommisjonen blant annet se på *personvern i justissektoren, og hvordan personvernet kan sikres ved økt bruk av digitale løsninger, herunder rettighetene til brukere av sosiale medier*, samt inkludere et særlig oppdrag om å *vurdere tilstanden for barns personvern* og tiltak for å styrke dette. For øvrig er mandatet åpent.

På de snart ti årene som har gått siden Personvernkommisjon leverte rapporten *NOU 2009: 1, Individ og integritet*, har Norge gjennomgått en omfattende digitalisering. Det er enorme muligheter knyttet til digitaliseringen av samfunnet, men det intensiverer også bruken av folks opplysninger i en helt annen skala enn vi har sett tidligere. Vi opplever, og vil gjøre det i stadig større grad fremover, juridiske og etiske dilemmaer hvor potensialet for betydelig samfunnsgevinst må veies opp mot grunnleggende personvern hensyn.

Samfunnet er avhengig av at innbyggerne har tillit til at opplysningene om dem blir håndtert på en sikker og rettferdig måte. Hvis folk ikke har tillit, vil de være mer forsiktige med å dele opplysningene sine. Norge er et samfunn kjennetegnet av høy tillit. Denne tilliten kan vi ikke ta for gitt. Hvordan vi velger å samle inn og bruke personopplysninger om befolkningen legger samtidig premissene for hvilket samfunn vi ønsker å leve i.

Vi mener Personvernkommisjonen bør løfte blikket og identifisere de viktigste dilemmaene vi står overfor i dagens datadrevne virkelighet og gi en helhetlig statusrapport over utfordringene for personvernet. Personopplysninger er en viktig ressurs, og tilgang til opplysningene gir innsikt i og kunnskap om folks liv, vaner, interesser og behov. Denne kunnskapen påvirker maktbalansen i samfunnet. Personvernkommisjonen bør utrede hvilke konsekvenser den stadig mer omfattende innsamlingen og behandlingen av personopplysninger har for den enkeltes autonomi og selvbestemmelse, og for samfunnet og demokratiet som helhet.

Vi vil med dette som bakgrunn kommentere innspillene som foreligger til mandat, samt komme med innspill til andre problemstillinger vi mener det er viktig at en personvernkommisjon ser på. Vi mener Personvernkommisjonen primært bør ha fokus på områder der det er nasjonalt handlingsrom, det vil særlig si når det gjelder offentlige myndigheters bruk av personopplysninger til kontroll og analyseformål.

2. Personvern i justissektoren

Datatilsynet har gjentatte ganger tatt til orde for at det opprettes en kommisjon som tar for seg status for personvernet i justissektoren. Vi mener at en gjennomgang av justissektoren bør være en sentral del av utvalgets mandat og da særlig knyttet til tiltak som innebærer overvåkning av befolkningen.

Siden terrorangrepene i USA i 2001 har vi sett en rekke personverninngrepene tiltak i Norge på dette området. Tiltakene har hatt som mål å forebygge eller bekjempe kriminalitet, terror eller internettrelaterte trusler. Da datalagringsdirektivet ble vedtatt av EU-kommisjonen i 2011, åpnet Stortinget for føre-var-innsamling av data om alle norske borgere. Kommisjonsvedtaket ble imidlertid senere kjent ugyldig av EU-domstolen, blant annet fordi lagring kan føre til at folk får en følelse av å være under konstant overvåking.

I 2016 fikk politiet tilgang til å bruke dataavlesing ved etterforskning, avverging og forebygging av alvorlig kriminalitet. Samme år ble også et forslag om å innføre et digitalt grenseforsvar lagt fram. Et slikt tiltak vil kunne innebære overvåking av kommunikasjonen til de fleste innbyggerne i Norge, uten hensyn til om de har vært involvert i en straffbar handling eller ikke.

Dette er eksempler på tiltak som innebærer inngrep i personvernet til den enkelte. Økt lagrings- og prosesseringskapasitet, samt bruk av kunstig intelligens, muliggjør mer omfattende og dyptgående overvåkingstiltak, og er noe som vil utfordre personvernet også i årene fremover.

Vi mener det er viktig at en personvernkommisjon ser nærmere på det presset som det samlede omfanget av tiltak setter på personvernet. Vi mener det er viktig at kommisjonen løfter blikket og legger grunnlaget for en debatt om hva slags samfunn vi ønsker, og hvor langt det er riktig å gå når det gjelder å begrense innbyggernes frihet.

I vårt høringsvar til rapporten fra Lysne II-utvalget om digitalt grenseforsvar (DGF) pekte vi på at behovet for en personvernkommisjon på justisfeltet større enn noen gang. Vi påpekte her at det vil være uansvarlig å gå videre med utvalgets forslag uten en slik kommisjon. Vi har imidlertid notert oss at Regjeringen har varslet at den planlegger å legge frem en nytt forslag om digitalt grenseforsvar om ikke lenge. Det vil være svært uheldig, mener vi, å gå videre med forslaget før personvernkommisjonen har sluttført sitt arbeid.

Datatilsynet er opptatt av hvordan tiltak som medfører inngrep i kommunikasjonsvernet kan føre til **nedkjølingseffekt**. Teorien om nedkjølingseffekt går ut på at vi legger bånd på oppførselen vår dersom vi ikke vet hvordan opplysningene som samles inn om oss blir brukt. Hvis vi er usikre på hvem som har tilgang til opplysningene vi legger igjen, er vi tvunget til å

ta hensyn til denne usikkerhetsfaktoren. Vi vil begynne å tenke gjennom hva vi skriver, hva vi foretar oss og hvem vi har kontakt med. En følge av nedkjølingseffekten kan være at vi unnlater å gjøre helt ordinære gjøremål. Vi kan for eksempel unngå å låne en bestemt bok på biblioteket eller å ringe psykologen, i frykt for hvordan disse opplysningene eventuelt kan bli brukt senere. Men nedkjølingseffekt handler også om press på ytringsfriheten, som i neste konsekvens kan svekke demokratiet ved at borgerne begrenser sin deltakelse i åpen meningsutveksling. Et sviktende kommunikasjonsvern har for eksempel konsekvenser for anonyme kilders mulighet til å kommunisere fritt med journalister. Personvernkommisjonen bør se nærmere på fenomenet nedkjølingseffekt, herunder hvilke konsekvenser et sviktende kommunikasjonsvern har for kildevernet og for minoritetsgruppers tillit til myndighetene.

3. Personvern ved bruk av digitale løsninger, herunder rettighetene til brukere av sosiale medier

Det er i dag store utfordringer knyttet til folks personvern når de bruker internettbaserte tjenester, herunder sosiale medier. Vi mener imidlertid at personvernkommisjonen ikke bør bruke ressurser på å utrede hvordan rettighetene til brukerne av internettbaserte tjenester utfordres, da dette er regulert i personvernforordningen og annen lovgivning.

Vi ser imidlertid store utfordringer når det gjelder **informasjonssikkerhet**, og mener Personvernkommisjonen bør se på hvordan kompetansen på dette området kan styrkes. Datatilsynets inntrykk er at virksomheter, både private og offentlige, ikke i tilstrekkelig grad identifiserer hvilke trusler deres behandling av personopplysninger er utsatt for. Stadig flere virksomheter velger å sette ut tjenester som omfatter behandling av personopplysninger til eksterne aktører. Samtidig erfarer vi at kompetansen på sårbarhets- og risikovurderinger ikke er tilfredsstillende.

Innen helsesektoren fremstår det eksempelvis ofte, blant annet i lovforslag og forskriftsforslag om nye registre, som om truslene mot informasjonssikkerheten primært er knyttet til egne ansattes feil eller ulovlige handlinger. Dette er en mangelfull analyse av risikobildet. Konsekvensen av mangelfulle risikovurderinger gjør virksomhetene sårbare for innbrudd og lekkasjer av data. Datatilsynet ila i 2017 ni helseforetak i Helse Sør-Øst overtredelsesgebyr for å ikke ha oppfylt pliktene til sikkerhetsledelse, risikovurderinger og tilgangsstyring i forbindelse med tjenesteutsetting av IKT-Drift til utlandet.

Enkeltpersoner forventer at personvernet og informasjonssikkerheten blir ivarettatt når virksomheter behandler personopplysningene deres. Når innbyggerne er i kontakt med offentlige virksomheter er det ikke alltid at kommunikasjonskanalene er sikret. Det gjelder for eksempel kommunikasjon på ukryptert e-post, manglende kryptering av nettsider, eller dårlig håndtering og administrasjon av nettsteder.

Digitaliseringen av samfunnet innebærer at stadig større mengder personopplysninger samles inn og behandles. Dette skjer samtidig som selve behandlingen av personopplysninger i stadig økende grad tjenesteutsettes til aktører i Norge eller i utlandet. Denne utviklingen krever nye måter å vurdere risiko på. Personvernkommisjonen bør se på hvordan risikovurderinger gjøres i dag og komme med forslag til tiltak for å heve kompetansen på dette området.

4. Barn og personvern

Datatilsynet stiller seg positive til at Personvernkommisjonen skal vurdere tilstanden for barns personvern og tiltak for å styrke det. Datatilsynet er svært opptatt av barns personvern og opplever at dette stadig vekker blir satt under press både i barnas barnehage- og skolehverdag og på deres fritid.

Registrering og kartlegging av barn begynner allerede fra før de er født, og gjennom barneårene i barnehagen og grunnskolen. Det finnes enormt med opplysninger om barn før de er gamle nok til selv å kunne samtykke eller stille spørsmål ved bruken av alle opplysningene. Eksempler her er kartlegging av språk, adferd og utvikling som foregår i ulike barnehager. I grunnskolen tas det i bruk verktøy for å forebygge mobbing og måle klassetrivsel, samt bruk av læringsanalyse i ulike fag.

Personvernkommisjonen bør diskutere hvilke konsekvenser det kan ha for barn hvis de må dra med seg en hale av digitale spor fra barnehagen og oppover i skolesystemet, spor som hele tiden vil legge premisser for hvordan de behandles. Vil vi utstyre våre barn med «digitale tatoveringer» som vil få avgjørende innflytelse på deres videre livsløp? Barn forandrer seg, modnes og utvikles hele tiden. Bruk av dataanalyse i skolen må ta hensyn til dette.

De siste årene har utdanningssektoren vokst frem som et nytt og attraktivt marked for etablerte IT-kjempene som Google og Apple, og blant nye nisjeselskaper. Datatilsynet erfarer at skoleeierne ofte mangler kunnskap og kapasitet til å sette krav til produkter og tjenester som de kjøper. I tillegg har skolene stramme budsjetter å forholde seg til, og de mange gratis læringsressursene som finnes på markedet representerer derfor et attraktivt alternativ til kostbare betalingstjenester. Gratis applikasjoner har imidlertid en pris. Valutaen det betales i er elevenes personopplysninger. For noen elever og deres foresatte vil det være akseptabelt å betale med sine personopplysninger, for andre ikke. Det problematiske med bruk av personopplysninger som betalingsmiddel i skolesektoren er at det ikke er eleven selv som tar avgjørelsen. Det er skoleeieren som aksepterer betaling med personopplysninger på vegne av elevene. Personvernkommisjonen bør se på hvordan skoleeiere kan bli bedre bestillere av digitale tjenester.

5. Andre viktige problemstillinger en personvernkommisjon bør se på

5.1 Sammenstilling av data for å løse myndighetsoppgaver

Vi er i startgroppen for bruken av stordata-analyse og kunstig intelligens. Offentlige myndigheter sitter på store mengder data om enkeltindivider. Teknologien kan blant annet brukes til å profilere og forutsi atferden til enkeltmennesker og til grupper av mennesker. Vi erfarer at offentlige myndigheter i stadig større grad ønsker å sammenstille opplysninger om borgerne på tvers av ulike offentlige virksomheter for å persontilpasse og automatisere tjenester til innbyggerne og til ulike typer kontrollformål. UDI bruker allerede maskinlæring til å treffe enkelte typer vedtak. NAV og Skatteetaten jobber med løsninger for å avdekke trygde- og skattemisbruk ved hjelp av stordata-analyse. Bekjempelse av arbeidslivskriminalitet og svart arbeid er også eksempler på områder der det gjennomføres tiltak for å legge til rette for informasjonsflyt mellom etatene.

Bruk av stordata og kunstig intelligens utfordrer flere sentrale personvernprinsipper, blant annet prinsippene om formålsbestemthet, dataminimalisering og rettferdig behandling. Personvernforordningen trekker opp tydelige grenser for hvordan data kan brukes, blant annet bestemmelser som regulerer bruken av automatiserte avgjørelser. Det finnes likevel et betydelig handlingsrom for norske myndigheter til å bestemme hvordan personopplysninger om norske borgere skal sammenstilles og brukes fremover for å effektivisere forvaltningen.

Personvernkommisjonen bør trekke opp noen rammer for hvordan – og i hvor stor utstrekning – myndighetene kan sammenstille og analysere opplysninger om den enkelte. Hvor mye opplysninger og dermed kunnskap om den enkelte kan myndighetene sammenstille og analysere uten at det røkkes ved maktbalansen i samfunnet og enkeltindivids tillit til myndighetene? Vår erfaring er at lovforslag som er på høring ofte er mangelfullt utredet når det gjelder personvernkonsekvensene. Å lage løsninger som muliggjør utnyttelse av store datamengder, samtidig som personvernulempene for enkeltindividet reduseres mest mulig, vil bli avgjørende fremover.

Hvordan vi skal sørge for at kunstig intelligens utvikles og tas i bruk på en måte som er til det beste for mennesket er en stor og viktig oppgave. Vi mener regjeringen bør nedsette en egen kommisjon som ser på dette spørsmålet særskilt.

5.2 Helsesektoren og personvern

5.2.1 Utnyttelse av den norske befolkningens registerdata

Det har den siste tiden blitt gjennomført en rekke utredninger og evalueringer som har endt opp med ulike forslag til hvordan vi bedre og mer effektivt skal kunne bruke helsedata til ulike formål, og hvordan vi skal kunne realisere gevinstene av disse dataene. Det er bred enighet om at helsedata har stor verdi.

Helsedataprogrammet utreder for eksempel nye metoder for tilgjengeliggjøring gjennom Helseanalyseplattformen. Potensialet som presenteres gjennom denne plattformen innebærer helt nye måter å samle inn opplysninger, gjennom for eksempel innbyggernes eget utstyr. Data skal sammenstilles og analyseres ved hjelp av stordata-teknologi og kunstig intelligens og resultatene skal brukes til nye formål i for eksempel legemiddelmiddelindustrien og næringslivet.

Vi ønsker at kommisjonen undersøker hvorvidt realiseringen av verdiene som ligger i mer omfattende innsamling og sammenstilling av helsedata kan ha en kostnad sett fra et personvernståsted, og om personvern hensyn kan tilsi en mer restriktiv utvikling. Personvernkommisjonen bør også se på hvordan innebygd personvern kan brukes for utvikle løsninger som er akseptable fra et personvernperspektiv.

5.2.2 Bruk av helsedata og selvbestemmelse

Når vi mottar helsehjelp må vi naturlig nok avgi opplysninger om oss selv. Det er imidlertid vårt inntrykk at mange ikke vet at helseopplysninger de avgir når de mottar helsehjelp også blir brukt til andre formål, slik som kvalitetssikring og forskning. Selvbestemmelse er et

viktig personvernprinsipp. Vi er opptatt av hvordan mangelfull informasjon om hvordan helseopplysninger blir brukt til ulike formål, potensielt kan føre til tap av tillit overfor helsevesenet.

Datatilsynet mener at personvernkommisjonen bør se på hvordan retten til selvbestemmelse over helsedata bør ivaretas. Videre bør konsekvensene av å ikke kunne bestemme selv utredes. Kan det for eksempel medføre tap av enkeltmenneskets tillit overfor helsevesenet? I de tilfellene hvor selvbestemmelse ikke er aktuelt, foreslår vi at kommisjonen ser på andre mulige tiltak som kan gi borgerne størst mulig kontroll over egne helsedata. Slik tiltak kan for eksempel dreie seg om informasjon og innsyn, rett til begrenset behandling, reservasjonsløsninger og sperremuligheter.

5.2.3 Digitaliserte helsetjenester og pasienter

Helsetjenesten og utøvelsen av pasientrettigheter blir stadig mer digitaliserte. Dette er et klart mål for sektoren, uttalt blant annet i Stortingsmelding nr. 9 (2012-2013) En innbygger – en journal. Det foregår store nasjonale løp blant annet innen utvikling av en felles pasientjournal i Midt-Norge (Helseplattformen), en felles nasjonal journal for kommunehelsetjenesten, Nasjonal Kjernejournal, resept- og apotekløsninger og Personlig Helsearkiv.

Digitale data gjør det enklere å samle, koble og bearbeide data. Det er også enklere å bruke data som er samlet inn på nye måter, for eksempel gjennom velferdsteknologi eller privat utstyr som kan gi viktig informasjon om en persons helseforhold. Digitaliseringen skal gjøre relevant data tilgjengelig på en mer effektiv måte for å dermed kunne gi bedre helsehjelp. Samtidig medfører den nye personvern- og sikkerhetsutfordringer som må ivaretas.

Utviklingen av Helsenorge.no er et viktig skritt for å gi pasienter innsyn og informasjon, og det er en praktisk løsning for å administrere helsetjenester, samtykker og reservasjonsløsninger. Utøvelse av pasientrettigheter blir enklere, samtidig som det kan oppstå nye utfordringer knyttet til mengden av informasjon, kompleksiteten i informasjonen og valg man må ta stilling til.

Personvernkommisjonen bør se på hvordan man kan gi befolkningen informasjon på en forståelig måte, slik at pasientene kan ha kontroll over egne data og ta informerte valg i størst mulig grad.

Med vennlig hilsen

Jørgen Skorstad
avdelingsdirektør

Catharina Nes
fagdirektør

Kopi: Kommunal- og moderniseringsdepartementet
v/Statsforvaltningsavdelingen
Postboks 8112 Dep, 0032 OSLO

