# Representantforslag 56 S

**(2010–2011)**

fra stortingsrepresentantene Trond Helleland, Ingjerd Schou, Arve Kambe, Torbjørn Røe Isaksen, Michael Tetzschner og Erna Solberg

**Dokument 8:56 S (2010–2011)**

**Representantforslag fra stortingsrepresentantene Trond Helleland, Ingjerd Schou, Arve Kambe, Torbjørn Røe Isaksen, Michael Tetzschner og Erna Solberg om styrking av personvernet**

Til Stortinget

## Bakgrunn

Personvern handler om å kunne kontrollere informasjon om en selv og hva den brukes til. Personvernet er i dag under press på nær sagt alle områder i samfunnet. Det enkelte menneske har krav på beskyttelse av sitt privatliv. Utbredelse av ny teknologi innebærer at den private sfæren stadig blir mer gjennomsiktig og kontrollerbar. Det er viktig å beskytte privatlivet, både når det gjelder private interesser og offentlige etater. En kombinasjon av den teknologiske utviklingen, ønske om nye tiltak i bekjempelsen av kriminalitet, informasjon om samfunnsutviklingen og stadig mer omfattende offentlige etater/organisasjoner gjør at personvernet gradvis taper.

Retten til privatliv er en grunnleggende verdi i et liberalt demokrati. Dagens teknologi gjør det mulig å samle inn, lagre, sammenstille og formidle persondata i nesten ubegrenset omfang. Derfor er det nødvendig at politikken trekker grensene som teknologiske fremskritt har opphevet.

Rettsstatens oppgave er å beskytte enkeltmennesker mot overgrep fra hverandre, men den har også til oppgave å beskytte oss mot overgrep fra staten selv. Derfor er det avgjørende at staten er varsom med å samle inn, lagre og sammenstille informasjon om borgere. I de tilfeller der det likevel er nødvendig å samle inn informasjon, er det avgjørende at personvernet ivaretas på en god måte og at sikre rutiner for oppbevaring og sletting følges. Det gjelder for eksempel ved innsamling av informasjon om trafikkdata, personlig økonomi og pasienters helsetilstand. Innsamling og forvaltning av all denne informasjon svekker de verdier som vårt samfunn i stor grad bygger på; tillit mellom mennesker, rett til et privatliv, rett til å bestemme over eget liv, ytringsfrihet, rettssikkerhet og beskyttelse mot statlig overgrep.

NOU 2009:1 Individ og integritet, personvern i det digitale samfunnet, beskriver det på følgende måte:

«Ny teknologi for å samle inn og analysere personlige opplysninger dukker stadig opp. Mange av disse nye teknologiene for overvåkning, sporing og analyse favner videre, og pløyer dypere, enn tidligere, og overskrider de naturlige barrierene som tidligere utgjorde hindre mot overvåkning og sporing. Disse teknologiene forbedres og raffineres dessuten hele tiden, både kvantitativt og kvalitativt. Kvantitative fremskritt muliggjør mer overvåkning av flere individer. Kvalitative fremskritt muliggjør en overvåkning som både er mer usynlig og mer effektiv enn tidligere.»

Personvern er en helt sentral verdi for at vi skal føle at vi lever i et fritt og trygt samfunn tuftet på tillit mellom mennesker og mellom individ og stat. En naturlig konsekvens av et svakt personvern er at borgernes tillit til stat og trygghet for egen rettssikkerhet blir en trussel mot nødvendig og velbegrunnet informasjonstilgang i samfunnet. Frykten for at informasjon misbrukes, vil kunne skape et mer lukket samfunn.

Personvernopplysningsretten kan beskrives gjennom noen grunnleggende prinsipper som gjelder for all behandling av personopplysninger. Disse grunnleggende prinsippene kan sies å være selve kjernen i internasjonal og nasjonal personvernregulering. Prinsippene kan deles inn som følger:

**Rettmessig og rettferdig behandling**

All behandling av personopplysninger krever rettslig grunnlag, og den behandlingsansvarlige skal ta tilbørlig hensyn til den registrertes berettigede personverninteresser. Sensitive personopplysninger skal være underlagt strengere vern enn alminnelige personopplysninger.

**Brukermedvirkning og kontroll**

Prinsippet om brukermedvirkning og kontroll kommer til uttrykk i personvernlovgivningens bestemmelser som skal sikre transparens, det vil si bestemmelser om samtykke som behandlingsgrunnlag, informasjonsplikt, innsynsrett og meldeplikt. Autentiserings- og identitetsforvaltningsløsninger gjør det mulig å gjennomføre innsynsretten på en mer effektiv måte.

Brukermedvirkning og kontroll handler også om at brukeren skal kunne ha kontroll over utlevering og videre behandling av egne personopplysninger. Et grunnleggende skille er derfor mellom «transaksjonsfasen» hvor brukeren kan velge å utlevere opplysninger, og «videre behandling» hvor opplysninger om brukeren er blitt utlevert. Når opplysninger først er blitt utlevert, har brukeren liten eller ingen kontroll på behandlingen.

**Formålsbestemthet**

Den behandlingsansvarlige skal før innsamling og behandling av personopplysninger angi et klart og uttrykkelig formål med behandlingen. Personopplysninger skal kun brukes til de formål de er innsamlet for, og ikke benyttes for uforenlige formål. Hvis man avviker fra dette prinsippet i enkelte tilfelle, skal det klar lovhjemmel til.

Derfor er det ikke nok at to offentlige etater blir enige seg imellom om at det er en god idé å utveksle informasjon. Personopplysninger på avveie er alltid brudd på personvernet.

**Minimalitet**

Personopplysninger skal bare innhentes, lagres og behandles i den grad de er nødvendige for å oppnå formålet med behandlingen av opplysningene. Det må fremdeles være et tilbud om anonyme løsninger i sammenhenger der det ikke er nødvendig å identifisere seg. Personopplysningsloven stiller i liten grad krav til, eller legger føringer for, minimalitet og anonymitet.

Kort oppsummert oppstiller loven et forbud mot å samle inn irrelevante opplysninger, og en plikt til å slette eller anonymisere opplysninger når formålet er oppnådd.

**Datakvalitet**

Personopplysninger skal ha tilstrekkelig kvalitet for det formålet de skal brukes til. Dette innebærer for eksempel at opplysningene skal være godt nok oppdaterte, presise og relevante sett opp mot formålet med behandlingen.

**Informasjonssikkerhet**

Den behandlingsansvarlige skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til autentisering, konfidensialitet, tilgjengelighet og integritet ved behandling av personopplysninger.

Autentisering dreier seg om å få visshet om at en part virkelig er den han utgir seg for. Forskjellige metoder for autentisering gir forskjellig grad av sikkerhet. Med konfidensialitet menes egenskapen å ikke røpe informasjon for uvedkommende parter. Som regel knyttes teknikken kryptering til å oppnå konfidensialitet, men kryptografiske metoder kan også benyttes for autentisering og integritet.

Integritet betyr at informasjonen ikke er endret eller skadet. Dette kan dreie seg om tilfeldige feil ved lagring eller overføring av informasjon, og det kan dreie seg om bevisste handlinger fra uvedkommende. Tilgjengelighet er vissheten om at kommunikasjon mellom to eller flere parter faktisk er mulig. Graden av tilgjengelighet som er ønsket eller nødvendig, varierer fra system til system.

Det er viktig å iverksette tiltak for å sikre at informasjon ikke er tilgjengelig uten autorisasjon, at informasjon ikke uautorisert endres eller ødelegges, men samtidig at informasjon er tilgjengelig og anvendelig for medarbeidere slik at pålagte oppgaver kan utføres.

**Elektroniske spor**

Personvern innebærer blant annet at opplysninger om oss har en ekstra beskyttelse, slik at det skal være en grense for hvor nær inn på oss andre skal få lov til å komme, dersom vi ikke ønsker det selv. Personverndebatten både her hjemme og internasjonalt har i tillegg de senere år båret preg av nye personvernutfordringer knyttet til «elektroniske spor». Elektroniske spor er et bilde på et bredt spekter av opplysninger som typisk genereres og lagres ved bruk av ulike elektroniske hjelpemidler.

Studier av personvernproblematikk knyttet til elektroniske spor viser at det siden begynnelsen av 1990-tallet har vært en drastisk økning i mengden elektroniske spor, og at disse blir stadig mer innholdsrike. Metodene for å analysere denne typen data har utviklet seg i takt med den teknologiske utvikling, og gjør det mulig å gi et nyansert bilde av gruppers eller enkeltpersoners ressurser, bevegelsesmønster, omgangskrets og interesser.

**Skattelister**

Snoking i andres privatliv er rett og slett blitt enklere. Et navn gir andre lett adgang til informasjon om inntekt, formue og skatt. Samtidig får man informasjon om fødselsdato og postnummer. Ved hjelp av dette kan man få gateadresse, skråfoto av hus og eiendom, telefon, offentlige og private verv, informasjon om alle de andre som har verv i samme bedrift, samt økonomiske resultater og forhold. Dette kan linkes opp mot bilder fra offentlige opptreden eller andres private nettsider. Tilgang til en stor del av denne informasjonen legger det offentlige til rette for, og nøkkelen akkurat her ligger i skattelistene.

Kombinasjonen av alle opplysningene kan gjøre det enkelt for kriminelle å gjennomføre identitetstyverier, som er et stadig økende problem. Kredittkort i andres navn kan altfor enkelt bestilles med korrekte opplysninger om inntekt, skatt og formue. Stortingsrepresentanter fra Høyre tok i eget representantforslag opp forslag om å redusere tilgangen til informasjon i skattelistene og redusere faren for tilknyttet kriminalitet (Dokument 8:11 S (2010–2011)).

**Grensesetting**

Personvernundersøkelsen i 2005 viser at nordmenns holdning til kontroll og kameraovervåking er under endring. Det er en økende aksept for kontroll og overvåking om hensikten er å bekjempe kriminalitet. De aller fleste av oss har også stor tiltro til at personopplysninger og sensitiv informasjon som vi gir fra oss, blir behandlet på en betryggende måte. Men Datatilsynets erfaring viser et annet bilde. Svært mange virksomheter, både offentlige og private, mangler rutiner og kontroll for hvordan slike opplysninger skal behandles.

Nyheter om personopplysninger på avveie møter oss rett som det er i mediene. Nødvendigheten av klare regler for innhenting og oppbevaring av personopplysninger blir større jo flere spor vi legger igjen. Vi kan bidra til å redusere faren for misbruk om vi er kritiske til behov og formål hver gang vi blir møtt med krav om å gi fra oss litt av vår egen identitet. For den enkelte kan det være vanskelig å se hvilken risiko som finnes for innsamling og misbruk av personopplysninger. Derfor trenger vi noen som kan bruke sine erfaringer til å stille kritiske spørsmål og sette grenser, enten det er Datatilsynet eller andre offentlige aktører.

**Loggføring**

Vi har i dag stor tillit til offentlige instanser som politi, sykehus, trygde- og velferdsforvaltningen og kommunene. Disse instanser forvalter svært mye sensitiv informasjon om den enkelte innbygger. Dette så vi tydelig i høst, da det viste seg at Nav krenket personvernet hos enkeltindivider, noe Nav hjemlet i folketrygdloven nye § 21-4 a. Teknologien gjør det imidlertid ikke bare mulig å etablere og koble store registre. Den gjør det også mulig å regulere tilgang til informasjon og loggføre hvem som har oppsøkt informasjonen.

Den enkelte bør ikke bare ha rett til å vite hva som lagres av informasjon om seg selv, men også rett til å vite hvem som bruker informasjonen, og hva den skal brukes til. Folk flest har tillit til institusjonene, men ser man på Datatilsynets kontroller og resultatene av disse, er det diskutabelt om det offentlige Norge er tilliten verdig.

Et av de største reelle personvernproblemene vi har i dag, er at sensitive personopplysninger kommer på avveie – både fra offentlige og private registre. Eksempelvis skjer det ved at en utro tjener selger bankkontoutskrifter til media, som danner grunnlag for oppslag om kjente personer. Det kan også tenkes at slike registre lekker informasjon med enda mer alvorlige motiver. Registrering av hvem som aksesserer informasjon i registrene vil virke forebyggende på utro tjenere, og muligheter for etterforskning ved lovbrudd.

Faktum er at mange kan være interessert i hva vi foretar oss i hverdagen. Kommersielle aktører har store muligheter til å benytte automatiserte løsninger for å trekke konklusjoner ut av sporene vi legger igjen. Kraftig IT-verktøy brukes til å systematisere enorme mengder informasjon, og finner sammenhenger i det som for oss andre virker som uhåndterlige mengder data. Vi legger blant annet igjen spor hvis vi benytter fingeravtrykk, når vi laster ned musikk og filmer fra Internett, og når vi lar oss kameraovervåke på tenkelige og utenkelige steder. Det er bare fantasien som setter grenser for hva all denne informasjonen kan brukes til. Den beskyttende sfæren blir stadig snevrere. Det er det enkelte individ som må bære den tunge belastningen når personvernet svekkes, både psykisk, sosialt, økonomisk og tidsmessig.

I dagens samfunn er det en stor grad av selveksponering. Mange har behov for å dokumentere livet sitt for andre. Når andre tar dette valget for oss, og offentliggjør sider av vårt privatliv som vi ønsker å ha for oss selv, blir situasjonen imidlertid en annen. Det kan være svært ødeleggende når informasjon som legges ut på Internett, misbrukes og benyttes til helt andre formål enn de opprinnelige. Når noen stjeler en annens identitet og sprer krenkende uttalelser i vedkommendes navn, råder maktesløshet og sinne.

**Bompasseringer**

Med innføringen av det nye autopassystemet blir hver bompassering i dag lagret, enten du bruker Autopass eller blir fotografert for deretter å få faktura hjem. Per i dag registrerer bomselskapene passeringsopplysninger etter retningslinjer gitt av Vegdirektoratet. Skattedirektoratet kan etter ligningsloven

kreve innsyn i opplysninger knyttet til konkrete kjøretøy benyttet i næringsvirksomhet. I praksis gjøres det i bomselskapene ikke noen forskjell mellom lagring av passeringsopplysninger for kjøretøy brukt i næringsvirksomhet eller privat bruk.

**Barn og personvern**

I forbindelse med barns opphold i barnehage og skole melder det seg ofte spørsmål som gjelder barnas personopplysninger. Økte krav om offentlighet får også innvirkning i skolen. Det er viktig at barn sikres når det gjelder bruk av personopplysninger i skolehverdagen. Lister over elever og barn i skoler og barnehager er etter den nye offentlighetsloven med forskrift, som trådte i kraft 1. januar 2009, offentlige dokument. Hovedregelen er da at så lenge listene bare inneholder navn, adresse, telefonnummer og eventuelt fødselsnummer, er hele listen offentlig og kan oppgis ved krav om innsyn. Datatilsynet har pekt på at klasselister med hensyn til dagens lovgivning bør være så knappe som mulig, da alle kan kreve innsyn i klasselister med hjemmel i offentlighetsloven.

**Personvernansvarlig**

Menneskelig svikt er ofte forklaringen som gis når det går galt. Men menneskelig svikt er ofte et resultat av systemsvikt og manglende ledelse. En ansatt i kommunens PP-tjeneste som mister en minnepenn med all informasjon om barna som har vært innom tjenesten, er et eksempel på dette. Likeså når en ansatt tar med seg jobb hjem og ikke sletter informasjonen – informasjon som raskt kan spres av tankeløse personer på Internett, eller ved gammeldags sladder. Informasjon som kan bli hengende ved den skadelidende livet igjennom, og som kan bli liggende tilgjengelig på nettet for alltid. Kompetanse og oppmerksomhet om personvern må derfor være til stede i den enkelte virksomhet og være gjenstand for kontinuerlig diskusjon. Ordningen med personvernansvarlig legger til rette for dette. Dessverre er det altfor få offentlige virksomheter som har denne ordningen.

Ingen skal for eksempel bli gjenstand for individrettet forskning uten at de selv eller deres verge har samtykket til dette under full informasjon. Et individ har rett til å begrense spredning av identifiserbar informasjon om seg selv. Visse kategorier av opplysninger, slik som genetisk informasjon, skal ingen ha rett til å kreve utlevert.

## Forslag

Forslagsstillerne ønsker at det skal føres en restriktiv praksis ved elektronisk registrering, kobling, bruk og omsetning av personopplysninger, og fremmer derfor følgende

f o r s l a g :

I

Stortinget ber regjeringen sørge for at informasjon om inntekt og skatt gjøres offentlig tilgjengelig ved forespørsel, der forespørrerens navn blir registrert og personen det innhentes opplysninger om, får varsel (etter dagens modell for innhenting av kredittopplysninger).

II

Stortinget ber regjeringen sikre at offentlige registre og opplysningsbanker, slik som helsevesenet og Nav, etablerer logg for hvem som innhenter informasjon, og at den enkelte får rett til innsyn i loggen knyttet til sin person.

III

Stortinget ber regjeringen begrense Navs mulighet til å innhente personopplysninger samt komplette pasientjournaler, og legger til grunn at den berørte pasient gis kjennskap til at journalen er utlevert.

IV

Stortinget ber regjeringen sikre at det etableres en personvernansvarlig ved alle større institusjoner og etater som har tilgang til sensitive personopplysninger, eksempelvis Nav, helsesektoren og justissektoren.

V

Stortinget ber regjeringen fremme forslag om fjerning av Skattedirektoratets hjemmel i ligningsloven til å kreve innsyn i opplysninger knyttet til konkrete kjøretøy benyttet i næringsvirksomhet ved elektronisk bompassering.

VI

Stortinget ber regjeringen utarbeide retningslinjer for å sikre personvernet i forbindelse med innhenting og bruk av personopplysninger i skolen. Retningslinjene må sikre at personopplysninger blir behandlet, oppbevart og slettet på forsvarlig vis.

VII

Stortinget ber regjeringen iverksette tiltak for å skolere barnehageeier og barnehageansatte i personvernloven, samt innføre en bestemmelse om at innhenting og lagring, samt overførsel av personopplys-

ninger mellom barnehage og skole, kun skal skje etter informert samtykke fra foreldre/foresatte.

VIII

Stortinget ber regjeringen endre offentlighetsloven slik at klasselister kan forbli skolens eiendom, og således begrenses til den krets som har normal nytte av dem.

IX

Stortinget ber regjeringen sikre at forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter også hensyntar personvernet.

X

Stortinget ber regjeringen pålegge også store private registre, som i bank og forsikring, å etablere logger for hvem som innhenter personsensitiv informasjon, og at den enkelte får rett til innsyn i loggen knyttet til sin person.

17. desember 2010