Sammendrag fra Personvernkonferansen 7. desember 2012, Hotell Bristol, Oslo.

(http://www.jus.uio.no/ifp/om/organisasjon/seri/arrangementer/2012/personvernkonferansen.html)

Av Per Inge Østmoen, EFN

Konferansens bidragsytere med respektive temaer var de følgende:

1. Innledning ved professor Dag Wiese Schartum, Senter for rettsinformatikk, UiO

Hvordan skal lovgivning på området være for å virke best mulig? Schartum ga en kort orientering om Personopplysningsloven som er det primære verktøy for å styre personvernlovgivningen. Hvilke virkemidler står til rådighet ut over lovgivning, og hvordan skal vi få lovene best mulig? Schartum listet opp virkemidler: Rettslige virkemidler, økonomiske virkemidler, organisatoriske virkemidler, pedagogiske virkemidler og teknologiske virkemidler. Bare lov alene gir neppe tilstrekkelig effekt, mente Schartum innledningsvis. Organisasjonsansvar og forhold rundt dette er enklest å innarbeide i lovreglene. Når det gjelder regeltekster er disse bestemmende for hvor vanskelig eller lett det er å kommunisere reglene. Kunnskap om reglene er viktig, og reglene må være innlært, forstått og akseptert for å ha effekt. Det er også et spørsmål om hvor mye personvern skal koste og hvem som skal betale for personvernet. Skal det kunne lønne seg å etterleve regler om personvern? For personvern koster, dersom det skal gjennomføres i praksis. Både rutiner og tekniske tiltak medfører omkostninger.

2. Forsker Tommy Tranvik, Senter for rettsinformatikk, Avdeling for forvaltningsinformatikk, UiO. Tema: Hva vet vi om hvilken effekt personvernlovgivningen har?

Tranvik innledet med å si at det finnes nokså lite forskningsbasert kunnskap både i Norge og internasjonalt om hvorvidt, hvordan og hvorfor/hvorfor ikke lovgivningen på personopplysningsområdet etterleves i offentlige og private virksomheter og etater. Men hva skjer på etterlevelsesfronten i Norge, kan vi si noe om det? Tranvik henviste her til funn fra studier basert på situasjoner i offentlige institusjoner. Vurderingen av etterlevelse påvirkes av forventninger til regulatorisk suksess. Den mest ambisiøse definisjonen på suksess er at alle overholder hver eneste regel hele tiden, og at ett regelbrudd er ett for mye. Med en slik ambisjon vil ethvert lavere nivå oppleves som grader av fiasko. Ofte når man snakker om regulatorisk suksess, har man ikke på forhånd definert hva man snakker om, og da blir det vanskelig å bedømme effektene.

Personopplysningsloven med forskrift er både bredderegulering, som strekker seg på tvers av samfunnsområder, og dybderegulering som griper langt inn i virksomhetsinterne forhold. Hvis du skal ha både bredde og dybde, får du kanskje et overordnet regelverk som kan være vanskelig å forstå hvordan skal etterleves i en konkret organisatorisk kontekst. Det er for eksempel ikke enkelt å vite hvor grensen går mellom hva som er lovlig og hva som er ulovlig. Hvis regelkategoriene ikke alltid er like robuste og handlingsdirektivene ikke alltid er like tydelige, vil resultatet lett bli at behandlingsansvarlig pålegges til dels vage, kompetanseinsentive og arbeidskrevende oppgaver. Ofte leses ikke lovteksten, informasjonen kommer fra helt andre kilder. Tranvik spurte: "Er det rimelig å ha like store forventninger til regulatorisk suksess for personopplysningsloven med forskrift som for tobakkskadeloven?"

Dette var et retorisk spørsmål. Men Tranvik har observert både i offentlig og privat sektor at det ikke er realistisk å ha altfor store forventninger. Omfanget av regeletterlevelse befinner seg mellom to ytterpunkter: Ingen overholder alle reglene og ingen bryter reglene. Etterlevelsen varierer langs

tre dimensjoner typisk sett: 1. Regeldimensjonen, forskjellige regler etterleves i ulik grad. 2. Tidsdimensjonen, samme regel etterleves i ulik grad på forskjellige tidspunkter. 3. Organisasjonsdimensjonen, samme regel etterleves i ulik grad i forskjellige deler av virksomheten. Det siste er typisk for store virksomheter med oppdeling i ulike sektorer og funksjoner.

Hvorfor etterleves reglene? To hovedforklaringer: 1. Formålet med reglene har stor legitimitet, dvs. at loven/regelverket oppfattes som viktig og riktig. 2. Det er et ønske om å fremstå som kompetent og lovlydig, noe som anses å gi inntrykk av profesjonalitet og seriøsitet overfor omgivelsene. Men det er også tilleggsforklaringer: 1. Eksterne "sjokk" i form av kontroller av for eksempel Datatilsynet eller medieoppmerksomhet omkring "uheldige episoder." 2. Interne initiativ ved personutskiftninger, og ved påtrykk fra interne aktører som kan være for eksempel tillitsvalgte, verneombud eller personvernombud.

Hvorfor etterleves regler ikke? Tranvik hadde tre hovedforklaringer: 1. Inkompetanse, mangler evne til å omsette regler til lokal praksis. 2. Manglende regelkunnskap, kjenner ikke til reglene. 3. Prioriteringsvegring, manglende vilje til å bruke tid, penger og stillingsprosenter på etterlevelse.

Dessuten tre mindre viktige forklaringer: 1. Prinsipiell motstand, noen få bryter reglene av prinsipp. 2. Uenig i regelinnholdet, har en viss betydning i enkelte situasjoner. 3. Opportunisme, man spekulerer i at kontroll og sanksjoner mangler eller ikke vil komme og tror at man vil komme unna uten å bli straffet. Dette er sannsynligvis en liten faktor. Hva kan gjøres? Hvilke tiltak kan tenkes å påvirke etterlevelsen hos behandlingsansvarlig? 1. Ulike lovgivningsstrategier - kan ha en viss betydning. 2. Øke antallet kontroller, styrke sanksjonsregimet - kan ha en viss betydning og da overfor opportunister. 3. Øke informasjons- og veiledningsomfanget - vil trolig ha en viss betydning. 4. Etterlevelse "by design." Kan få betydning, men krever en annen måte å jobbe med etterlevelse på.

3. Førsteamanuensis Lee A. Bygrave, Senter for rettsinformatikk, UiO. Tema: Globalt problem - global regulering?

Bygrave begynte med å si at han er opptatt av de personvernmessige utfordringene som følger med en global verden. Hans første delsvar er "Global regulering." Når utfordringene er globale er vel også løsningene globale, foreslo han. Men er det så enkelt? Bygrave fokuserte på rettslige instrumenter, som er utarbeidet av Europarådet og OECD. Hans første poeng var at vi allerede er et godt stykke på vei til en global offentlig regulering på personvernområdet. Bygrave tenkte da på lovgivning som omfatter både offentlig og privat virksomhet. Veksten i lover akselererer. Den fremtidige ekspansjon vil etter Bygraves oppfatning først og fremst skje i Asia og Afrika. Utviklingen så langt har blitt styrt av Europa, mente Bygrave. Det eksisterer betydelige forskjeller i lovgivningen mellom landene i Europa, noe som gjenspeiler subsidiaritetsprinsippet i EUs lovgivning. (Se dette!)

Kan vi forvente større grad av harmonisering av lovverket i Europa og utenfor Europa? Mange har etterlyst en overordnet traktat eller i alle fall et sett med "kjøreregler" som gjelder globalt. Europarådet vedtok i 2001 en konvensjon om datakriminalitet. Trenger vi en traktat med potensiell global anvendelse? Vil vi i så fall ende opp med en vag og uklar tekst som preges av at den er utformet i et klima av uenighet, tautrekking og kompromisser? Det tar i ethvert tilfelle lang tid å utarbeide slike traktater, og på grunn av alle faktorer som kriminalitetsbekjempelse og mye annet som kommer inn blir det mye uenighet. Kontrakter kan også regulere dette området, og USA er et "unntaksland" fordi USA tradisjonelt er tilhenger av kontrakter fremfor offentlig rettslig regulering. Når det gjelder virkemidler kan kontrakter være mer slagkraftige enn lover, fordi kontraktene er direkte bindende for de som slutter seg til. Et spørsmål for seg er hvordan Kina vil oppføre seg på dette området. Bygrave tenkte seg at Kina vil innføre personvernlover, men på slik måte at

funksjonen blir avdempet.

Bygrave klarte ikke å gi noen overbevisende begrunnelse for sitt utsagn om global utfordring - global løsning, og akkurat dette med at det hele tiden uten begrunnelse hevdes at globale problemer må løses globalt er generelt lite begrunnet. I stedet gjentas den nevnte påstanden som et mantra som blir hengende i luften. Man kunne like gjerne, og kanskje med større rett, si at globale problemer som er oppstått i stor grad som en følge av globale makt- og dominansstrukturer bare kan løses ved desentralisering av makt og større autonomi for mindre enheter. Dette er et stort filosofisk spørsmål, og den overfladiske gjentakelsen av mantraet global utfordring - global løsning - kan nok med hell vurderes atskillig mer grundig enn hva som ofte har blitt gjort i offentlig debatt og i menneskenes tenkning.

4. Forsker Gisle Hannemyr, Institutt for informatikk, UiO. Tema: Privacy Enhancing Technology og Privacy by Design - hva er det og hvilken nytte kan det ha?

Hannemyr startet med å slå fast at det internasjonalt er et vidt spektrum av oppfatninger rundt personvern. Hvordan bør forholdet mellom regulering med teknologi regulering med lov være? Lawrence Lessig sa i 2000 at "Code is law." Skal jus utøves gjennom teknologi? "Vi er i dag i svært stor grad integrert i nettverk (social-technical ensembles) som består av både samfunnsmessige og tekniske komponenter, og som kan virke bestemmende for vår situasjon." Lessig sier: "Every age has its potential regulator, its threat to liberty...Ours is the age of cyberspace. It, too, has a regulator. This regulator, too, threatens liberty... This regulator is code."

Hannemyr mente at det burde bli et perspektivskifte fra trusler til muligheter til styrking av personvernet. Disse mulighetene foreligger.

Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary and unwanted processing of personal data, without the loss of the functionality of the information system." (Blarkom, Borking and Olk, 2003) Men også en samlebetegnelse på ICT-tjenester.

Privacy by Default is a software design concept that is presently being considered by a number of data protection authorities. Broadly defined, Privacy by Default would prohibit the collection, display, or sharing of any personal data without explicit consent from the customer. Også prinsipp for programvare der samtykke gis/kreves mht. håndtering av personopplysninger.

Privacy by Design er et begrep som er skapt og popularisert av Ann Cavoukian, Information & Privacy Commissioner, Ontario, Canada.

Privacy by law: Et internsjonalt eksempel på dette er det såkalte EU cookie directive. Hannemyr påpekte at dette er uten praktisk betydning fordi det ikke skiller mellom intern sporing på en nettside, og ekstern sporing hvor tredjepartsaktører ("third party cookies") sporer brukerens atferd på et større antall nettsider. Et norsk eksempel som Hannemyr trakk frem er Personopplysningsloven. Paragraf 12 i denne loven sier at "Fødselsnummer og andre entydige identifikasjonsmidler kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering." Akkurat her syndes det mye¸ og spredningen av person- og fødselsnummer er betydelig. For å beskytte individet kan man bruke "hash"-løsninger slik at koden ikke kan reverseres og bringes tilbake til utgangspunktet. Dermed kan man heller ikke spore tilbake til individet. Her kan man bruke en design ved at man unngår sentral lagring, og i stedet legger informasjonen i et smartkort eller en annen enhet som individet bærer med seg. Designerne bør få opplæring i hvordan benytte PET's og Privacy by Design i konstruksjoner og tekniske løsninger. Lovgivere bør på sin side bli kjent med og være

oppmerksomme på at regulering bør befatte seg med mål og ikke med de konkrete mekanismene som står til rådighet for designerne, mente Hannemyr. Dette er et meget viktig poeng, fordi når premissene først er lagt vil senere valg baseres på disse.

5. Førsteamanuensis Tone Bratteteig, Institutt for informatikk, UiO. Tema: Kan brukermedvirkning gi bedre personvern?

Bratteteig arbeider sammen med Hannemyr, og er opptatt av brukermedvirkning i design av informasjonssystemer. Bratteteig beskrev hvordan systemer er utformet slik at brukeren skal gjøre bestemte ting, men ofte gjør ikke folk hva som systemet legger opp til at brukeren skal gjøre. For å forstå brukerne, for å forstå at de ikke handler med vond vilje eller er dumme, må bruken undersøkes. Bruk er veldig mange ting, og bruk kan også være automatiserte funksjoner der brukeren ikke er oppmerksom på hva som skjer. Brukere er mange forskjellige folk, i mange forskjellige roller og med forskjellige interesser. På alle de arenaene vi bruker teknologiske systemer, ser vi dette. Ofte brukes det samme system av mange brukere, men samme bruker kan også bruke mange ulike systemer. Bruk i praksis er derfor viktig å forstå. Designere tenker på tekniske løsninger, og ønsker å lage en løsning som er mulig og ønskelig. Vi lager alltid noe som bygger på noe vi har sett og er kjent med fra før. Så strekker vi metoder og materialer litt lenger. "Er det mulig å gjøre sånn?"

Selv om det har blitt utviklet et system som fungerer godt i seg selv, er det ikke sikkert at det fungerer i den sammenhengen hvor det skal inngå i praktisk bruk. Bruksorientert design tenker på helheten. Brukerundersøkelser tar sikte på å finne ut hvordan ulike typer design oppfattes av brukeren. Personvern vil være en del av dette. Hvordan skal man bevare personvernet for både ansatte og pasienter? En utfordring her er den digitale logikken. Hva som er spesielt med datamaskiner: De lager representasjoner, abstraksjoner. Det viktigste de gjør, er å forandre input til output. Vi kan representere hva som helst med hva som helst. En utfordring er at bruk av slike maskiner er en kunnskapsbasert aktivitet. Bruk kan karakteriseres ved samspillet mellom betingelser for aktiviteten og brukeren.

En annen utfordring er at det er skille mellom innhold og form. En stor utfordring er at det er et skille mellom representasjon og virkelighet. Vi lager kategorier. Noen kategorisystemer lager virkeligheten, for eksempel har du ikke en diagnose får du ikke sykepenger. Enda en utfordring er bruk uten bruk. Er det greit at vi samler opplysninger om folk, er det greit at vi flytter grensene mellom hva som er personlig og hva som er offentlig tilgjengelig? Endelig er en viktig utfordring brukermedvirkning i design. Hvordan skal designet være for å tilpasses bestemte tilstander? Medbestemmelse er et ideal som ikke alltid er så lett å gjennomføre i praksis.

6. Advokat Rolf Riisnæs, fra WikborgRein. Tema: Privat regulering: Internkontrollsystemer, personvernpolicyer, bruk av avtaler, bransjevise normer og standardisering.

Riisnæs arbeider med internkontrollsystemer, personvernpolicyer, bruk av avtaler, bransjevise avtaleformer og standardisering. Han mener at internkontroll er det viktigste men kanskje mest undervurderte elementet i personopplysningsloven. Gjennom loven innføres en plikt til å etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av personopplysningsloven. Internkontrollen vedrører kontroll, overvåkning og dokumentasjon av hvorvidt disse kravene er overholdt. Internkontrollbestemmelsene har lett for å bli oversett og "falle under radaren." Men de er viktige, for ikke å si overordnet viktige. Tiltakene gjelder rutiner for oppfyllelse av plikter, informasjonssikkerhet, sikring av de registrertes rettigheter og prosedyrer og rutiner for identifisering og håndtering av avvik. Har vi innhentet samtykke, har vi lovlig grunnlag for den behandlingen vi holder på med? Er det etablert rutiner for sletting av opplysninger, kan vi være sikre på at de faktisk blir slettet?

Hvis man gjennomfører kartlegging av slike faktorer identifiserer man hvilke umiddelbare tiltak som trenger å gjennomføres. Hvilke opplysninger innhentes og lagres? Hvem gjør det, om hvem innhentes opplysninger, hvorfor og hvor lenge beholdes opplysningene? Hvordan er forholdet til innhenting av samtykke? Kravet til et informert samtykke kan knyttes opp mot en aktuell regel, for eksempel den personvernerklæringen som finnes på Datatilsynets hjemmesider. Et informert samtykke forutsetter at den det innhentes opplysninger om kjenner til betingelsene, og forstår hva som foregår. Dette setter i praksis begrensninger for hvor mye vi kan forvente av et krav om samtykke - hvor informert er i realiteten et samtykke? Databehandleravtaler sikrer det rettslige grunnlaget for databehandlerens behandling av personopplysninger. De skal sikre klarhet og bevissthet rundt partnernes roller og hva behandlingen kan og skal bestå i. Den du inngår databehandleravtale med, er ikke nødvendigvis den som behandler dataene. Hvilke krav stiller dette til en databehandlingsavtale? Hvilke krav må kunne stilles til underleverandører og underordnede ledd i databehandlingssystemet?

Bransjevise atferdsnormer og standardisering har ingen fremtredende stilling i norsk rett, men har likevel praktisk viktighet på visse områder. Bransjevise atferdsnormer finnes, vi har en bransjenorm for e-billettering som gjør at det er mulig å reise anonymt også med elektroniske billettsystemer. Inkassobransjen har normer som er utarbeidet av Datatilsynet.

7. Fagdirektør Cecilie B. Rønnevik, Datatilsynet. Tema: I hvilken grad bør personvernlovgivning være teknologiuavhengig?

Cecilie Rønnevik har arbeidet med personopplysningsloven i ni og et halvt år. Prinsippet om "teknologinøytral regulering" innebærer at man favoriserer eller forskjellsbehandler urimelig visse former for teknologi eller visse tjenester. Vi ønsker også å hindre at reguleringen påvirker teknologiutviklingen. Datatilsynet mener at ny teknologi er i utgangspunktet hverken positiv eller negativ for personvernet. Det er hvordan teknologien brukes som er avgjørende. Selv om teknologien vil gjøre at en behandling blir mulig, enklere eller billigere, så er den rettslige adgangen like begrenset som før. Personopplysningsloven er i all hovedsak formålsstyrt, det er behandlingsformålet som er styrende for hvem som kan behandle opplysningene og hvordan de skal behandles og brukes. Teknologien er uansett relevant ved anvendelsen av regelverket. Behandlingen må følge EMK artikkel 8 om forholdsmessighet.

Eksempler på teknologiens relevans i personvern er spørsmålet om hva en bestemt teknologi innebærer. Hva er for eksempel kameraovervåkning? Hva er forskjellen mellom kameraovervåkning i tradisjonell forstand og gjenkjennelsesteknologi? Kameraene er på en måte blitt et symbol på overvåkningssamfunnet, men hvor reelt er dette?

En teknologibasert lovregulering kan ta utgangspunkt i konkrete hensyn som er relevante for den aktuelle teknologien. Men det er flere problemer med den. Reguleringen vil måtte bli omfattende hvis det også skal tas høyde for de ulike behandlingsformålene. Teknologien vil også gjerne utvikle seg raskere enn regelverket klarer å følge med, og derfor blir lovgivningen foreldet.

Derfor mente Rønnevik at lovgivningen i størst mulig grad bør være teknologinøytral, slik at behandlingene reguleres likt, uavhengig av metoder og teknologi. Det er altså formålet, altså i denne konteksten viljen til å sikre personvernet, som det bør tas utgangspunkt i som grunnpremiss.

--

Per Inge Østmoen