Fra rådet til tinget

Teknologirådet

Ein ny personvernpolitikk

Fra rådet til tinget nr. 17, november 2007

Samandrag

Sterk vekst i datainnsamling og lagring
Utviklinga innan IT og mobil kommunikasjon gjer svært utvida rom for innsamling, lagring og analyse av data om den enkelte. Alle stader vi ferdast – på internett, i trafikken eller på tur med mobilen slått på – legg vi igjen elektroniske spor. Det er òg fremma forslag om systematisk lagring av slike spor, blant anna gjennom datalagringsdirektivet og kvitvaskingsdirektivet frå EU. Ei europeisk studie Teknologirådet har leia, har sett på utviklinga innan IKT og vurdert dei konsekvensane ei slik utvikling kan få for personvernet.

Uoversiktlege konsekvensar på lang sikt
Sjølv om den enkelte kan vere klar over at teknologien legg igjen spor, er det totale biletet så omfattande at ein ikkje kan rekne med at vanlege brukarar kan vurdere konsekvensane for personvernet på lang sikt. Difor har styresmaktene ei viktig rolle i å legge til rette slik at personvernet får best mogleg kår.

Sikkerheits- og overvakingssystem må datostemplast og evaluerast
Ein del tiltak som grip inn i personvernet er meint å beskytte samfunnet mot kriminalitet eller terror. Det er viktig at slike ekstraordinære tiltak ikkje automatisk blir permanente, og at ein med jamne mellomrom evaluerar om systemet er naudsynt. Vidare bør ikkje system eller tiltak som handsamar personopplysningar takast i bruk utan at det er gjennomført ei vurdering av konsekvensane for personvernet.

Folk bør få tilgang til eigne mapper og loggar
Eit resultat av stadige krav til effektivisering og betre offentlege tenester er meir utveksling av informasjon mellom ulike etatar. Slik samanstilling av informasjon gjer borgaren meir gjennomsiktig for forvaltninga. Dette bør balanserast med at borgaren òg får høve til å følje sin eigen saksgang, inkludert loggar som syner kven som har hatt tilgang til hans eller hennar informasjon.

Kvifor treng vi ein ny personvernpolitikk?

Personvern er ein rett og ein viktig verdi i samfunnet vårt. Den teknologiske utviklinga har blant anna har gjort mobiltelefon, bankkort, autopassbrikker og data uunnverleg for dei fleste av oss. I praksis er det umogleg å delta i samfunnet i dag utan å legge igjen elektroniske spor – og på denne måten svekke personvernet.

Personvernet blir fortrengt av andre behov
Borgarane i det moderne samfunnet må heile tida sette personvernet opp mot andre goder for å kunne fungere.

Tryggleik
75% av alle nordmenn synest det er greitt med meir overvaking viss det kan føre til eit tryggare samfunn, viser ei undersøking Teknologirådet har gjennomført. Samstundes meiner nær halvdelen at det ikkje er greitt at ein blir overvaka om ein ikkje har gjort noko gale.

Tilgang til informasjon og tenester
Dei fleste veit at det finst store mengder personopplysningar om dei i offentlege register og private kundedatabasar. Dette betyr at andre kan få tilgang til deira trygdestatistikk eller helsedata, men det betyr òg at dei sjølv kan få betre og meir tilrettelagde tenester frå det offentlege.

Deltaking i samfunnet
Folk flest ønskjer å ha ein beskytta privatsfære – men dei vil òg bruke mobiltelefon og kredittkort. I løpet av kort tid har meir enn 400 000 nordmenn registrert seg på Facebook, og mange legg ut bilete og til dels personleg informasjon på denne eller andre nettstader. I aldersgruppa 16-24 år nytter nesten 90% såkalla lynmeldinger. Det er naudsynt å gje opp noko av vernet om privatlivet for å kunne vere ein deltakar på den sosiale arenaen.

Tenester som er brukarvennlege og lettvinne
Det er greitt å kunne vere anonym av og til, men til kva for ein pris? Det er raskare og enklare å kjøre gjennom bomringen dersom ein har ei autopassbrikke, og når datamaskina aksepterer informasjonskapslar (cookies) er det ikkje naudsynt å logge inn på nytt kvar gong ein vitjar ein nettstad. Kontantar erstattast i aukande grad med betalingskort. Kvifor? Fordi det er lett.

Korleis ein vel å balansere desse områda mot personvernet er oftast eit val for den enkelte. Trass i det vart valet i stort grad påverka av politikk og lovar frå styresmaktene:

- Finst det anonyme alternativ?
- Kva for krav blir sette fram når det skal etablerast nye offentlege system?
- Kor skal det vere lov å sette opp kamera for overvaking?

I Noreg veit vi at innbyggjarane har stor tillit til styresmaktene, og dette gjer det ekstra viktig at dei forvaltar dette ansvaret på ein god måte.

Spor som er lagra blir ikkje sletta
Om du passerer ein bomstasjon, har mobiltelefonen slått på, surfar på internett eller har kontakt med styresmaktene, legg du igjen elektroniske spor i form av data. Utviklinga i IT-sektoren dei siste åra har gjort at det oftast løner seg å behalde data framfor å slette dei.

Fordi så mange av dei teknologiane vi bruker til dagleg verker inn på personvernet vårt, er det i praksis blitt umogleg for den enkelte å halde oversikta over alle spora som blir lagt igjen, og ikkje minst å verne seg mot dette.

Eit ubalansert forhold
Mange har eit bevisst forhold til det å registrere seg på nett eller gi frå seg personleg informasjon i andre høve. Likevel kan ein ikkje forvente at dei skal ha oversikt over de langsiktige, samla konsekvensane dette har for personvernet. Det er stor skilnad mellom private og profesjonelle aktørar når det gjeld kunnskap om korleis persondata kan takast i bruk og verdien av slike data. Profesjonelle aktørar har ofte økonomiske interesser i dei data som blir samla inn, og derfor bør dei òg ha eit større ansvar.

Den som ønskjer å vere mest mogleg anonym i samfunnet i dag, vil fort oppdage at det både kan krevje mykje innsats og vere dyrt økonomisk: Anonyme løysingar gjer det ofte vanskeleg med kvantumsrabattar og andre tilbod, og dei fleste personvernfremmande teknologiane krev både innsats og kunnskap for den som vil ta dei i bruk.

Viktig med ei "føre var"-tilnærming
Utviklinga innan IKT kjem ikkje til å snu. Dette betyr at system med dårleg design som blir utvikla og tatt i bruk i dag kan påverke personvernet i heile levetida til systemet. Til dømes kan data som ikkje blir sletta nyttast til formål ein ikkje eingong hadde vurdert då systemet vart utvikla. Dei langsiktige effektane av den utviklinga vi er inne i er uklare: Korleis vil dei vala vi gjer i forhold til personvern i dag påverke vår måte å leve på i framtida?

Å bruke eit "føre var"-prinsipp når nye system skal utviklast betyr ikkje å stanse utviklinga av IT-system. Utfordringa ligg i å designe systema slik at dei òg tar omsyn til personvern. Dette kan til dømes bety at det ikkje blir lagra meir data enn naudsynt, og at data blir sletta når dei ikkje lenger er i bruk.

Utfordringar for personvernet – og korleis dei kan møtast

Den europeiske studia legg fram sju utfordringar knytt til personvern, saman med forslag til tiltak som kan bøte på desse.

Utfordring nr 1: Tryggleik utan at personvernet blir svekka
Styresmaktene ønskjer å skape et sikkert samfunn, til dømes gjennom å innføre tekniske løysingar eller overvaking. Som ein grunnregel bør fordelane ved slike løysingar vurderast nøye og samanliknast med alternative løysingar: Kan betre lys i gatene ha same effekt som eit kamera?
I enkelte tilfelle kan overvakingstiltak eller –system rettferdiggjerast fordi dei faktisk gjer auka tryggleik og eit sikrare offentleg rom.

■ *Overvakingssystem bør berre takast i bruk om dei er effektive, vanskelege å omgå og vil føre til reell betring av tryggleiken*
Proporsjonalitetsprinsippet slår fast at overvakingssystem berre må innførast om fordelane veg tyngre enn dei sosiale ulempene, inkludert overtramp mot personvernet, tap av autonomi, sosial diskriminering eller påtvungen konformitet.

■ *Overvakingssystem bør evaluerast regelbunde*
Når nye overvakingssystem blir innført i samfunnet, til dømes antiterrortiltak, nye politimetodar eller strengare grensekontroll, bør tiltaket evaluerast nøye. Verknadene av systemet – både dei positive og negative – bør evaluerast regelbunde av eit uavhengig offentleg organ.

Overvakinga bør vere effektiv, ikkje lett å omgå, og ha reell verknad på tryggleiken for at innbyggjarane sitt personvern ikkje skal bli krenka unødig. Om eit overvakingssystem fører til ein betring i tryggleik som rettferdiggjer dei sosiale ulempene, bør tiltak som kan minimere desse ulempene setjast i verk.

Før eit system blir sett i drift bør ein fastsette når tiltaket skal evaluerast, eller avviklast om det ikkje lenger er behov for det (såkalla *sunset clause,* eller *datostempling*). Tiltak som er sette i verk i ein særskild situasjon bør ikkje automatisk bli permanente.

Utfordring nr 2: eForvaltning gjer borgarane meir gjennomsiktige for styresmaktene
Hovuddrivkreftene bak eForvaltning er ønsket om auka effektivitet og lågare kostnader i offentleg administrasjon, saman med betre, meir tilgjengelege tenester for brukarane. Løysingar for eForvaltning krev ofte auka utveksling av informasjon mellom ulike etatar, til dømes kan sosialkontoret (NAV) ha behov for data både frå helsesektoren og skatteetaten. Ei viktig utfordring er korleis teknologien kan bidra, ikkje berre til å gje meir effektiv forvaltning, men også til å styrke personvernet til den enkelte borgar.

■ *Gje borgarane reelt høve til informert samtykke*
Det er kan utviklast teknologiske løysingar for å gjere det lettare for borgarane å gje *frivillig, spesifikt og informert* samtykke til utlevering av data. Utveksling av persondata mellom ulike etatar bør berre skje etter eit formelt spørsmål til brukaren.

■ *Gje brukarane tilgang til eigne mapper og loggar*
Det er fullt mogleg å designe IT-system slik at brukarane sjølv kan få tilgang til å sjå "mappa" si. Dette vil gjere det enklare for brukarar å nytte retten til innsyn, som òg kan bli meir omfattande enn i dag.

Det bør vere mogleg for den enkelte å følgje sin eigen saksgang og å studere loggar for å sjå kven som har oppretta, endra eller slått opp på "deira" informasjon. Dette er spesielt viktig fordi slike elektroniske mapper har gjort det lett for etatar og sakshansamarar å utveksle data.

Utfordring nr 3: Handhevinga av personvernet er for svak
I dei fleste europeiske land finst det personvernlovgiving, men anledninga til å handheve denne er ofte svært avgrensa.

■ *Styrk Datatilsynet sitt mandat*
Styresmaktene bør vurdere om Datatilsynet skal få større høve til å sette i verk tilsyn, etterforske saker der det er mistanke om overtramp, og ha kontinuerleg tilsyn med handsaminga av persondata i verksemder. Som eit minstekrav bør tilsynet ha kapasitet til å handsame klagesaker og utstede førelegg.

■ *Sanksjonane bør stå i forhold til vinsten ved overtramp mot personvernet*
Om det ikkje finst passande sanksjonar eller straffer vil private verksemder ha låg motivasjon for å utvikle og innføre IT-system som tek omsyn til personvernet, særleg om slike system inneber ein auka kostnad. Personvernlovgivinga bør oppdaterast slik at handhevinga kan virke preventivt i forhold til verksemder som ignorerer omsynet til personvernet. Straffa bør stå i forhold til vinsten.

Utfordring nr 4: Personvern tas ikkje med når systema blir utvikla
I mange høve kunne krenking av personvernet vore unngått om vern av persondata hadde vore med allereie i dei første fasane i utviklinga av eit nytt system. Dette gjeld både for juridiske og tekniske løysingar.

■ *Vurdering av konsekvensar for personvern*
Ei vurdering av konsekvensane for personvernet (Privacy impact assessment, PIA) er ein prosess som skal hjelpe verksemder å vurdere om tekniske system dei utviklar eller endrar vil ha følgjer for handsaming av personopplysningar.

Ei slik konsekvensvurdering skal gjennomførast allereie i planleggingsfasen av prosjektet. Slik kan personvernprinsipp takast med når prosjektet blir designa, eller prosjektet kan i verste fall stoppast før utgiftene blir for store. Slike vurderingar er det krav om ved offentleg innkjøp blant anna i Canada.

Det er billegare å byggje omsyn til personvernet inn i systema frå starten enn å endre systema i ettertid.

■ *Personvernfremmande teknologiar (PET)*
Personvernfremmande teknologiar (Privacy enhancing technologies, PET) bør systematisk integrerast i utviklinga av nye system. Slike teknologiar kan ikkje løyse alle personvernproblem, men dei kan i stor grad bidra til å minimere den mengda av data som blir samla inn og analysert.

Eit viktig prinsipp er at berre dei data som er naudsynte for å utføre oppgåva blir samla inn – ikkje data det berre er "kjekt å ha". Det å levere tenester utan å samle inn for mykje data bør oppmuntrast.

■ *Bidra i utviklinga av internasjonale standardar for personvern*
Det er behov for internasjonale standardar for personvern. Slike standardar er ein føresetnad for å kunne utvikle IT-system i tråd med personvernet. Det er fleire fordelar med å ha internasjonale standardar: Dei aukar tilliten hos forbrukarane og sikrar lik handsaming av person vern over heile verda, og dei bidrar til at det blir lettare for verksemder å opptre ansvarleg.

Redaksjon
Christine Hafskjold, Tore Tennøe

Abonnement
post@teknologiradet.no
Du kan lese alle utgåver av *Fra rådet til tinget* på
www.teknologiradet.no

Utfordring nr 5: Verda rundt oss blir trådlaus
I stadig større grad er vi omgitt av trådlause nettverk som kommuniserer med gjenstandar vi ber på oss (såkalla *intelligente omgivnader)*. Det kan vere med mobiltelefonen eller PC-en, men òg med autopassbrikka i bilen vår eller små brikker i varene vi har kjøpt, kleda vi har på oss eller ID-kort vi ber med oss. Norske pass som er produsert etter oktober 2005 inneheld til dømes ein liten radiosendar (RFID).

■ *De intelligente omgivnadane må bli synlege*
Alle slike system bør innehalde funksjonar som gjer at dei kan garantere transparens for brukaren – det vil seie at brukaren kan vite kva for data som blir utveksla og når det skjer.

Gjenstandar som inneheld sendarar (til dømes RFID-brikker) bør vere tydeleg merka. Når ein kjem inn i eit rom eller går forbi stader der det er installert utstyr for å lese brikkene, bør dette vere skilta. I fall det er mogleg, bør løysingar leverast slik at "av" er standard innstilling, og at den som ønskjer å vere "på" må gje aktivt samtykke.

Innhaldet i dette innspelet er basert på eit prosjekt Teknologirådet har gjennomført saman med kollegaer i Danmark, Østerrike, Nederland, England, Belgia og Sveits. Saman har vi gått gjennom personvernet si stilling i Eurpoa. Resultata er samanfatta i rapporten "ICT and Privacy in Europe – Experiences from technology assessment of ICT and Privacy in seven different European countries".

Teknologirådet er eit uavhengig, rådgjevande organ for teknologivurdering. Det blei oppretta ved kgl. res. 30.april 1999 etter initiativ frå Stortinget. "Fra rådet til tinget" blir utgitt av Teknologirådet sitt sekretariat.