Representantforslag 94 S

(2011–2012)

fra stortingsrepresentantene Per Sandberg og Bård Hoksrud

Dokument 8:94 S (2011–2012)

Representantforslag fra stortingsrepresentantene Per Sandberg og Bård Hoksrud om IKT-havarikommisjon og styrket personvern

Til Stortinget

Bakgrunn

Norske myndigheter samler inn store mengder informasjon om den enkelte innbygger i dette landet. Det er et problem i forhold til personvernet, ikke minst når myndighetene lekker informasjonen til uvedkommende. Det offentlige Norge er allerede blant de dårligste på personvern, og utviklingen går i feil retning. Forslagsstillerne tar i dette representantforslaget til orde for en IKT-havarikommisjon, etter mønster fra flyhavarikommisjonen, for å begrense skadevirkningene av det offentliges lemfeldige behandling av sensitive personopplysninger, og for å finne årsaken bak statlige IKT-havarier.

Skattemyndighetene

Skatteetaten har lenge vært regnet for å være blant de beste innen offentlig sektor på IKT, men portalen Altinn opplevde et alvorlig sikkerhetsbrudd tirsdag 20. mars 2012, noe som førte til at hele portalen ble stengt. I en periode kunne 1 500–2 000 personer se profilen med fødselsnummer til Oslo-mannen Kenneth (36), da de logget seg inn for å sjekke selvangivelsen. I en pressemelding 23. mars 2012 skriver Altinn følgende:

«Personopplysninger skal ikke kunne lastes ned og 'caches' i Altinn, men en utilsiktet hendelse i 'cachemodulen' førte til at en persons navn og fødselsnummer ble synlig for andre brukere i Altinn i en periode på 17 minutter før løsningen ble stengt ned kl 18.34 tirsdag 21. mars.»

Ifølge en artikkel på Teknisk Ukeblads nettside 19. mars 2012, slaktes Altinn i en hemmelig rapport fra sommeren 2011 som Det Norske Veritas utarbeidet på oppdrag fra Næringsdepartementet. I rapporten kommer det visstnok frem at testmetodene ikke har vært gode nok og at det er en risiko for at løsningen ikke kan bygges ut til å håndtere tjeneste- og trafikkøkningen. Altinn har også tidligere hatt problemer, blant annet var sidene nede, ifølge Dagbladet 22. mars 2011, fordi trafikken ble høyere enn forventet.

Skattelistene ble tidligere lagt åpent ut på Internett med informasjon om fullt navn, inntekt, formue, fødselsår og postnummer, og man trengte ikke engang elementære norskkunnskaper for å finne frem i systemet. Denne praksisen ble strammet inn fra 2011 slik at skattelistene for 2009 er de siste som ligger åpent på Internett. Det er imidlertid fortsatt mulig å snoke på andre, men man må nå ha egen PIN-kode og logge seg inn på MinID. Skattelistene er et eksempel på hvordan Arbeiderpartiet, Sosialistisk Venstreparti og Senterpartiet har utlevert informasjon om norske borgere som kan brukes av utenlandsk mafia til å identifisere potensielle ofre i Norge. Forslagsstillerne mener at folks inntekt og formue er å betrakte som sensitive personopplysninger, og at staten ikke skal utlevere slik informasjon til uvedkommende.

Transport

Norske bilister som kjører på norske veier overvåkes på flere forskjellige måter. Frem mot 2013 kan man få så mange som 40 strekninger der man måler gjennomsnittshastighet mellom to punkter på veien. Systemet innebærer at alle som passerer det første punktet avfotograferes, noe Datatilsynet har advart

imot. Fremskrittspartiets representanter fremmet i forbindelse med statsbudsjettet for 2012 forslag i Innst. 13 S (2011–2012) der man anmodet Stortinget om å be regjeringen snarest avvikle strekningsvis-ATK. Statens vegvesen, Vegtrafikksentralen overvåker dessuten biltrafikken på Østlandet med over tusen videokameraer spredt utover veinettet.

Statens vegvesen har også gjort livet enklere for kriminelle. Dersom en kriminell ser en familie på bilferie, kan vedkommende sende bilens registreringsnummer på SMS til 2282 og få utlevert fullt navn og hjemkommune til bilens eier. Denne informasjonen kan brukes til å finne frem til full adresse, slik at familiens hjem kan ranes mens de fortsatt er på bilferie. Myndighetene i mange andre europeiske land, som for eksempel Polen, nekter å utlevere slike opplysninger til uvedkommende.

En hovedutfordring innenfor samferdsel er at man innfører systemer uten å ta hensyn til personvern i designfasen, det vil si PET («Privacy-Enhancing Technologies») og «Privacy by Design».

Politi og nødnett

Forslagsstillerne vil også vise til den håpløse situasjonen som råder innen justissektoren. Det meste av datautstyr er gammelt, noe som medfører store utfordringer innen den enkelte etat og i samhandling med andre. I denne sammenheng vises det til innføring av ny straffelov som ble ferdig behandlet og vedtatt på Stortinget i 2009. Det var da forutsatt at nytt IT-system, som kunne håndtere den nye loven, skulle implementeres innen 2012–2013. Etter forslagsstillernes oppfatning var dette i seneste laget, når man vet at lovendringsprosessen allerede hadde vart i mange år før loven ble vedtatt. Likevel har ikrafttredelsestidspunktet blitt utsatt to ganger allerede, og loven kan ikke begynne å virke før tidligst i 2017. Fra evalueringen av 22. juli 2011 vet man også at systemet med varsling av riksalarm ikke fungerer. Dette skyldtes rot med dataanlegg og for dårlige systemer og rutiner for effektiv varsling.

Videre har forslagsstillerne blitt informert om problemer med IKT-løsninger i domstolene. Systemet har vært utdatert i mange år, og det nye systemet som nå brukes fungerer dårlig. Dette fører til at plattformen ofte kollapser og gir dermed store negative konsekvenser for dommerne. Dommerne har gitt mange eksempler på at dommer må skrives på nytt fordi den som er skrevet har blitt borte i datasystemet. Videre berettes det om protokollasjoner som blir borte, slik at vitner som har vært kalt inn, må kalles inn på nytt. Det har også vært episoder hvor meddommere er kalt inn for å undertegne den endelige dommen, men hvor de har måttet dra med uforrettet sak fordi det ikke har vært mulig å ta utskrift. Etter forslagsstillernes oppfatning er dette helt uakseptabelt for en nasjon som tar mål av seg til å være et moderne samfunn.

Nødetatene er svært misfornøyde med nødnettet, og hovedårsaken er at Tetra ikke har datakapasitet. Dette kom dramatisk til syne den 22. juli 2011, da brannvesenet etterlyste tegninger av regjeringsbygget. Nødetatene ville sende bilder av sårede til Oslo universitetssykehus, Ullevål (OUS), for å få råd på stedet, men det fungerte ikke. Tegninger over høyblokken i regjeringskvartalet fantes selvsagt digitalt, men kunne ikke sendes til redningsmennene på stedet fordi Tetra ikke hadde kapasitet. Da Stortinget i 2004 behandlet spørsmålet om nødnett i Budsjett-innst. S. nr. 4 (2004–2005), gikk Fremskrittspartiets medlemmer av komiteen inn for en teknologinøytral anbudsrunde med vekt på dataoverføringskapasitet som åpner for direktesendte bilder, medisinsk data og posisjoneringsinformasjon for alle enheter på et ulykkessted. Begrunnelsen for dette var at det hadde vært for mye oppmerksomhet på en teknologi (TETRA) til fortrengsel for de behov etatene har, og muligheter som ligger i stadig nye teknologiske vinninger. I stortingsbehandlingen ble det understreket, som en forutsetning, at nødnettet ikke skulle være et utviklingsprosjekt. Her ble Stortinget ført bak lyset, alt som har blitt gjort har vært utvikling. Mange av innvendingene fra Fremskrittspartiets medlemmer av komiteen mot den valgte løsningen har dessverre slått til. Resultatet har vært forsinkelser, problemer med implementeringen av de tekniske løsningene og store kostnadsøkninger. Tetra er i ferd med å bli en varslet katastrofe. Ny teknologi gjør at man kunne brukt eksisterende nett, 3G- og 4G-nettene til Telenor, Netcom og Network Norway samt CDMA-nettet til Ice, GSMR-nettet til Jernbaneverket og tilgjengelig «Wi-Fi» i byområder. Alt dette får man i dag på én brikke. Kommunikasjon kan krypteres og ved store ulykker kan kapasitet prioriteres til nødetatene. Staten hadde kunnet spare mange milliarder kroner, samtidig som sårbarheten ville være langt mindre ved at man kunne hatt mange nett å spille på om ett faller ut. Samtidig kunne man ha fått datakapasitet til for eksempel skanning av fingeravtrykk, ID og lignende. Forslagsstillerne peker på at saken om nødnett tidligere har vært gjenstand for uforsvarlig behandling i Stortinget, og viser til protokolltilførsel fra medlemmene fra Fremskrittspartiet og Høyre i transport- og kommunikasjonskomiteens møte 8. juni 2009, etter å ha tapt voteringen om ikke å behandle St.prp. nr. 83 (2008–2009) om økt kostnadsramme for første byggetrinn i vårsesjonen:

«Komiteens medlemmer fra Fremskrittspartiet og Høyre avviser behandling av ytterligere nye saker før Stortinget 19. juni 2009 avslutter før sommeren. Med to uker igjen til avslutningen av flere saker og debatt om disse sakene i Stortinget, vil behandling av ytter-

ligere saker etter disse medlemmers oppfatning ikke kunne gjennomføres på en forsvarlig måte.»

Ifølge Tidskrift for Den norske legeforening 18. august 2010 brukes helsevesenets radiosamband aktivt i bare halvparten av norske legevaktdistrikter. En grunn til dette kan kanskje være at avisredaksjonene lytter på helseradioen, noe som viser at det er et stort behov for et sikkert nødnett.

Innenfor Schengen-landene trenger man egentlig ikke pass, men folk i Norge har hittil ikke hatt noen annen form for ID som de kan bruke i Schengen. Unntaket er landene i den nordiske passunionen, siden man i 1958 ble enige om opphevelse av passkontrollen ved de fellesnordiske grensene. Man har i løpet av de siste 10 årene derfor planlagt å få på plass et frivillig nasjonalt elektronisk ID-kort, men det siste man har hørt om kortet er at det kan komme på plass i løpet av 2013. I mange land er det obligatorisk å gå med ID-kort, for eksempel i Hong Kong (fra 11 år) og Thailand (fra 7 år). I Norge er det obligatorisk med ID-kort i rengjøringsbransjen og byggebransjen for å forhindre grov utnyttelse av arbeidskraft.

Forslagsstillerne er imot å gjøre elektroniske ID-kort obligatoriske for hele befolkningen, og er skeptiske til den økte overvåkningen dette kan medføre. I tillegg er det alltid en risiko for at frivillige offentlige ID-kort på sikt kan gjøres om til obligatoriske. Elektronisk ID er viktig og vil bedre sikkerheten betydelig for borgerne og det offentlige. Det finnes gode kommersielle løsninger, og det er ingen grunn til å utvikle noe selv fra bunnen. Forslagsstillerne mener at norske myndigheter bør gå i forhandlinger med sine partnere i Schengen-landene for å få på plass en godkjenningsordning for private ID-kort. På den måten vil for eksempel norske bankkort kunne godkjennes som ID-kort i Schengen-området, uten at offentlige løsninger må utvikles.

IKT i helsesektoren

Når man går til en fastlege eller psykolog i Norge, registreres opplysningene man gir fra seg i en elektronisk pasientjournal (EPJ). Selv om man gir fra seg denne informasjonen i full fortrolighet, vil blant annet helsepersonell og Nav-ansatte som jobber med helserelaterte oppgaver (jf. § 21-4 i folketrygdloven), få tilgang til pasientjournalen. Dette åpner for snoking i svært personsensitive opplysninger, og kan også føre til at pasienter holder tilbake informasjon om egen helsetilstand. NRK Sørlandet hadde for eksempel en artikkel 6. april 2011 om en sykehusansatt som snoket flere hundre ganger i pasientjournaler. Elektronisk pasientjournal er imidlertid et skritt i riktig retning med hensyn til papirbaserte journaler som for eksempel vaskehjelpen på sykehuset i verste fall kan få tilgang til. Manglende IKT-systemer i Oslo-sykehusene har endt med en situasjon der pasientjournaler blir sendt i taxi og post mellom de ulike sykehusene, med den risiko det medfører både for persondata på avveie, men også for at behandlingen av pasientene blir unødig utsatt.

IKT-systemene i norske sykehus henger langt etter de andre europeiske land. Stadig flere sykehus verden over går i dag over til å være helt papirløse, i den forstand at alle prosesser og informasjonsutvekslinger skjer elektronisk. Felles for disse sykehusene er at de bruker 4–6 pst. av sine budsjetter til investeringer og drift av IKT-systemene, i Norge bruker man 2,2 pst. av budsjettene på tilsvarende tjenester. Norske helsetjenester er preget av enorme IKT-systemer som ikke snakker sammen. I de mest graverende tilfellene kan et enkelt helseforetak ha over 100 ulike IKT-systemer som fungerer uavhengig av hverandre. Dette hindrer nødvendig effektivitet, informasjonsflyt og sikkerhet for pasientene. I fagmagasinet «Overlegen» fra oktober 2011 kommer det frem at det totalt i Oslo universitetssykehus eksisterer mer enn 1 000 dataprogrammer, hvorav 200–250 er direkte knyttet til pasientbehandlingen. Investeringsbehovet innen IT alene i OUS er i samme artikkel estimert til å være 1,5 mrd. kroner frem til 2015.

Forslagsstillerne mener derfor det er behov for en rekke tiltak både på kort og lang sikt for å styrke satsingen på IKT i helsesektoren. Det vises i den sammenheng til Dokument 8:24 S (2011–2012), der en samlet opposisjon foreslår følgende:

«Stortinget ber Regjeringen etablere en statlig finansieringsordning for IKT-satsning i helsetjenesten, der 10 mrd. kroner stilles til rådighet for alle regionale helseforetak i løpet av en periode på fem år. Beløpet skal gis som et rentefritt lån, som er avdragsfritt de første fem årene. Valg av IKT-løsninger skal styres nasjonalt, og det må sikres at systemene fungerer på tvers av helseforetakene og mellom forvaltningsnivåene.»

Forslagsstillerne mener det er hevet over tvil at det kreves en sterkere nasjonal styring for å sikre at hele helsetjenesten blir sikret et IKT-system i alle helseforetakene som gjør at informasjon mellom sykehusene i de ulike helseforetakene kan utveksles raskt og effektivt til det beste for pasienten. Videre mener forslagsstillerne at det er nødvendig å øke investeringene til IKT-systemer i spesialisthelsetjenesten betydelig. Dersom man skal få til det uten at dagens ventelister blir enda lengre, mener forslagsstillerne at det er nødvendig å øremerke midler til IKT-satsingen i en overgangsfase. Det vises i den sammenheng til Innst. 11 S (2011–2012) i forbindelse med statsbudsjettet for 2012 der forslagsstillerne tar til orde for betydelig økte investeringer både i IKT-systemer og medisinsk utstyr.

Nav

NAV har fortsatt systemer som er utviklet på 1970- og 1980-tallet. Både Riksrevisjonens rapport, jf.: «Riksrevisjonens Dokument 1 (2009–2010): Svakheter i etatsstyringen, for dårlig internkontroll og manglende samordning av IKT-systemer», og en ekspertgruppe har slått fast at et nytt datasystem er nødvendig for å kunne gjennomføre etatens oppgaver korrekt og effektivt. Forslagsstillerne er kjent med at regjeringen er i gang med å fornye IKT-verktøyet hos Nav, men det er mye arbeid igjen før IKT-systemene i Nav er i stand til å håndtere den mengden data som det legges opp til. Det vises til at Nav bruker 150 mill. kroner hvert år av sitt budsjett for å drifte disse gamle systemene.

Nav har dessverre som praksis at man bruker personnummer i headingen på brev man sender ut, fordi personnummeret er deres referanse til saker. Dette er ikke bra når andre personer eller etater får tilgang. Romerikes Blad hadde 27. mars 2012 en artikkel om et ektepar som hadde fått et brev fra Nav med opplysninger om en ukjent mann, inkludert mannens navn, adresse, fødselsnummer og detaljerte sykehistorie.

Den norskspråklige avisen Thailands Tidende hadde 1. mars 2012 en sak der Nav hevdet at tradisjonell postgang mellom Norge og Thailand var sikrere enn e-post, og at B-post til Thailand tok opptil en halv måned. Forslagsstillerne mener at Nav bør kunne bruke sikker elektronisk kommunikasjon der dette åpenbart er mest hensiktsmessig. Direktoratet for forvaltning og IKT utarbeidet på bakgrunn av politikken om «digital førstevalg» DiFi-rapport 2011:7 En felles meldingsboks, der man anbefalte Altinn som felles meldingsboks for elektronisk dialog mellom innbyggerne og det offentlige. I rapporten anbefaler også DiFi at kommersielle aktører på sikt kostnadsfritt skal kunne formidle meldinger til og fra det offentlige. Posten Norge har fulgt opp ved å tilby Digipost, og danske E-boks er også på vei inn i det norske markedet. Danmark har på dette området kommet mye lenger enn Norge. E-Boks har eksistert i 10 år, og har avtale med dansk forvaltning om å være tjenestetilbyder av felles meldingsboks for utveksling av meldinger mellom forvaltningen og innbyggerne. 76 av 98 danske kommuner har gjort E-boks til en obligatorisk løsning for alle innbyggerne. 1,3 millioner dansker får sin lønnsslipp på E-boks. Både Digipost og e-Boks tjener penger ved å ta betalt fra dem som sender sikker e-post, basert på volum, mens mottakerne ikke betaler. Dersom Norge skal gjøre det obligatorisk med elektronisk meldingsboks av denne typen, er det svært viktig å sørge for at sikkerheten er god nok og at det er konkurranse mellom flere aktører. Sikker elektronisk meldingsboks kunne ha løst utfordringene knyttet til Navs bruk av B-post til utlandet.

Generell IKT-politikk

Forslagsstillerne påpeker at bruk av elektronisk kommunikasjon mellom privatpersoner og folk flest forutsetter at folk har tillit til at kommunikasjonen ikke blir overvåket av uvedkommende. Derfor har Fremskrittspartiets representanter gått inn for å lovfeste vern av ytringsfrihet og anonymitet på Internett, jf. Dokument 8:55 S (2011–2012). Det er en utfordring for personvernet at stadig mer informasjon om den enkelte blir lagret i offentlige datasystemer.

Forslagsstillerne mener at offentlige IT-prosjekter fra starten må fokusere på PET (Privacy-Enhancing Technologies) og «Privacy by Design». Personvern kan ikke bare være et tilleggsmoment man bygger på toppen av IKT-systemene i etterkant.

Forslagsstillerne påpeker at mange IT-prosjekter i offentlig sektor har vært preget av store overskridelser. Hovedårsaken til at det ofte går galt er at bestillerkompetansen i det offentlige er for dårlig, og det offentlige endrer spesifikasjoner og krav i løpet av prosessen. En annen viktig grunn til dette er at man i altfor stor grad har satset på nyutvikling istedenfor å velge velprøvde løsninger, og at man har for detaljerte krav til løsningene man ønsker seg. Offentlige aktører, som sykehussektoren, setter i gang store prosjekter uten god nok kompetanse, ref. journalsystemene på OUS Ullevål, Rikshospitalet og A-hus der man forsøkte å sy tre systemer sammen til ett, mot sterke advarsler fra IT-bransjen.

Offentlig sektor stiller gjennom sitt avtaleverk Statens standardavtaler (SSA) så rigide krav at mange IKT-aktører kan bli skremt bort fra å gi anbud. Dette medfører at det offentlige i mange tilfeller ikke får den beste leverandøren og heller ikke den beste prisen. Et kroneksempel på dette er følgende punkt i Statens standardavtaler:

«Leverandøren kan ikke holde tilbake ytelser som følge av Kundens mislighold, med mindre misligholdet er vesentlig og Kunden skriftlig har erkjent misligholdet eller misligholdet er fastslått gjennom en av tvisteløsningsmekanismene i kapittel 16.»

Forslagsstillerne viser til at Stortingets transport- og kommunikasjonskomité tidligere har behandlet offentlig IKT-strategi i Innst. S. nr. 158 (2006–2007) til St.meld. nr. 17 (2006–2007) Eit informasjonssamfunn for alle, der det var en tverrpolitisk enighet om at IKT-politikken er viktig for å skape forutsigbarhet vedrørende spørsmål som er avgjørende for vår evne til modernisering av offentlig sektor, innovasjon og nyskaping.

Det er behov for en IKT-havarikommisjon

Offentlige myndigheter samler inn for mye informasjon om innbyggerne, og beskytter denne informasjonen for dårlig. Forslagsstillerne vil på denne bakgrunn ha en IKT-havarikommisjon som kommer

inn og ser på hva som gikk galt når offentlige og kritiske IT-systemer kollapser, der store IT-prosjekt sporer av, eller personvernet har blitt svekket. En slik kommisjon skal ikke først og fremst fordele skyld, men gjøre at offentlig sektor kan lære av feilene man har gjort. Tanken er at det som en slik kommisjon kommer frem til, skal legges inn i søkbar database slik at man kan lære av feilene. Forslagsstillerne mener også at myndighetene må begrense det offentliges stadig mer aktive rolle når det gjelder informasjonsinnhenting om den enkelte borger.

Forslag

Forslagsstillerne vil på denne bakgrunn fremme følgende

f o r s l a g :

Stortinget ber regjeringen opprette en IKT-havarikommisjon, etter mønster fra flyhavarikommisjonen, som skal finne årsaken bak statlige IKT-havarier og IKT-relaterte personvernbrudd. Administrasjonen av dette legges til et eksisterende organ.

29. mars 2012