Teknologirådet

Kongens gate 14
0153 Oslo, Norway
T: +47 23 31 83 00
www.teknologiradet.no

Vår ref.: 18.14
Dato: 12.08.2014

Invitasjon til høring om Norges nasjonale toppdomener og personvern

Tid: onsdag 10. september 2014, kl. 09:00-13:00
Sted: Litteraturhuset, møterom Kverneland, Wergelandsveien 29, 0167 Oslo
Frist: for påmelding/skriftlige innspill: 5. september 2014

Snowden-avsløringene har igjen satt datasikkerhet, internettpolitikk og personvern høyt på den politiske dagsordenen.

Teknologirådet vurderer et konkret forslag fremmet av Håkon Wium Lie på Personverndagen 2014 om å utnytte de nasjonale toppdomenene .sj og .bv til å styrke personvernet for norske internettbrukere. I den forbindelse ønsker vi å invitere dere til å gi innspill til arbeidet i en åpen høring. Høringsrunden vil danne grunnlag for Teknologirådets innspill til Storting og regjering.

Forslag til vurdering

Norge råder over tre såkalte nasjonale toppdomener på internett: .no (Norge), .sj (Svalbard og Jan Mayen) og .bv (Bouvetøya). Av disse er kun .no i bruk.

Forslaget går ut på å ta i bruk de nasjonale toppdomenene .sj og/eller .bv for å etablere "soner" på internett med særskilte krav, regler og vilkår som setter råderett og kontroll over egne data og personvernet til den enkelte bruker i høysetet. Aktører som registrerer nettsteder under disse domenene, vil måtte underskrive en rettslig avtale som eksempelvis forplikter dem til at data skal lagres i Norge og at kommunikasjonen skal skje over krypterte forbindelser.

Et slikt tiltak kan være med på å sikre norske brukeres digitale data i en verden hvor stadig mer av både offentlig og privat kommunikasjon og samhandling skjer over internett. Samtidig gir det norske myndigheter en mulighet til å sende et tydelig signal, og til å markere seg internasjonalt, i den pågående debatten om internettets fremtid.

Mer informasjon om selve forslaget og relevant bakgrunnsmateriale finnes under.

Spørsmål til høringen

Gjennom høringen ønsker vi å belyse særlig følgende tre spørsmål knyttet til forslaget:

1. Vil det være mulig å knytte krav om datasikkerhet og personvern til toppnivå domenenavn, som de norske .sj og .bv? Hvilke fordeler og ulemper vil slike krav kunne gi, og for hvem?

2. Er det nødvendig og ønskelig å ta i bruk .sj/.bv, eller kan en tilsvarende gevinst realiseres i det eksisterende .no-regimet?

3. Hvilke tekniske, juridiske og organisatoriske minimumskrav bør en eventuell ny regulering av landkodetoppdomene oppfylle for å gi norske nettbrukere bedre sikkerhet, styrket personvern og bedre råderett over egne data på internett? Er disse kravene gjennomførbare?

Nærmere om selve høringen

Vi har invitert utvalgte virksomheter til høringen (se liste nedenfor), men høringen er åpen for alle interesserte. Deltakere velger selv hvilke spørsmål de ønsker å belyse og om de ønsker å besvare alle spørsmålene. Alle skriftlige innspill vil bli publisert på våre nettsider.

Samtidig inviterer Teknologirådet til et åpent høringsmøte den 10. september på Litteraturhuset i Oslo. På høringsdagen vil deltakere som ønsker det få anledning til å holde et kort innlegg (prioritet gis deltakere som har levert skriftlige innspill før møtet).

Foreløpig program:

08:30 – 09:00 Kaffe og registrering

09:00 Åpning og velkommen
Tore Tennøe, direktør, Teknologirådet

Åpningsinnlegg: ”Internet Governance and Privacy after Snowden”
Prof. Ian Brown, Oxford Internet Institute (Storbritannia)

Presentasjon av forslag og kort oppsummering av skriftlige innspill
Robindra Prabhu, prosjektleder, Teknologirådet

Innspill fra forslagsstiller
Håkon Wium Lie, CTO, Opera Software og rådsmedlem i Teknologirådet

10:00 – 10:15 Kort pause m/kaffe

10:15 Innspill fra høringsdeltakere

11:45 – 12:15 Enkel lunsj

12:15 – 13:00 Diskusjonsrunde m/ innspill fra salen
Ordstyrer: Tore Tennøe, direktør, Teknologirådet

Oppsummering

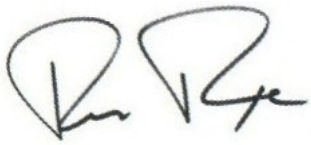
Påmelding og deltakelse

Påmelding innen **5. september** via våre nettsider. Ønsker du å holde et innlegg på møtet, ber vi om at du oppgir hvilke spørsmål du ønsker å belyse. Høringsmøtet er åpent for alle interesserte, men Teknologirådet forbeholder seg retten til å prioritere ved eventuell plassmangel.

Skriftlige innspill sendes til prosjektleder Robindra Prabhu innen samme frist, e-post: robindra.prabhu@teknologiradet.no.

Spørsmål knyttet til høringen kan rettes til prosjektleder Robindra Prabhu på telefon: 23 31 83 16 (kontor)/ 95 05 80 12 (mobil).

Med vennlig hilsen,



Tore Tennøe
Direktør

Robindra Prabhu
Prosjektleder

Inviterte:

Abelia, Datatilsynet, Digitalt personvern, Elektronisk Forpost Norge, Forbrukerrådet, Google Norge, IKT Norge, Håkon Wium Lie (forslagsstiller), Gisle Hannemyr (Institutt for informatikk, UiO), ISOC Norge, Jottacloud, Internet Governance 2 (Institutt for privatrett, Juridisk fakultet, UiO), Kommunal- og moderniseringsdepartementet, Kommunenes Sentralforbund, Microsoft Norge, Personvernnemda, Post- og teletilsynet, Samferdselsdepartementet, Senter for rettsinformatikk (Institutt for privatrett, Juridisk fakultet, UiO), Telenor, Uninett Norid

Bakgrunn

Fremveksten av internett og vår hyppige bruk av internettbaserte tjenester har gjort oss mer sporbare enn noen gang. Våre data flytter seg daglig over landegrensene og ligger ofte spredt i et utall ulike virksomheter i mange forskjellige land. Avtaler som Safe Harbour skal i prinsippet beskytte europeiske persondata i et internasjonalt data-økosystem, men har etter Snowden-avsløringene i 2013 blitt trukket i tvil og mistet nødvendig tillit. Med stadig flere ulike enheter koblet til internett (PC, smarttelefon, TV, nettbrett, osv.), og med stadig mer av våre data lagret i skytjenester, er det blitt vanskeligere for den jevne nettbruker å besvare spørsmål som:

- Hvilke data produserer jeg bevisst og ubevisst på internett?
- Hvor befinner mine data seg?
- Hvem har tilgang til mine data?
- Hva brukes mine data til?

Nasjonal kontroll av internett-infrastruktur

I kjølvannet av Snowden-avsløringene har flere land tatt til orde for en sterkere nasjonal kontroll av infrastruktur knyttet til internett. Et sentralt spørsmål i denne debatten er knyttet hvor våre data skal ligge og hvordan disse kan sikres mot uønsket bruk.

Geografisk plassering av data kan være viktig fordi det bestemmer hvilken jurisdiksjon dataene underlegges. Flere land (som bl.a. Tyskland, Brasil og India) vurderer derfor tiltak som skal sørge for at elektroniske data holdes på servere på nasjonale datasentre. Tidligere i år vurderte Brasil et lovforslag som stilte krav til at internettaktører som er aktive i Brasil må sette opp lokal infrastruktur i landet, slik at data knyttet til brasilianske brukere lagres i Brasil og ikke i utenlandske skytjenester. Etter Snowden-avsløringene rapporterte også den norske skytjenesten Jottacloud en markant vekst fra kunder som ønsket en lagringstjeneste med *norske* personverngarantier. Nylig ble dessuten den krypterte eposttjenesten protonmail.ch lansert med *sveitsiske* personverngarantier.

Hva kan og bør Norge gjøre?

Etter Snowden-avsløringene er det også betimelig å vurdere hva norske myndigheter kan gjøre for å sikre (norske) brukere sterkere personverngarantier på internett i fremtiden. En interessant mulighet i denne sammenheng er å ta i bruk de hittil ubrukte nasjonale toppdomenene .sj og .bv og gi disse en ny og særegen sikkerhetsprofil med et brukerorientert fokus. (Norge har dessuten svært gode forhold for store datasentre gjennom sin tilgang til billig og grønn energi, kaldt vann til avkjøling og dessuten store, kjølige fjellhaller.)

I første rekke vil dette kunne gi norske brukere en styrket sikkerhet på internett, for eksempel i kommunikasjonen med det offentlige. Skytjenester knyttet til domene vil kunne gi norske kommuner en garanti om at viktige personopplysninger lagres i Norge med særskilte krav til sikkerhet og tilgang.

På sikt er det også mulig at disse domenene kan utvikles til internasjonale merkevarenavn, som garantister for høy datasikkerhet, personvern og brukerkontroll over egne data. Således vil Norge kunne markere seg i den internasjonale debatten om internettets fremtid og sende et viktig signal til verden om hvilke prinsipper som bør være gjeldende for den videre utviklingen av internett.

Samtidig er det mulig at en slik bruk av nasjonale ressurser vil være med på å bidra til en uheldig "balkanisering" av internett, og at dette på sikt vil svekke internettet som en driver for innovasjon og økonomisk vekst.

Hva er domenenavn og hvorfor er de viktige?

På samme måte som telefonnummer identifisere et telefonapparat i telefonsystemet og gjør det mulig for to telefoner å kommunisere med hverandre, kan ulike enheter på internett identifisere og kommunisere med hverandre via såkalte IP-adresser.

Domenenavn er kjennetegn for slike IP-adresser og er bygget opp hierarkisk: i adressen www.teknologiradet.no, er ".teknologirådet" et såkalt hoveddomene og ".no" et landkodetoppdomene.

Til forskjell fra de fleste andre land, har Norge har foruten ".no" fått utdelt to ytterligere landkodetoppdomener:

.sj for Svalbard-Jan Mayen
.bv for Bouvetøya.

Per i dag er det kun ".no" som er i bruk. Landkodene ".sj" og ".bv" er således nasjonale internettressurser som ikke blir utnyttet i dag. Alle tre domene forvaltes av NORID, som også definerer reglene for registrering av domener under toppdomenet ".no".

Domenet ".no" er i utgangspunktet kun tilgjengelig for organisasjoner og firma som er registrert i Enhetsregisteret i Brønnøysund. Sammenlignet med andre land, har tildelingsprosessen av domener har i Norge vært underlagt forholdsvis streng kontroll. Dette har gitt en ryddig tildeling, og ".no"-domenet er i dag mindre plaget av såkalt "domain squatting"[1].

En registrering under ".no" garanterer imidlertid ikke for at dataene ligger i Norge og derfor underlagt norsk jurisdiksjon. Det finnes heller ikke garantier for at de som registrerer et domene under ".no", også er de som faktisk bruker det. Eksempelvis videresendes brukere fra den norsk-registrerte dating-tjenesten "match.no" automatisk til amerikanske "match.com" som råder over brukerdataene.

Forslag: Ett nytt sikkerhetsregime for norske nettbrukere gjennom toppdomenene .sj og .bv

Forslaget går ut på å åpne *.sj* og/eller *.bv* for bruk, og samtidig knytte disse domene opp til nye og strenge regler for domeneregistrering. Slik kan norske myndigheter bidra til å

[1] "Domain squatting" eller "cybersquatting" viser til fenomenet hvor aktørere registrerer eller omsetter et domenenavn med tydelig tilknytting til et varemerke som tilhører en annen, for så å tilby domenet til eieren av varemerket til en oppblåst pris.

etablere ”soner” på internett med et tydelig personvernfokus og om som er underlagt helt spesielle sikkerhetskrav. Disse kravene kan bl.a. være av typen:

- Alle data knyttet til nettstedet skal være underlagt norsk jurisdiksjon. Dataene skal derfor ligge på servere i Norge.
- Viktige persondata skal alltid krypteres.
- Det skal ikke være mulig å spore brukere over lengre perioder. Bruker tjenesten såkalte ”cookies”, skal disse slettes etter en fastlagt periode (for eksempel ett år).
- Domenet definerer og dikterer bruksreglene for tjenester. Ønsker en leverandør å opprette en ny internettjeneste under domenet, skal ikke brukeren behøve å akseptere et sett med betingelser – det er tjenesteleverandøren som aksepterer bruksreglene for domenet.
- Brukeren skal ha enkelt tilgang til sine persondata og ha anledning til å slette disse om ønskelig.

Særlig vil tydelig krav til lagring under norsk jurisdiksjon, standardiserte måter for brukeren å slette informasjon, samt eksplisitte krypteringskrav til data og datakommunikasjon kunne være med på å gi disse domenene et betydelig sikkerhetsløft i forhold til andre domener på internett.

Historikk

Forslaget ble først presentert av Håkon Wium Lie d. 28. januar 2014 på arrangementet ”Personverndagen 2014” i regi av Datatilsynet og Teknologirådet. Teknologirådet besluttet 13. juni 2014 å vurdere forslaget gjennom en åpen høring. Håkon Wium Lie presenterte ideen i en kronikk i Dagbladet 24.06.14.