Justitsministeriet
Sikkerhedskontor II

Dato 25. oktober, 2021

Høringssvar vedrørende:

Høring over udkast til forslag til lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester (Revision af reglerne om registrering og opbevaring af oplysninger om teletrafik (log-ning) m.v.) dateret 27. september, 2021.

På vegne af Citizen First (under etablering som en non-profit NGO med fokus på digital repræsentation af borgerne) har Priway følgende kommentarer:

1. Udgangspunktet er dårlige infrastruktur standarder i telesektoren (f.eks. 5G, NemID/MitID og EMV betalinger), som hverken sikrer borgerne eller systemerne ligesom cyberkriminelle har lette vilkår til at tracke ofre, målrette angreb og lave f.eks. identitetstyveri.

Det har ført til en situation, hvor den kommercielle infrastruktur a priori udfører invasiv overvågning som så udnyttes både kommercielt, kriminelt og af staten medmindre andre strukturer eksplicit sikrer mod dette.

Hvorvidt staten OGSÅ pålægger overvågning og hvorledes offentlige myndigheder tilgår sådanne sensitive person- og systemdata ændrer i princippet ikke på den grundlæggende problemstilling - man lovgiver om en forværring af en allerede dårlig sikkerhedsstruktur.

Hele lovforslaget forfalder derfor reelt til en ”pest eller kolera” diskussion af proportionaliteten mellem mere overvågning og den kriminalitets-bekæmpende hensigt.

Vi er sikre på at andre vil bruge kræfter på at diskutere om de konkrete aspekter og vælger ikke at tage yderligere stilling hertil, idet vi betragter den diskussion som ufrugtbar.

2. Vi konstaterer dog at lovforslaget reelt forsøger at gøre sikkerhed umuligt ved at PÅLÆGGE teleinfrastrukturen at strippe og blokere alle sikkerhedsmekanismer på vegne af borgeren og organisationer med henblik på at tilsikre en invasiv overvågning.

Det betyder at ingen borgere kan gå sikkert på nettet inkl. f.eks. Forsvarets personale, Rigspolitiet, politikere, forsvarsadvokater, journalister, forskere.

Her overser man en væsentlig pointe – hvor man aldrig vil kunne overtale kriminelle til selv at inkriminere sig, så har den almindelige borgere og legale personer en stærk egeninteresse i bedre sikkerhed, som man reelt blokerer og dermed forværrer.

Vores forslag er derfor at man i loven indbygger eksplicit understøttelse af FRIVILLIGT SELV-INKRIMINERENDE SIKKERHEDSSTRUKTURER SOM IKKE KAN OVERVÅGES, dvs. en godkendelsesmodel til at undgå logning, fordi de hensyn overfor en dommer som varetages af logningsbekendtgørelsen er tilgodeset på anden vis.

Hvad indebærer det? F.eks. at en militærperson kan gå på nettet og bevise overfor infrastrukturen at sessionen er legitim og sikkerhedsmæssigt valideret i forhold til formålet uden at hverken device eller borgeren kan identificeres i nettet.

Konkret kan det f.eks. ske ved at borgeren har et chipkort tilknyttet MitID som kan genere en ny ikke-linkbar kvalificeret digital signatur inkl. de nødvendige mekanismer til at bevise at sessionen er afledt af en godkendt struktur.

I tilknytning hertil at vedkommende kan stilles til ansvar og/eller overvåges i forhold til det formål, som sessionen vedrører.

På den måde kan en borger f.eks. bidrage til en reelt anonym sundhedsforskning i en sammenhæng og stå til ansvar og med en dommerhandling overvåges på de sociale net, hvis de konkrete betingelser er til stede.

Hvordan det konkret verificeres og specifikke krav hertil kan overlades til en certificerings/godkendelsesproces, mens selve loven kan være teknologi-neutral med fokus på de reelle behov.

På den måde opnås 3 kritiske forhold på samme tid:

a) En borger kan gå sikkert på nettet og gennemføre digitale transaktioner sikkert, hvorved både borgeren selv og alle involverede serviceleverandører sikres helt eller delvist mod cyberangreb – hvilket ikke er muligt i dag og ulovligt med det aktuelle forslag.

b) Det virker kriminalitetsforebyggende, fordi en stigende andel af samfundsprocesser vil forebygge kriminalitet og ansvar vil være nemmere at etablere.

c) Det betyder at de kriminelle får stadigt sværere ved at gemme sig, fordi det bliver nemmere og mere acceptabelt at fokusere på restgruppen. Hvis lovlydige borgere kan beskytte sig mod overvågning fjerner man et af hovedargumenterne mod logning som sådan.

Med henvisning til GDPR er teknologiens aktuelle stade sådan at sådanne strukturer snart bliver almindelige og dermed lovpligtige indenfor EU. Det bliver en hovedopgave for Citizen First at stille sådanne strukturer til rådighed for alle borgere på non-profit basis som en del af opgraderingen af cybersecurity.

På vegne af Citizen First

Stephan Engberg
Priway ApS