Datatilsynet

KOMMUNAL- OG
MODERNISERINGSDEPARTEMENTET
Postboks 8112 DEP
0032 OSLO

Deres referanse	Vår referanse	Dato
20/3645-1	20/03968-2	18.01.2020

Høringsuttalelse - Endringer i ekomloven (lagring av IP-adresser mv)

Vi viser til høringsbrev 09.10.20 – Endringer i ekomloven, (lagring av IP-adresser mv.) med høringsfrist 11.01.21. Datatilsynet har etter forespørsel fått en ukes forlengelse av høringsfristen.

I høringsnotatet foreslår Kommunal- og moderniseringsdepartementet og Justis- og beredskapsdepartementet (departementene) at det skal innføres en plikt for tilbydere av ekomtjenester til å lagre IP-adresser, slik at politiet kan få tilgang til IP-adressene for å forebygge og etterforske kriminelle handlinger.

I høringsnotatet er det fokusert på de tilfellene der hvor politiet ønsker opplysninger om en ip-adresse, men personvernkonsekvensene for den delen av forslaget som omhandler adgangen til å innhente alle ip-adressene en person har benyttet i et gitt tidsrom er i liten grad omtalt.

En ip-adresse kan ikke sammenliknes med abonnementsopplysninger til en fasttelefon. Bruken av ip-adresse har vokst i takt med digitaliseringen av samfunnet. Vi omgir oss med utstyr – pc, smartklokker, mobiler, biler etc. som tildeles forskjellige ip-adresser basert på hvilket nettverk og hvordan en er koplet til internett. Tildelt ip-adresse, navn og tidspunkt kan derfor også gi opplysninger om bevegelser når de settes i sammenheng over et gitt tidsrom.

I og med forslaget legger opp til at Politiet vil bli gitt mulighet til å innhente informasjon i forebyggingsøyemed uten domstolskontroll, så åpnes det for å lagre og få tilgang til opplysninger om ip-adresser som sier noe om bevegelser for store deler av den norske befolkning uten at de engang er mistenkt for en kriminell handling. Dette er en type skjult overvåking som hittil har vært underlagt streng kontroll, men som det nå åpnes for å gi tilnærmet fri tilgang til.

Datatilsynet er klar over de tungtveiende hensynene til å bekjempe nettovergrep, men finner at forslaget i liten grad er begrenset til denne type kriminalitet.

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 458 Sentrum 0105 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

Datatilsynet registrerer at det i høringsnotatet beregnes at det vil bli sendt 110 000 anmodninger. Når politiet etter tall fra SSB i 2019 etterforsket ferdig 288 124 saker, så innebærer det at store mengder personopplysninger vil bli innhentet uten forhåndskontroll i en betydelig del av politiets virksomhet.

Forslaget er formulert som en plikt overfor tilbydere, men vi ser at konsekvensen er innskrenkning i borgernes rett til kommunikasjon uten innblanding fra myndigheter, noe som må utredes nærmere.

Forslaget innebærer at nesten alle norske borgere vil bli registrert når de benytter internett og at deres bevegelser basert på ip-adresse tilknyttet mobiltelefon, tingenes internett som bil, klokker og helsedingser, nettverk på hjem, skole, bibliotek, arbeidsplass og andre steder vil lagres.

Dette medfører at alle norske borgere med mobiltelefon eller annet nettilkoblet utstyr vil kunne følges, siden mobiler og liknende utstyr stadig kommuniserer via mobildata og Wifi og dermed ber om IP-adresse flere ganger i timen. Veldig mange apper er satt opp for å kobles til internett med jevne mellomrom i løpet av timen og døgnet. Kommunikasjonen går nå via mobildata og wifi og ikke i like stor grad som før via tale og SMS.

Det innebærer at kommunikasjonsvernet blir svekket - noe som har konsekvenser for ytringsfrihet, retten til fritt søke informasjon, kildevernet og bevegelsesfriheten. Dette kan igjen medføre en nedkjølingseffekt og en svekkelse av det det demokratiske fundament i Norge.

Dette er et uforholdsmessig inngrep i norske personvern som ikke kan begrunnes i de tungtveiende kriminalitetsbekjempende hensyn som foreligger, uten at tilgangen begrenses og at det rammes inn av de rammene som allerede foreligger i straffeprosessloven når det gjelder domstolskontroll.

Slik forslaget er formulert så tilfredsstiller det ikke kravene som oppstilles i de nylige avsagte EU-dommene *Digital Rights/Quadrature* om krav til uavhengig forhåndskontroll som må foreligge ved innhenting av ip-adresser knyttet til navn og tidspunkt.

Når det gjelder utlevering av ip-opplysninger med utgangspunkt i et navn vil Datatilsynet understreke at dette vil kunne innebære en kartlegging av en persons bevegelser ved at tilbyder bes om å opplyse hvilke ip-adresser personen har benyttet i f.eks. i en måned. Forslaget inneholder ingen begrensninger av omfang eller konkretisering av nødvendighet. Innhentingen vil foregå i det skjulte da det ikke foreligger forhåndskontroll eller underretning til den registrerte. Når forslaget også åpner for å innhente til forebygging, så vil det kunne innebære en kontinuerlig skjult overvåking av personer som ikke engang er mistenkt for å ha begått en kriminell handling.

En slik skjult overvåkning vil være i strid med Grl. § 102 og EMK art. 8 som oppstiller strenge vilkår for når skjult overvåking kan tillates. De såkalte Weber-kriteriene stiller blant annet krav til uavhengig forhåndskontroll for å iverksette skjult overvåking.

Inngrepet i personvernet skjer i det dataene lagres og Datatilsynet er bekymret for både en formålsutglidning når det gjelder myndighetenes tilgang til dataene og den stadig større utbredelsen av tingenes internett som gjør at vi blir omgitt av et stadig mer finmasket nett av elektronisk kommunikasjon som kan brukes til å kartlegge enkeltindividet.

Datatilsynet er helt imot at eventuelle opplysninger skal gjøres tilgjengelig i sivile saker. Dette illustrerer hvorfor lagring av opplysninger til et formål alltid innebærer en risiko for formålsutglidning. I høringsnotatet argumenteres det med tungtveiende kriminalitetsbekjempende hensyn som ikke kan begrunne hvorfor det er nødvendig med en så omfattende overvåking i åndsverkssaker.

Forslaget må sees i sammenheng med det samlede overvåkingstrykket i samfunnet. Når det i forslaget nevnes at utlevering av brukerinformasjon fra nettsteder og nettjenester (for eksempel sosiale medier) kan danne grunnlag for en etterforskning og at PST kan benytte tilgangen til å etterforske radikalisering på nett, så vil dette ha konsekvenser for borgernes tillit til å kunne uttrykke seg lovlig og fritt på internett uten å bli overvåket av myndighetene.

I Datatilsynets personvernundersøkelse 2019/2020 svarer 16% at de har unnlatt å delta i en debatt i kommentarfelt eller på Facebook fordi de er usikre på om myndigheter slik som politiet, PST eller etterretningstjenesten, kan få tilgang til informasjonen. Dette er et oppsiktsvekkende høyt tall i et land hvor tilliten til offentlige myndigheter generelt sett er høy.

Forslaget må også sees i sammenheng med den mulige gjennomføringen av tilrettelagt innhenting etter ny lov om etterretningstjenesten. Hvis tiltaket gjennomføres så vil store deler av norske borgeres internettkommunikasjon være tilgjengelig for myndighetene. I ny lov etterretningstjenesten er det åpnet for mekanismer for å dele overskuddsinformasjon med blant annet politiet.

Dette viser hvor viktig det er å vurdere de enkelte forslagene om myndighetenes tilgang til borgernes privatliv i sammenheng for å unngå at overvåkingssamfunnet stadig innskrenker individets frihet.

Regjeringen har nedsatt en personvernkommisjon for å vurdere personvernets stilling i Norge, som blant annet skal se på personvern i justissektoren. Det er uheldig at både dette forslaget og forslaget om tilrettelagt innhenting gjennomføres før kommisjonen har utredet og vurdert mulige konsekvenser for demokratiet og samfunnet ved at et så inngripende tiltak blir innført.

Datatilsynets konklusjon

Datatilsynets konklusjon er at det ikke bør innføres en plikt til å lagre ip-adresser, og at hvis det gjennomføres så må tilgangen begrenses til de sakene hvor det har størst betydning, som nettovergrep og deling av overgrepsbilder, samt at reglene om bevisinnhenting i straffeprosessloven følges og det må foretas en uavhengig forhåndskontroll av om vilkårene for innhenting er oppfylt.

Datatilsynet mener derfor at forslaget ikke kan vedtas i sin nåværende form og må endres. Uansett må personvernkonsekvensene av alle sider av forslaget utredes nærmere.

Forslaget innebærer også at alle tilbyderne må etablere en ny database for politiets bruk over tildelte ip-adresser som er en behandling som er omfattet av personvernforordningen. Denne behandlingen vil være underlagt personopplysningsloven og personvernforordningen. En slik database vil kreve et høyt kvalitetsnivå og forslaget innebærer en plikt for over 300 tilbydere til å opprette og samordne denne type database. Dette vil være en ny behandling av personopplysninger siden den skal tilrettelegges for et nytt formål. Det er ikke tidligere vært en plikt til å lagre denne typen opplysninger. En slik database vil også måtte omfattes av en tilstrekkelig beskyttelse slik personvernforordningen krever. En slik beskyttelse vil både omfatte lagringen og utlevering til både politi og den registrerte.

Den registrerte har etter personvernforordningen en rekke rettigheter som retten til innsyn, sletting, korrigering, dataminimering etc. Høringsnotatet drøfter ikke hvordan forholdet mellom de registrertes rettigheter og plikten til å lagre skal løses, noe som kan skape store praktiske og rettslige utfordringer for tilbyderne.

Forslaget drøfter i liten grad forholdsmessigheten og nødvendigheten av at nesten alle norske borgere skal registreres. De aller fleste vil aldri være mistenkt i en straffesak og for noen grupper, som barn, så vil registreringen i svært liten grad kunne begrunnes i kriminalitetsbekjempende hensyn.

Vi lever i en tid hvor den individuelle frihet er under press og hvor det stadig innføres nye overvåkningstiltak både i privat og offentlig sektor. Hvordan dette forandrer samfunnet og individets mulighet til danne selvstendige tanker som uttrykkes fritt og leve et liv som ikke begrenses av sporing er for tidlig å konkludere noe sikkert om. Men det er god grunn til advare om at når friheten innskrenkes, så blir den borte og det demokratiske fundament i samfunnet forvitres.

Konsekvenser for personvernet

I en rettsstat må det finnes klare grenser for hvilke tiltak staten kan iverksette med tanke på å forebygge og etterforske straffbare forhold.

Dagens rettstilstand gjenspeiler dette. Det kan ikke iverksettes etterforskning, med mindre det som følge av anmeldelse eller andre omstendigheter er rimelig grunn til å undersøke om det foreligger straffbart forhold som forfølges av det offentlige, jf strpl § 224.

Dersom tiltaket retter seg mot en konkret person kreves det i tillegg at det foreligger er en kvalifisert mistanke mot vedkommende. Vilkårene er enda strengere når formålet med tiltaket er å avverge straffbare handlinger. Det kan ikke iverksettes målrettede tiltak for å forebygge straffbare handlinger, med mindre det er rimelig grunn til å tro at noen kommer til å begå bestemt angitte lovbrudd.

I høringsnotatet er det åpnet for at opplysninger kan innhentes for å forebygge kriminelle handlinger uten noe nærmere beskrivelse av hvordan man tenker at dette skal foregå. Hva som ligger i begrepet forebygging er vanskelig å definere og det egner seg derfor lite som et vilkår for å iverksette overvåking. Vil det innebære at en person som er tilknyttet et radikalt miljø vil kunne få sine ip-opplysninger få innhentet for å se om han for eksempel deltar på faste møter i en bestemt moske ved at han beveger seg fra hjemmet og er tilknyttet moskeens nettverk som benyttes til leksehjelp hver fredag? Eller når det er andre møter på samme sted? Datatilsynet vet ikke, men når terskelen senkes så lavt som forebygging, så må det konkret utredes og beskrives i høringsnotatet.

Datatilsynet mener lagringen av ip-adresser kan ses som en forskuttert etterforskningsmetode, som skal kunne tas i bruk før gjeldende vilkår for å ta i bruk ordinære metoder er oppfylt.

Selvbestemmelsesrett

Den enkeltes selvbestemmelsesrett er et helt grunnleggende personvernprinsipp; enhver skal i utgangspunktet ha rett til å bestemme over sine egne personopplysninger, med tanke på hvem som behandler dem, til hvilke formål de benyttes osv. Dette utgangspunktet gjelder uavhengig av om opplysningene er sensitive eller ikke.

I dag behandler tilbyderne disse opplysningene med hjemmel i en privatrettslig avtale som er frivillig inngått mellom dem og deres kunder. I henhold til forslaget skal opplysningene i stedet lagres med hjemmel i et lovpålegg overfor tilbyderne. Dette betyr at individet gjennom forslaget fratas den råderetten hen i dag har over disse opplysningene. Det representerer et klart brudd på den enkeltes personvern.

Datatilsynet vil i den forbindelse bemerke at det å avstå fra å bruke elektroniske kommunikasjonsformer, for å bevare kontrollen over egne opplysninger, ikke er et praktisk alternativ i dagens samfunn. Vi er avhengig av pc og mobil for å få gjort daglige gjøremål, jobb og skole.

Det er klart at hensynet til personvernet må avveies mot andre tungtveiende hensyn, som kriminalitetsbekjempelse, men da må inngrepet rammes inn av tilstrekkelige kontrollmekanismer.

Rett til frihet fra statlige myndigheter

Datatilsynet vil minne om at et demokrati kjennetegnes ved at det er borgerne som kontrollerer staten, og ikke motsatt. Det er derfor helt nødvendig å sikre maktbalansen mellom borgerne og staten.

I den forbindelse er et sentralt poeng at innsamling og lagring i henhold til forslaget skjer i statlig regi, gjennom et absolutt lovpålegg. Staten gis gjennom lagringen et maktmiddel, som bidrar til å forrykke balansen mellom stat og individ, og medfører derfor et klart brudd på personvernet. Ved endrede samfunnsforhold vil en slik

forskyvning kunne få dramatiske konsekvenser noe som blant annet ble drøftet av Lysne-utvalget i utredningen om digitalt grenseforsvar.

Rett til anonym ferdsel

Den enkeltes rett til å bevege seg fritt i samfunnet, uten plikt til å legitimere seg eller la seg identifisere, er en sentral del av den enkeltes autonomi og en viktig del av et demokratisk samfunn. Det å kunne delta i politikk, foreningsliv, møter og foredrag uten å være bekymret for om en spores er en forutsetning for et aktivt samfunnsliv.

Forslaget vil gjøre det mulig å tegne et bilde av hvor den enkelte befinner seg rent fysisk, nærmest til enhver tid. Slik sett vil forslaget utfordre retten til anonym ferdsel.

Forbud mot overskuddsinformasjon

Forbud mot bruk av overskuddsinformasjon er en sentral del av personopplysningsregelverket Det er altså forbudt å behandle andre eller flere personopplysninger enn det som er nødvendig for å nå formålet med behandlingen.

Selv om det er umulig å tallfeste nytten av lagringen, så er det liten tvil om at det aller meste av det som skal lagres vil være å anse som overskuddsinformasjon. For det første vil personkretsen som omfattes av lagringen være klart større enn den personkretsen som faktisk gjennomfører slike lovbrudd som det her er tale om.

Videre vil det lagres opplysninger som etter sin art og innhold ikke kan knyttes til pågående eller fremtidig kriminalitet.

Forslaget setter innsamling av overskuddsinformasjon i system, og innebærer derfor et klart brudd på personvernet.

Om forslaget til lagring av ip-adresser – hva foreslås lagret?

Forslagets § 2-8 a pålegger tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste skal lagre de opplysninger som er nødvendige for å identifisere abonnenten med utgangspunkt i

a) offentlig IP-adresse og et tidspunkt for kommunikasjon eller

b) offentlig IP-adresse, et tidspunkt for kommunikasjon og portnummer benyttet ved kommunikasjonen, dersom samme offentlige IP-adresse er tildelt flere abonnenter samtidig.

Om ip-adresser

En ip-adresse, tidspunkt for kommunikasjon og navn på abonnement slik forslaget ønsker lagret sier for det første noe om når en person har kommunisert på internett, men også noe om hvor personen befinner seg.

Det er viktig å understreke at en ip-adresse ikke kan sammenliknes med abbonementopplysninger om en gammeldags fastelefon. Ip-adresser tildeles hver gang en enhet som pc, laptop, mobil, smartklokke, bil etc. koples opp på internett og vil forandres basert på hvilket nettverk man er koplet til.

Det vil si at for en vanlig bruker av mobil og pc i Norge, så vil en om morgenen ha en ip-adresse knyttet til hjemmenettverket for både mobil og pc. Når en beveger seg så vil mobilen få tildelt ip-adresser vi basestasjoner, så kopler en seg kanskje på Vys nett på toget, så jobb eller skole, bibliotek, kafe eller treningssenter, hjem til en venn eller en kjæreste hvor en blir natten over for så ta flytoget til Gardermoen hvor en etterhvert kopler seg opp på hotellet i Ålesund etc. Dette er noe enhver kan forsøke om sine egne bevegelser på internett ved hjelp av gratistjenester, og det må forventes at politiet har minst like gode verktøy uten at det opplyses i høringsnotatet.

Det er spesielt relevant der hvor forslaget åpner for å innhente ip-opplysninger med utgangspunkt i en konkret person i et gitt tidsrom. I pkt. 7.5.2 opplyses det «Innhenting med utgangspunkt i en konkret abonnent vil videre bidra til å begrense mengden av opplysninger som innhentes.» Datatilsynet er ikke enig i dette, da denne innhentingen vil være mer inngripende overfor den det retter seg mot.

Dette er en alvorlig mangel ved forslaget som må utredes nærmere. Forslaget inneholder ingen begrensninger av omfang eller konkretisering av nødvendighet, og når forslaget åpner for å innhente til forebygging, så vil det kunne innebære en kontinuerlig skjult overvåking av personer som ikke engang er mistenkt for å ha begått en kriminell handling.

Det er ikke redegjort for i forslaget om politiet besitter opplysninger som kan kople ip-adressen til den enkelte basestasjon til et gitt tidspunkt, noe som kan medføre en ytterligere kartlegging av bevegelser eller på hvilke vilkår politiet kan anmode tilbyder om denne informasjonen.

Når det gjelder utlevering av ip-adresser der samme offentlige ip-adresse deles av flere brukere samtidig vil også kunne innebære at presisjonsnivået vil kunne bli lavt og medføre en risiko for vilkårlig utpeking av mistenkte være tilstede.

En annen utfordring er at forslaget retter seg mot 300 tilbydere, og i noen tilfeller vil det også være MVNO'er (Mobile Virtual Network Operator) involvert. Disse sitter på informasjonen om abonnenten og ikke IP-adressen. Prosessen med å få korrekte opplysninger tilknyttet hver enkelt ip-adresse vil derfor kunne involvere flere aktører.

Etter Datatilsynets mening så vil det være større personvernbekymringer knyttet innføringen av IPv6 da det muliggjør en fast ip-adresse som kan følge bruker på flere enheter og som dermed gjør sporing enklere. De personvernmessige forhold rundt Ipv6 er ikke behandlet i høringsdokumentet og dette er å anse som en mangel.

Om forslaget til lagring av ip-adresser – hva kan hentes ut og på hvilke vilkår?

I forslaget åpnes det for at politiet eller PST kan innhente nødvendige opplysninger om ip-adresse, abonnement og tidspunkt for tilkopling for å forebygge eller etterforske en handling hvor strafferammekravet settes til minimum ett eller to års fengsel, eventuelt i kombinasjon med unntak for spesifikke straffebud der IP-informasjon er av særlig stor betydning.

I tillegg til det foreslås det at politiet kan innhente opplysninger om ip-adresser knyttet til en enkelt person i et gitt tidsrom.

Innhentingen er ikke underlagt domstolskontroll eller annen type forhåndsgodkjenning, men det legges til grunn i høringsnotatet at politiregisterloven og Datatilsynets tilsynsmyndighet vil innebære tilstrekkelig kontroll og oppfylle de krav som følger av de siste EU-dommene *Digital Rights/Quadrature* og EMK-praksis.

Om vilkårene for innhenting og kravet til forhåndskontroll i EU og EMK-praksis

EU-domstolen har nylig avsagt prinsipielle dommer som forbyr generell og udifferensiert innsamling av teledata. I dommene så omtales også innsamling og utlevering av opplysninger knyttet til ip-adresser til politimyndigheter.

I forslag til § 2-8 a foreslås det en plikt til å lagre:

> «opplysninger som er nødvendige for å identifisere abonnenten med utgangspunkt i
>
> a) offentlig IP-adresse og et tidspunkt for kommunikasjon eller
>
> b) offentlig IP-adresse, et tidspunkt for kommunikasjon og portnummer benyttet ved kommunikasjonen, dersom samme offentlige IP-adresse er tildelt flere abonnenter samtidig.»

Datatilsynet er av den oppfatning av at dette er i strid med kommunikasjonsvernet og de siste EU-dommene, spesielt i *La Quadrature du Net* (sak C-511/18 og sak C-512/18).

Et sentralt punkt er at der hvor en ip-adresse knyttes til både et navn og et tidspunkt, så vil det inneholde opplysninger som knytte en person både til nettaktivitet, men også hvor en person befinner seg.

Utfordringen er at siden ip-adresser knyttet til en person basert på hvilket nettverk personen er tilknyttet, så vil tidspunktet for kommunikasjonen være avgjørende for å få rett identifikasjon. EU-domstolen krever da forhåndskontroll for utlevering i motsetning til der hvor bare navn og ip-adresse registreres.

Domstolens utgangspunkt i 153 er at

> «Eftersom IP-adresser kan anvendes til bl.a. at foretage en udtømmende sporing af en internetbrugers søgemønstre og dermed af den pågældendes onlineaktiviteter, gør disse oplysninger det imidlertid muligt at skabe en detaljeret profil af denne internetbruger. (…) udgør således alvorlige indgreb i internetbrugerens grundlæggende rettigheder.

Men at dette kan nyanseres. I dommen så skilles det mellom i 154

> «…skal der tages hensyn til den omstændighed, at IP-adressen i det tilfælde, hvor en lovovertrædelse er begået online, kan udgøre det eneste efterforskningsmiddel, der kan gøre det muligt at identificere den person, som denne adresse var tildelt på det tidspunkt, hvor den pågældende overtrædelse blev begået.»

Og i 157

> «Hvad endelig angår de data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, gør disse data det ikke i sig selv muligt at få kendskab til datoen og tidspunktet for samt varigheden og modtagerne af den kommunikation, der er foretaget, og heller ikke de steder, hvorfra denne kommunikation har fundet sted, eller oplysning om, hvor ofte denne kommunikation har været foretaget med visse personer i en bestemt periode, hvilket indebærer, at disse data bortset fra de pågældendes kontaktoplysninger, såsom deres adresser, ikke tilvejebringer nogen form for oplysninger om den foretagne kommunikation og dermed om disse personers privatliv. Det indgreb, som en lagring af disse data indebærer, kan således principielt ikke kvalificeres som alvorligt (jf. i denne retning dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 59 og 60).»

Det går et tydelig skille mellom der hvor ip-adressen er knyttet til et navn og tidspunkt, og der hvor ip-adressen kun knyttes til et navn og ikke sier noe om når kommunikasjonen har foregått.

I avsnitt 168 omtales spesielt det tilfelle der hvor det skal lagres ip-adresser knyttet til en person i et gitt tidsrom. Uttalelsen fastslår at dette kun kan gjøres i en tidsperiode som er begrenset til det som er strengt nødvendig, og noe som er i strid forslagets løsning om å foreta en generell og udifferensiert innsamling av alle ip-adresser i forkant, for så å be om adressene som er knyttet til en person i etterkant av innsamlingen.

Der hvor ip-adressen er knyttet til både et navn og tidspunkt, så vil alle de rettsikkerhetsmekanismer som er knyttet til praksis fra EU-domstolen måtte gjøres gjeldende. Det vises til Tele2/Watson-dommen, hvor det stilles krav i premiss 119 at det må fastlegges objektive kriterier for når myndighetene kan få adgang til opplysningene og tilgang prinsipielt kun kan gis der hvor en person er mistenkt for å planlegge, ville begå eller har begått en alvorlig kriminell handling.

> «For så vidt som en generel adgang til samtlige lagrede data – uafhængigt af, om der foreligger nogen forbindelse, selv indirekte, til det forfulgte mål – ikke kan anses for at være begrænset til det strengt nødvendige, skal den pågældende nationale lovgivning således være baseret på objektive kriterier med henblik på fastlæggelsen af de omstændigheder og

> betingelser, hvorunder de kompetente nationale myndigheder skal gives adgang til abonnenters eller registrerede brugeres data. I denne henseende kan der i forbindelse med målet om bekæmpelse af kriminalitet i princippet kun gives adgang til data vedrørende personer, der er mistænkt for at planlægge, ville begå eller have begået en alvorlig lovovertrædelse eller på en eller anden måde være involveret i en sådan lovovertrædelse.»

Dette innebærer at forslagets krav om «nødvendighet» i liten grad gir tilstrekkelig veiledning for hva som skal utleveres og at «forebygging» blir et for vidt begrep for når det er legitimt å innhente opplysningene.

I tillegg krever domstolen i 120 en uavhengig forhåndskontroll av om vilkårene er oppfylt.

> «Med henblik på i praksis at sikre fuld iagttagelse af disse betingelser er det afgørende, at de kompetente nationale myndigheders adgang til de lagrede data i princippet, undtagen i behørigt begrundede hastende tilfælde, er undergivet en forudgående kontrol, der foretages af enten en domstol eller en uafhængig administrativ enhed, og at denne domstols eller denne enheds afgørelse træffes på grundlag af en begrundet anmodning, som navnlig fremsættes af disse myndigheder inden for rammerne af procedurer med henblik på forebyggelse, afsløring eller strafferetlig forfølgning»

Det legges også til grunn i 121 at for at registrerte som har fått utlevert sine opplysninger fra tilbyder til politiet skal kunne ivareta sine rettigheter etter personvernforordningen og politiregisterloven, så langt som mulig skal underrettes. Dette vil være spesielt relevant der flere brukere deler en felles ip-adresse, som for eksempel en skole hvor en stor del av utleveringen ikke vil ha relevans for etterforskningen.

EMK

Når det gjelder kravene som EMK stiller til lagring og utlevering av ip-adresser så drøfter ikke høringsnotatet det faktum at utlevering av opplysninger om hvilke ip-adresser en person har benyttet i et gitt tidsrom vil være å anse som skjult overvåking, spesielt siden forslaget åpner for å gjøre dette i forebyggingsøyemed. I tillegg vil også være tilfeller der hvor etterforskning er iverksatt overfor en person uten at hen er klar over det.

Forslaget innebærer en registrering av nesten alle norske borgere som på en eller annen måte benytter ip-adresse, og det åpner for at politi eller PST i saker hvor det er «nødvendig» vil kunne innhente alle ip-adresser knyttet til en person i et gitt tidsrom. Dette åpner for en kontinuerlig overvåkning unntatt domstolskontroll og Kontrollutvalget for kommunikasjonskontroll, ved at politiet kan be om ukentlige eller daglige oppdatering av benyttede ip-adresser og dermed lage seg et bilde av personens bevegelser.

I saker som omhandler statlig overvåking har EMD gjennom sin praksis derfor etablert en rekke minimumskrav kalt Weber-kriteriene formulert i *Weber og Saravia* som må være oppfylt for at bulkinnhenting av kommunikasjonsdata skal være i tråd med menneskerettighetene.

Weber-kriteriene kan sammenfattes som krav til:

- den nasjonale loven som lovfester inngrepet må være tilgjengelig, herunder er det et krav til tilstrekkelig klar beskrivelse av hvilke forhold som kan begrunne innhenting og lagring av opplysninger, og en angivelse av hvilke personer eller grupper som kan bli gjenstand for tiltaket
- prosedyre for forhåndsgodkjenning
- prosedyrene for lagring, tilgang, bruk, deling og sletting av data
- kontrollmekanismer, herunder underretning til den registr
- krav til et effektivt rettsmiddel

Kravene i EMK art. 8.2 er kumulative, det vil si at *alle* kravene må være oppfylt for at et inngrep kan anses å være innenfor de rettslige skranker. Samtidig er det viktig å poengtere at det må foretas en helhetsvurdering av alle kravene for å fastslå om et inngrep er berettiget. Dersom et av kravene ikke er tilstrekkelig ivaretatt, vil det kunne avhjelpes ved sterkere oppfyllelse av et av de andre kravene. Det er totale forslaget som må vurderes på en helhetlig rettslig og samfunnsmessig måte.

Høringsnotatet behandler ikke dette spørsmålet, som må anses som svært sentralt i forståelsen av tiltakets rekkevidde og konsekvenser.

Nødvendighetskriteriet og forholdet til personopplysningsloven

I forslagets 2-8 b er det formulert at det kun er opplysninger som er «nødvendig» for å forebygge eller etterforske en straffbar handling med en gitt strafferamme som skal utleveres. Høringsnotatet gir liten veiledning i hvordan begrepet «nødvendig» skal forstås.

I merknad til den foreslåtte § 2-8b ber det blant annet pekt på at det ikke kan innhentes flere opplysninger enn det som i det enkelte tilfellet trengs for formålet, og at det det må foretas en konkret vurdering av behovet for opplysningene, som må veies mot hensynet til kommunikasjonsvernet.

Tilbyderne er omfattet av personopplysningsloven da det er klart at ip-adresser, både statiske og dynamiske, er personopplysninger og spesielt der hvor de er i kombinasjon med abonnementsopplysninger.

En utlevering vil da måtte hjemles i personvernforordningen art. 6 nr. 1 c, en rettslig forpliktelse, og i og med at begjæringen om utlevering ikke er foreslått å være gjenstand for en vurdering av NKOM eller domstol, så vil det være tilbyders ansvar på påse at det ikke utleveres opplysninger i strid med personvernforordningen.

Tilbyder vil ha et ansvar for hverken å bryte ekomloven og personopplysningsloven.

Forslaget innebærer også at tilbyderne må etablere en database over tildelte ip-adresser som er en behandling som er omfattet av personvernforordningen. Den registrerte har her en rekke

rettigheter som retten til sletting, korrigering, dataminimering etc. Høringsnotatet drøfter ikke hvordan forholdet mellom de registrertes rettigheter og plikten til å lagre skal løses.

Personopplysningsloven gjelder ikke for saker som behandles eller avgjøres i medhold av rettspleielovene (domstolloven, straffeprosessloven, tvisteloven og tvangsfullbyrdelsesloven mv.). jf. § 2 annet ledd bokstav b, men dette unntaket vil jo ikke kunne anvendes på tilbyderens behandling av ip-opplysningene da deres behandling ikke er omfattet av disse lovene.

Det må stilles svært strenge krav til kvalitetene på opplysningene i databasen over ip-opplysninger og i og med den ikke kan reguleres av politiregisterloven, så vil det være personvernforordningen som gjelder.

Det er heller ikke tatt stilling til om hvordan unntaket i personopplysningsloven § 16 bokstav b om unntak fra retten til informasjon og innsyn etter personvernforordningen artikkel 13, 14 og 15 for opplysninger som det er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger.

Dette vil jo eventuelt gjelde et svært lite antall av de registrerte, mens f.eks. alle barn som har en mobiltelefon og skole-pc vil bli registrert når de logger seg på internett.

Forslaget er formulert som en plikt overfor tilbydere, men er i realiteten enn innskrenkning i borgernes rett til kommunikasjon uten innblanding fra myndigheter. Ethvert inngrep overfor borgernes rettigheter krever hjemmel i lov, men slik forslaget er formulert tar det ikke stilling til hvilke begrensninger i sine rettigheter de registrerte eventuelt må tåle. Hvordan skal man for eksempel møte et krav om sletting fra et barn som mener at behandling av akkurat hen sine ip-opplysninger ikke er nødvendig?

Eller mer konkret en journalist som ber om sletting med begrunnelse i kildevernet?

For å kunne ivareta sine rettigheter så er det avgjørende å kunne få innsyn i hvilke opplysninger som lagres og hva som eventuelt kan bli utlevert. Det er ikke drøftet i høringsnotatet hvordan det skal løses praktisk. I det tilfelle der hvor abonnementsholderen ikke er den samme som brukeren, så vil det kunne medføre praktisk og rettslige utfordringer for å få tilgang. Det vil også være en utfordring å få tilsvarende opplysninger som politiet der hvor det er flere tilbydere knyttet til en persons ip-adresser. Det er imidlertid viktig at retten til innsyn i de opplysninger som lagres om en, i dette tilfellet IP-opplysninger, ikke innskrenkes.

Sivile søksmål

Datatilsynet er helt imot at eventuelle opplysninger skal gjøres tilgjengelig i sivile saker. Dette illustrerer hvorfor lagring av opplysninger til et formål alltid innebærer en risiko for formålsutglidning.

Personopplysninger knyttet til IP-adresser er meget usikre. Den lagringen som foretas av tilbyderne i dag er ikke etablert for å benyttes for straffeforfølging eller i sivile saker og det vil utgjøre en stor risiko for at feil person vil bli plukket ut.

I høringsnotatet argumenteres det med tungtveiende kriminalitetsbekjempende hensyn, men det kan ikke begrunne hvorfor det er nødvendig med en så omfattende overvåkning i åndsverkssaker. Dette er et eget formål, som det på langt nær ligger så tungtveiende hensyn bak.

Dette går også utover Stortingets anmodningsvedtak nr. 944, 15. juni 2017 hvor regjeringen utredet om det rettslige handlingsrommet for generell lagring av IP-adresser og relevant trafikkdata bør utvides, som et nødvendig virkemiddel i kampen mot kriminalitet, herunder overgrep mot barn.

Datatilsynet forstår også *Quadrature* slik at det er kun kriminalitetsbekjempelse som formål som eventuelt kan rettferdiggjøre en lagringsplikt. Tilgang i sivile saker, særlig på et så upresist rettsgrunnlag som i dag, kan dermed medføre at hele lagringsregimet underkjennes på EU/EØS-rettslig grunnlag.

Avsluttende bemerkninger

Datatilsynet mener at forslaget ikke er tilstrekkelig godt nok utredet i og med at sentrale menneskerettslige spørsmål og forholdet til personopplysningsloven ikke er avklart.

Et tiltak av dette omfanget kan ikke oversendes Stortinget uten at dette har blitt utredet grundigere og sendt på ny høring.

Personvernkonsekvensene av lovforslaget er ikke tilstrekkelig vurdert i notatet, noe som er en plikt etter personvernforordningen art. 35. For å ivareta den demokratiske kontrollen med forvaltningen, må Stortinget få forelagt informasjon som gjør at det kan ta stilling til påregnelige konsekvenser og risiko ved å innføre hjemler som kan yte stor påvirkning på personvernets stilling i Norge.

Datatilsynet vil også bemerke at Stortinget i anmodningsvedtak nr. 944, 15. juni 2017 spesielt ba om at hensynet til personvern skulle ivaretas.

Det følger av personvernforordningen art. 36 nr. 4 at medlemsstatene skal rådføre seg med tilsynsmyndigheten ved utarbeiding av forslag til lovgivning som skal vedtas av et nasjonalt parlament, eller av et reguleringstiltak som er basert på slik lovgivning, og som er knyttet til behandling av personopplysninger. Denne plikten inntreffer dersom vurderingen av personvernkonsekvenser i medhold av art. 35 konkluderer med at forslaget sannsynligvis vil medføre høy risiko for den registrertes rettigheter og friheter. Regelen i art. 36 nr. 4 innebærer at slik forhåndskonsultasjon må gjennomføres før lovforslaget sendes ut på ordinær høring. Dette er en plikt som følger av personvernforordningen, og en eventuell unnlatelse vil kunne innebære et brudd på personvernforordningen, og dermed også Norges EØS-rettslige forpliktelser.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Jan Henrik Mjønes Nielsen
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer