Jesper Lund
IT-Politisk Forening

Europaudvalget, 3. februar 2017

Muligheder og risici ved ePrivacy

Tak for invitationen til dette møde. Min baggrund for dette indlæg er i høj grad IT-Politisk Forenings medlemskab af European Digitial Rights (EDRi), som meget aktiv inden form områderne privacy og persondatabeskyttelse, specielt i forhold til EU-lovgivning. EDRi har nedsat en arbejdsgruppe om revision af ePrivacy lovgivningen, hvor vi er i fuld gang med at analysere det nye forslag.

Den 10. januar 2017 har Kommissionen fremsat et forslag til en forordning om beskyttelse af personlige data i elektronisk kommunikation, som skal erstatte det nuværende ePrivacy direktiv 2002/58 (eller e-databeskyttelsesdirektivet, som det også hedder).

Det overordnede formål er at supplere den almindelige persondatalovgivning med regler, som er specifikke for elektronisk kommunikation, og som giver en højere grad af beskyttelse.

Det er der behov for. Elektronisk kommunikation, både indhold og metadata, indeholder ofte mere følsomme detaljer om borgernes privatliv end almindelige personoplysninger i registre. Mange lande har i deres forfatning særlige bestemmelser om beskyttelse af kommunikationshemmeligheden, for eksempel vores egen § 72 i grundloven.

Det nuværende direktiv for beskyttelse af elektronisk kommunikation (ePrivacy) er fra 2002. Fordi persondatadirektivet fra 1995 erstattes af persondataforordningen, er der behov for en opdatering af ePrivacy reglerne, så de to lovgivninger er konsistente i deres indbyrdes referencer.

Forslaget til ny ePrivacy forordning indeholder samtidig en meget vigtig teknologisk opdatering, så det afspejler de kommunikationstjenester som borgerne benytter i dag. I 2002 dækkede fastnet og mobiltelefoni med tale og sms stort set al elektronisk kommunikation, og de eksisterende regler omfatter kun teleselskaber.

I dag bruger vi smartphones og de såkaldte over-the-top (”OTT”) kommunikationstjenester, som Skype, Facebook Messenger, WhatsApp og DM på Twitter. Antallet af SMS-beskeder hos teleselskaberne falder faktisk, men det er ikke fordi danskerne kommunikerer mindre med hinanden. De bruger bare andre tjenester, som ikke er omfattet af det nuværende ePrivacy direktiv.

Hvis man sammenligner ePrivacy reglerne med den kommende persondataforordning er den primære forskel, at der ikke er mulighed for at behandle persondata uden samtykke via det princip som hedder legitim interesse. Legitim interesse indebærer, at virksomheden skal afveje sine egne interesser i at bruge persondata mod datasubjektets, altså borgerens, interesser.

Grundlaget for behandlingen under ePrivacy er enten brugerens samtykke eller en specifik tilladelse i lovgivningen.

At ophæve ePrivacy direktivet, som nogle har foreslået i forbindelse med evalueringen af direktivet, ville føre til en dårligere beskyttelse af kommunikationshemmeligheden, selv når persondataforordningens generelt skærpede behandlingsregler træder i kraft i maj 2018.

Derfor er vi overordnet set meget glade for at Kommissionen har valgt at fremsætte et forslag om en ny ePrivacy forordning.

Det nyt forslag omfatter de samme tre hovedområder som det nuværende direktiv:

- Elektroniske kommunikationstjenester
- Beskyttelse af brugerens terminaludstyr (”cookie reglerne”)
- Uopfordrede markedsføringshenvendelser (her er der ingen reelle ændringer i forhold til de nuværende bestemmelser)

Derudover ændres bestemmelserne om tilsynsmyndigheden.

Elektroniske kommunikationstjenester

Den store forskel vedrørende elektroniske kommunikationstjenester er at OTT-tjenester bliver omfattet af de samme regler som teletjenester. Det gælder VoIP-tjenester som Skype, besked-tjenester som Facebook Messenger, og email-tjenester som GMail. Det er meget positivt, da det udvider beskyttelsen af borgerens privatliv i forhold til i dag, og harmoniserer kravene på et højt beskyttelsesniveau.

Hovedprincipperne fra det nuværende direktiv videreføres. Kommunikationsdata (både indhold og metadata) må kun behandles af udbyderen til at overføre selve kommunikationen, og ikke til andre formål uden samtykke.

Metadata er oplysninger om hvem der kommunikerer hvem, hvor de er (lokation), og tidspunkt og varighed for kommunikationen. Metadata kan være ligeså afslørende som indholdet af kommunikationen, specielt når det er muligt at katalogisere store mængder metadata, enten en persons sociale graf (kontakter) eller personens færden i

den fysiske rum via lokationsdata.

Det nuværende direktiv kræver sletning af metadata (trafikdata) ved afslutning af kommunikationen, medmindre oplysningerne skal bruges til fakturering eller hvis staten via en lov stiller krav om at visse metadata skal gemmes, som logningsbekendtgørelsen.

Derudover kan kommunikationsdata behandles til tillægstjenester som brugeren har bedt om via et særskilt samtykke. Det kunne f.eks. være en lokationstjeneste som sender en sms med reklamer fra butikker i nærheden af hvor man er. Et dansk teleselskab kører forsøg med en sådan tjeneste.

Disse elementer videreføres for teleselskaber og indføres som nye lovkrav for OTT-tjenester.

Der er også lempelser af databeskyttelsen efter ønske fra den europæiske teleindustri, som formentlig har et godt ”big data” øje for alle de data, som genereres i forbindelse med elektronisk kommunikation.

Det bliver muligt **med samtykke** at levere metadata til udbyderens egne tjenester. Kommissionen omtaler såkaldte ”heat maps” som et eksempel. Det kunne være optælling af hvor mange personer der er i bestemte dele af byen, eller hvor Folkemødets deltagere kommer fra.

Derudover får udbyderne mulighed for at behandle og gemme visse metadata til formål som netværkssikkerhed og kontrol af servicekvaliteten, som de ikke har i dag. Det sidste vil være **uden samtykke**.

Den primære risiko ved forslaget er de nye muligheder for at gemme metadata, som kan afsløre væsentlige detaljer om borgernes privatliv. Borgerne kan også blive stillet over for at skulle give samtykke til en lang række formål, som kan være svære at overskue (måske med valg som er præ-udfyldt med ”ja”). Og mulighederne for at gemme metadata uden samtykke til kontrol af servicekvaliteten i forordningsforslaget mangler nogle begrænsninger og obligatoriske risikovurderinger.

Beskyttelse af brugerens terminaludstyr (”cookie reglerne”)

Jeg regner med at Anette Høyrup har dækket dette område, men at jeg kan give et lidt andet perspektiv.

Dette et svært område. Mange borgere og virksomheder er irriteret over de mange cookie banners som ses på hjemmesider. Men samtidig siger mange borgere, at de er bekymret for overvågning på internettet.

Cookie-reglerne blev indført ved en ændring af ePrivacy direktivet i 2009. Formålet er at beskytte borgerne mod tracking på internettet, altså det at en 3. part kan registrere hvilke websider borgeren besøger og lave en adfærdsprofil af borgeren. En adfærdsprofil, der kan bruges til målrettet markedsføring, hvor andre ultimativt kan komme til at træffe borgernes forbrugsvalg.

Denne tracking sker på baggrund af oplysninger fra browseren (”terminaludstyret”), typisk cookies. Meningen i 2009 var uden tvivl at borgerne skulle kunne sige nej til cookies og dermed tracking efter at have fået grundig information. Men det er ikke sket. Borgerne får ikke reel information, kun overfladiske oplysninger om formålet. Selv om der i direktivet tales om samtykke, er det sjældent muligt at sige nej, noget som er blevet kaldt ”cookie muren”.

Problemerne med tracking er blevet meget værre siden 2009. Vi har mange flere enheder, som er på nettet, og som kan indsamle data om vores adfærd. Der kan i nogle tilfælde være tale om en nærmest fuldstændig kortlægning af vores adfærd online og potentielt også i det fysiske rum.

Her kunne det være relevant at rejse spørgsmålet, om vi overhovedet skal tillade at private virksomheder laver disse fuldstændige kortlægninger af vores adfærd. I den forbindelse skal man huske at det, som vi i givet fald taler om her, ikke er et forbud mod reklamer på internettet, men et forbud mod systematisk overvågning/tracking af brugerne.

Men så langt vil Kommissionen ikke gå. I stedet prøver Kommissionen at løse den nærmest umulige opgave med at bevare kravet om samtykke og samtidig reducere antallet af cookie banners. Cookies der alene bruges til webstatistik vil ikke længere kræve samtykke. Det vil være til gavn for offentlig hjemmesider, men uden betydning for de fleste private hjemmesider, fordi de typisk har cookies til tracking.

Metoden til at få færre cookie banners, og anmodninger om samtykke, skal efter Kommissionens forslag ske ved at flytte samtykke-beslutningen til browseren. Nu bliver det desværre lidt teknisk, men browser leverandørerne (f.eks. Microsoft der leverer Internet Explorer) skal bede brugeren vælge mellem forskellige niveauer for modtagelse/afvisning af cookies, og dette valg i browseren bliver det fremtidige samtykke i forhold til cookies.

Der er fordele og ulemper for borgerne her. Alle vil nok glæde sig over færre samtykkeanmodninger, men samtykke via tilladelse eller afvisning af cookies i browseren bliver et generelt samtykke for alle websites. Det kan ikke blive et rigtigt informeret samtykke.

Vi kan også se en klar risiko for, at brugerne bliver presset til at tillade 3. parts cookies, dem som bruges til tracking, og så vil overvågningen bare ske i det skjulte.

Tilsynsansvaret

Kommissionens forordningsforslag siger til at tilsynsansvaret for hele ePrivacy området skal ligge hos datatilsynsmyndigheden i de respektive EU-lande. I dag har nogle lande, bl.a. Danmark, lagt ansvaret hos telemyndigheden (Erhvervsstyrelsen).

Vi ser dette som en klar styrkelse af borgernes privatliv online. Det formelle samarbejde mellem EU's datatilsynsmyndigheder kommer til at omfatte den særlige databeskyttelse inden for ePrivacy området. Det er vigtigt fordi danskerne benytter mange udenlandske tjenester, som Facebook.

Derudover vil den nuværende gråzone mellem Datatilsynets og Erhvervsstyrelsens ansvar i forhold til især lagring af cookies og den efterfølgende behandling af personoplysninger blive elimineret, fordi det nu er samme myndighed.

Tak for opmærksomheden.