Regler om tilrettelagt innhenting i ny lov om Etterretningstjenesten – hva er betydningen for personvernet?

Petter Bjerke
Partner, Faggruppeleder
personvern og immaterialrett

EUs datalagringsdirektiv skulle pålegge norske e-komtilbydere en plikt til å lagre ulike typer data opptil seks måneder. Plikten ble implementert i e-komloven i 2011, men trådte aldri i kraft, som følge av at EUs datalagringsdirektiv ble kjent ugyldig i 2014. Gjennom den nye loven om Etterretningstjenesten, som ble vedtatt 11. juni 2020 , har vi fått et nytt regelverk som omfatter innhenting og lagring av ulike typer data. Loven vil tre i kraft 1. januar 2021.

En endring fra den tidligere etterretningstjenesteloven av 1998 er at det kan oppstå en plikt for såkalt tilrettelagt innhenting. Tilrettelagt innhenting vil si at det innhentes grenseoverskridende elektronisk kommunikasjon til bruk for etterretningsformål. Enhver som tilbyr tilgang til elektronisk kommunikasjonsnett eller -tjeneste (e-komtilbydere), og tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten, kan få en tilretteleggingsplikt overfor Etterretningstjenesten. Tilrettelagt innhenting har direkte betydning for personvernet, noe vi vil se nærmere på i denne artikkelen.

Tilretteleggingspliktens formål og forholdet til personvernforordningen, GDPR

Tilrettelagt innhenting skal ivareta Etterretningstjenestens oppgaver. Etterretningstjenesten er Norges sivile og militære utenlandsetterretningstjeneste, og innhenter og bearbeider informasjon som gjelder norske interesser. En viktig hensikt med arbeidet er å kunne varsle om utenlandske trusler, for å danne grunnlag for myndighetenes avgjørelser om rikets sikkerhet.

Det er fremhevet i lovproposisjonen (Prop. 80 L) at den teknologiske utviklingen har medført at myndighetene i dag har begrenset mulighet for å oppdage, følge opp og hindre utenlandske trusler mot Norge. En av hensiktene med den nye loven er å gjøre den norske Etterretningstjenesten i større grad i stand til å kunne fange opp, følge opp og motvirke slike trusler. Flere av endringene er et resultat av en avveining av hensynet til dette, vurdert opp mot personvernhensyn. Det antas i lovproposisjonen at tilrettelagt innhenting forventes å ha stor etterretningsmessig verdi. I den forbindelse er det blant annet vist til erfaringer fra Sverige og Finland.

Kravet om at informasjonen som et klart utgangspunkt må være *grenseoverskridende* henger sammen med lovens virkeområde. Loven er ikke ment å dekke *innenlands* overvåkning (altså mellom borgere i Norge). Dette er politiets og PSTs oppgave. Personvernforordningen, GDPR, gjelder *ikke* for utenlandsetteretning. De alminnelige rettighetene i GDPR for de registrerte (retten til innsyn, varsling, sletting mv.) gjelder derfor ikke for de behandlingsaktiviteter som omfattes av den nye loven om Etterretningstjenesten. Sikkerhetsgarantier i forhold til borgernes personvern er søkt ivaretatt gjennom domstolskontroll og EOS-utvalget (nærmere om dette under). Videre har loven egne bestemmelser om behandling av personopplysninger slik som sletting, formålsbegrensing mm.

Metadata og innholdsdata

Før vi går nærmere inn på tilretteleggingspliktens innhold, er det viktig å klare *hvilke* typer data som omfattes av loven. En elektronisk kommunikasjon består av ulike typer *data.* For det første har man såkalt "*metadata".* Metadata er i loven definert som "*data som beskriver annen data eller som inneholder ekstra informasjon knyttet til data, blant annet data som beskriver formatet på innholdet, hvem som er avsender og mottaker, eller kommunikasjonens størrelse, posisjon, tidspunkt eller varighet*.

For det andre har man "innholdsdata" – dvs. *innholdet* i en elektronisk kommunikasjonen (f.eks. tekst, lyd, bilde). Mens loven har en uttømmende definisjon av *metadata,* er *innholdsdata* negativt definert som "*data som ikke er metadata*."

Tilretteleggingsplikt for ekomtilbydere og andre tjenestetilbydere

Ekomtilbydere og tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten, kan altså få en tilretteleggingsplikt overfor Etterretningstjenesten.

Det er forutsatt i lovproposisjonen at plikten også gjelder for internettbaserte "over the top-tjenester" (OTT-tjenester) som kan brukes til å overføre tekst, lyd og bilder. Forarbeidene gir ikke et klart svar på om det kun er OTT-tjenester i form av meldingstjenester og kommunikasjonstjenester som omfattes, f.eks. Messenger eller Zoom, eller om plikten også kan ilegges tilbydere av for eksempel strømmetjenester. Både formålet med loven og ordlyden tilsier imidlertid at tjenestene må være tilrettelagt for kommunikasjonsutveksling på en eller annen måte, for at plikten skal kunne gjelde.

Plikten innebærer at tilbyderne vil kunne bli pålagt å gjøre data tilgjengelig for Etterretningstjenesten ved såkalt "speiling". Det vil for eksempel kunne bety at en tilbyder av telefonitjenester vil kunne bli pålagt å tilgjengeliggjøre meldinger som er sendt på tvers av landegrensene, for Etterretningstjenesten. En slik "speiling" innebærer at både innholdsdata og metadata gjøres tilgjengelig for Etterretningstjenesten "live". Plikten kan omfatte ulike måter for tilrettelegging for utvalg, filtrering, testing, innhenting, lagring og søk.

Tilretteleggingsplikten inntreffer ikke uten at det først tas en beslutning om det. Sjefen for Etterretningstjenesten tar avgjørelsen, og det fremgår av loven at tilbyderen skal kunne få uttale seg først. Beslutningen kan gjelde for tre år.

Hvis det fattes en beslutning om tilrettelegging, må tilbyder bidra på de måter som fremgår av loven. Blant annet må tilbyder tillate at Etterretningstjenesten installerer utstyr på steder som kontrolleres av tilbyder, og sørge for tilgang til kommunikasjon uten krypteringshindre som tilbyder kontrollerer. Tilbyderne blir også ilagt en taushetsplikt.

En tilretteleggingsbeslutning påvirker imidlertid ikke hvordan tilbyderen må forholde seg til personvernregler generelt. For eksempel har beslutningen ingen betydning for hvor lenge tilbyder lagrer opplysninger, eller hvordan opplysningene for øvrig behandles i tilbyders egen virksomhet.

Utvalg og filtrering

Den tilrettelagte innhentingen er altså ment å kun fange opp grenseoverskridende elektronisk kommunikasjon.

Datatilsynet har i sitt høringssvar fremhevet at selv om formålet med den nye loven er å motvirke angrep fra utlandet mot Norge, vil endringene i stor utstrekning påvirke også brukere av telefoni- og kommunikasjons- og meldingstjenester innenfor Norges grenser. Grunnen til dette er at den tekniske infrastrukturen/servere ofte befinner seg utenfor Norge. Dette gjelder for eksempel tjenester som Snapchat og Messenger. De inngripende personverntiltakene rammer derfor ikke kun kommunikasjon over landegrensene, men også ofte kommunikasjon mellom personer som fysisk oppholder seg i Norge. Det er derfor inntatt en bestemmelse om at Etterretningstjenesten gjennom utvalg og filtrering skal søke å hindre lagring av metadata hvor både avsender og mottaker oppholder seg i Norge.

Det fremgår også av proposisjonen at det i dagens teknologiske situasjon ikke vil være mulig å hindre lagring av store mengder metadata om norsk innenlandsk kommunikasjon, og at plikten til å filtrere ut kommunikasjon innenfor Norges grenser, derfor er utformet som en plikt til å "søke" å hindre lagring av denne type data. Lovens faktiske nedslagsfelt vil derfor kunne bli større enn hva som samsvarer med formålet.

Lagring av metadata (data om data) i bulk

Med den nye loven blir det også adgang til såkalt innhenting og lagring av metadata i bulk, det vil si hvor en vesentlig andel av informasjonen antas å være irrelevant for etterretningsformål. Begrepet metadata brukes som nevnt for å beskrive data som beskriver annen data, eller som inneholder ekstra informasjon knyttet til data, for eksempel formatbeskrivende data, eller data om posisjon, tidspunkt, avsender og mottaker mv. Innholdsdata, som altså omfatter all data som ikke er metadata, omfattes ikke av adgangen til å lagre i bulk.

Datatilsynet påpekte i sin høringsuttalelse at analyse og sammenstilling av metadata vil kunne avsløre sensitive forhold om enkeltpersoner, og at dette er problematisk fra et personvernperspektiv. Departementet er i betydelig utstrekning enig. I lovproposisjonen uttales det at innhenting og lagring av metadata i bulk *"er det mest problematiske fra et personvernperspektiv",* og at inngrepet må *"regnes som betydelig".* Slik innhenting og lagring anses likevel å være viktig fra et etterretningsperspektiv.

Etterretningstjenesten må slette lagrede metadata senest etter 18 måneder.

Søk i metadata lagret i bulk krever kjennelse fra retten, og kan kun utføres av personell i Etterretningstjenesten som er vurdert som skikket til det, og som har gjennomgått særskilt opplæring.

Testinnhenting og testanalyser

Det blir også adgang til innhenting, lagring og analyse av testdata i et korttidslager. I proposisjonen blir det fremhevet at også dette er inngripende i personvernet, spesielt fordi det er tale om ufiltrert informasjon, men at dette er avgjørende for drift av systemet. Testinnhentingen skjer ved uttrekk av ufiltrert kommunikasjon, som ikke skal overstige 30 sekunder. Uttrekkene blir lagret i et kortidslager, og opplysningene kan ikke lagres lenger enn to uker.

Målrettet innhenting og lagring av innholdsdata

Lovvedtaket inneholder også regler om målrettet innhenting og lagring av innholdsdata, som altså omfatter alt som ikke er metadata.

Domstolen kan ved kjennelse gi Etterretningstjenesten adgang til å målrettet innhente og lagre innholdsdata. Det uttales i proposisjonen at selv om slik målrettet innhenting og lagring vil kunne være inngripende for de som rammes, er ikke regelendringene på langt nær like alvorlige for personvernet som lagring av metadata i bulk, og lagring av testdata. På tross av at tilgang til innholdsdata isolert sett må anses å være mer inngripende enn tilgang til metadata, innhentes og lagres ikke innholdsdata i bulk, og innhentingene er derfor mer spisset. Innhenting godtas kun for utenlandsetterretningsformål.

Kontrollmekanismer, sletting mv.

Vedtaket har flere bestemmelser som skal sikre etterlevelse og kontroll, sletting og øvrige rettssikkerhetsgarantier.

Som nevnt må domstolene være involvert ved visse avgjørelser. Flere høringsinstanser har imidlertid påpekt at det kan være vanskelig å føre en reell kontroll, idet flere av bestemmelsene er vage og gir stort rom for skjønn.

Det skal også utøves en løpende kontroll av det såkalte EOS-utvalget. EOS-utvalget skal blant annet se til at søk kun gjennomføres i samsvar med rettens kjennelser, og at korttidslageret og testdata kun brukes til teknisk understøttelse.

Nasjonal kommunikasjonsmyndighet (Nkom) skal føre tilsynet med utføringen av e-komtilbydernes bidragsplikt.

Det er også bestemt at Etterretningstjenesten ikke skal innhente informasjon til bruk for utførelse av politiets oppgaver. Det er derfor inntatt eksplisitte bestemmelser for å tydeliggjøre formålsbegrensningen til utenlands etterretning og forbud mot å innhente informasjon med politiformål og forbud mot industrispionasje. Opplysningene skal kun brukes til de fastsatte formålene.

Personopplysninger skal slettes når de ikke lenger er nødvendige for formålet med behandlingen. Metadata som er innhentet og lagret i bulk skal som nevnt være slettet etter 18 måneder.

Hva betyr endringene for personvernet?

Vi er enige med departementet og flere av høringsinstansene i at reglene om tilrettelagt innhenting har store konsekvenser for personvernet, og at det spesielt gjelder lagring av metadata i bulk og testene som kan gjennomføres av ufiltrert data. Det blir også interessant å følge med på hvordan reglene fungerer i praksis, herunder e-komtilbyderes og andre tjenestetilbyderes tilretteleggingsplikt, idet det på nåværende tidspunkt er noe uklart hvilke tilbydere som er omfattet og rekkevidden av plikten. Som vi har vært inne på, vil det heller ikke være mulig å fullt ut gjennomføre filtrering av metadata sendt mellom avsender og mottaker i Norge, slik at denne type data også vil kunne bli masselagret.

Services	Immaterialrett og teknologi