R E T S P O L I T I S K F O R E N I N G

Retspolitisk Forenings kommentar til udkast til beretning nr. 3 fra Folketingets Retsudvalg og Kulturudvalg.

Indledende bemærkninger og problemstilling.

Retspolitisk Forening (RPF) har noteret sig, at udvalgenes overvejelser tager udgangspunkt i sagen om videregivelse og offentliggørelse af fortrolige oplysninger i ugebladet Se og Hør. Således som Foreningen vurderer problemstillingen også i udgangspunktet, er den langt bredere og omfatter enhver registrering, behandling og videregivelse af personfølsomme oplysninger. Dette synes da også at kunne læses ud fra de bemærkninger udvalgene er fremkommet med under afsnittet "politiske bemærkninger", hvori det bl.a. hedder:

" At regeringen pålægges at udvide det af ministeren nedsatte tværministerielle embedsmandsudvalg, der skal kortlægge sikkerhedsproblemer, for så vidt angår betalingskort m.v., til at omfatte alle områder, hvor der opbevares personfølsomme oplysninger og data. Dette kan eventuelt ske i flere etaper, hvor forskellige områder afdækkes løbende, så hastigheden fremmes".

Tillige kan navnlig de efterfølgende pålæg til regeringen forstås som en erkendelse af, at problemstillingen er langt bredere og væsentligt mere kompliceret end et om end klart retsstridigt brud på fortrolighedsreglerne for NETS. Det hedder bl.a, at regeringen: skal

" ..aktivt at arbejde for, at persondatabeskyttelsen vægtes højt i det kommende EU-direktiv/ forordning på databeskyttelsesområdet. Regeringen opfordres til at samarbejde aktivt med bl.a. Tyskland og Frankrig, der i modsætning til Danmark har været særdeles aktive i den forløbne proces, for så vidt angår sikringen af personfølsomme data, herunder offentlige data".

Et brud på de gældende regler, således som det er sket i Se og Hør sagen, er i realiteten umuligt at gardere sig i mod, men skal naturligvis retsforfølges. Det skal desuden bemærkes, at konsekvensen af disse ulovlige handlinger både for så vidt angår NETS og Se og Hør forekommer behersket, objektivt set uinteressant og forholdsvis uskyldigt. Hvorvidt et medlem af kongehuset har benyttet sit kreditkort et eller andet sted i verden, synes at være en oplysning, der hverken er særligt overraskende eller interessant ud fra en generel synsvinkel

om beskyttelse af privatlivets fred. Se og Hørs brug af oplysninger fra NETS kan sammenlignes med videregivelse af såkaldte trafikdata, men i de mange tilfælde, hvor Se og Hør har benyttet oplysningerne, har anvendelsen været kendt, idet de benyttede data har været grundlag for offentliggørelse af journalistisk bearbejdede meddelelser. Dette indebærer selvsagt ikke en accept af de begåede ulovligheder, men retter fokus mod den behandling og videregivelse, der finder sted på et helt lovligt grundlag.

EU's arbejde med et nyt direktiv om databeskyttelse må imidlertid forventes kun i særdeles begrænset og kun indirekte omfang at tage stilling til indsamling, bearbejdning og videregivelse af data indsamlet af medlemslandendes efterretningstjenester eller retshåndhævende myndigheder, da disse myndigheders virksomhed ikke umiddelbart er omfattet af unionens traktatbestemmelser og derfor heller ikke er dækket af bestemmelserne i unionens menneskerettighedscharter.

RPF læser opgavebeskrivelsen i beretningsudkastet s. 2 for de foreslåede parlamentariske arbejdsgrupper, således, at disse alene skal tage stilling til indsamling, behandling og videregivelse af personoplysninger, der befinder sig i private eller koncessionerede databaser. Det anføres således:

" afdækning af beskyttelsen af borgernes personfølsomme oplysninger og forventes konkret at se på i hvert fald følgende områder:
– Logningsreglerne og personoplysningsloven.
– EU's nye databeskyttelsesforordning og forbedringer af persondataloven, herunder retten til at blive glemt på nettet.
– Eksternt tilsyn med overholdelse af gældende lovgivning, herunder Datatilsynets kompetencer og ressourcer, samt andre tilsynsorganer af relevans for området og behovet for eventuel oprettelse af nye organer.
– Behovet for samling af it- og datasikkerhed ved en ansvarlig ressortminister.
– Internt tilsyn, herunder sikkerhedsgodkendelse af personer med adgang til personfølsomme data, samt opdeling af medarbejdere i flere sikkerhedsniveauer, der regulerer adgangen til oplysninger.
– Erfaringen med anonymisering af data, således at fordelene ved store datasæt til brug f.eks. forskning eller
kommerciel udnyttelse af big data ikke umuliggøres, men at det samtidig sikres, at data ikke kan føres tilbage til en kendt identitet."

Retspolitisk Forening finder det væsentligt og positivt, at udvalgene er opmærksomme på disse problemstillinger, men skal tillige anføre, at de angivne problemstillinger ikke forekommer dækkende for behovet for en grundig bearbejdning af samtlige spørgsmål, der vedrører data, der omfatter oplysninger, der kan henføres til grundlovens bestemmelser om brud på meddelelseshemmeligheden (§ 72), der alene hjemler en *særegen* lovfæstet undtagelse fra kravet om retskendelse.

Foreningen skal herefter bemærke:

Offentligt indsamlede oplysninger, herunder oplysninger indhentet af efterretningstjenesterne. Den relevante lovgivning er lovene om politiets og forsvarets efterretningstjenester, lov om center for cybersikkerhed samt persondataloven.

> I tilslutning hertil bør tillige nævnes den såkaldte logningsbekendtgørelse, der forpligter teleselskaberne til opbevaring og registrering af ganske betydelige datamængder (ifl. Justitsministeriet alene i 2008 450 mia. posteringer). Logningsbekendtgørelsen ændres dog, således, at de såkaldte sessionslogninger (internetlogninger) glider ud. Det må imidlertid forventes, at bekendtgørelsen helt ændres som følge af EU-domstolens dom af 8. april 2014, der erklærer bekendtgørelsens underliggende EU-retsakt (det europæiske logningsdirektiv (2006/24/EC)) for et for omfattende og alvorligt indgreb i retten til privatlivets fred og ikke i tilstrækkelig grad tager hensyn til beskyttelse af personoplysninger.

1. Loven om Forsvarets Efterretningstjeneste

Forsvarets Efterretningstjeneste kan *indsamle og indhente* oplysninger, der *kan* have betydning for tjenestens efterretningsmæssige virksomhed (FE-lovens §3). Som udgangspunkt er persondataloven ikke gældende for tjenestens virksomhed. Tjenesten kan *behandle* enhver personoplysning vedrørende en i Danmark hjemmehørende fysisk person, hvis behandlingen…. må antages at have betydning for varetagelsen af tjenestens opgaver efter lovens § 1, stk. 1 og 4, eller er nødvendig for varetagelsen af tjenestens opgaver efter § 1, stk. 2. Disse opgaver er i lovteksten beskrevet bredt, men skal selvsagt forstås i lyset af tjenestens funktion som Danmarks udenrigsefterretningstjeneste og militære efterretningstjeneste.

Tjenesten kan *behandle* oplysninger vedrørende en i Danmark hjemmehørende fysisk person efter samme kriterier. *Videregivelse*, herunder videregivelse til udenlandske myndigheder og private, af sådanne oplysninger kan bl.a. ske, såfremt videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den, oplysningen angår. Bestemmelsen skal formentlig forstås i snæver forstand. Men til gengæld kan der i så fald også videregives private fortrolige oplysninger om strafbare forhold, politisk observans m.m.

Det vil i denne sammenhæng være væsentligt, at få præciseret, hvilket anvendelsesområde denne videregivelsesmulighed har, da de specielle bemærkninger til bestemmelsen i forslaget til lov om forsvarets efterretningstjeneste ikke forholder sig til dette spørgsmål.

Retspolitisk Forening anbefaler, at lovene om politiets og forsvarets efterretningstjenester ændres, således, at videregivelse af private fortrolige oplysninger uden samtykke til udenlandske myndigheder eller private fysiske eller juridiske personer alene kan som led i et ske internationalt samarbejde om forebyggelse og bekæmpelse af forbrydelser, der er strafbare i Danmark. Oplysninger, der kan indebære en risiko for tortur eller anden umenneskelig behandling, skal dog ikke kunne videregives.

Der har i offentligheden, efter RPF's opfattelse med rette, været fokus på *videregivelse* af såkaldte rådata, der kan indeholde oplysninger om danske statsborgere eller personer, der har lovligt ophold her i landet. Samarbejdet med udenlandske efterretningstjenester rejser en lang række problemer navnlig ved videregivelse af data vedrørende danske fysiske og juridiske personer. (FE)Lovforslagets bemærkninger (pkt. 4.4.3.) anfører herom, at der: " skal være mulighed at der for at videregive rådata, idet videregivelsen samtidig bør bero på en afvejning af behovet for at videregive og de risici, der kan være forbundet hermed. I forbindelse med videregivelse af rådata bør det derfor indgå som en afgørende faktor, om videregivelsen af data ka**n** indebære en risiko for tortur eller anden umenneskelig behandling. "I betragtning af, at der er tale om rådata, der netop er karakteriseret ved at være data, der hverken er erkendte eller behandlet, forekommer bemærkningerne om afgørende vægt på risiko for tortur m.m. i forbindelse med videregivelse at være et usikkert kriterium, da anvendelsen af en sådan faktor forudsætter en databehandling, som ikke finder sted.

Retspolitisk Forening anbefaler, at der i forbindelse med egen videregivelse eller bistand til videregivelse til udenlandske myndigheder eller private fysiske eller juridiske personer indsættes en spærring, således at oplysninger om danske statsborgere og herboende udlændinge med lovligt ophold, alene kan videregives som led i et ske internationalt samarbejde om forebyggelse og bekæmpelse af forbrydelser, der er strafbare i Danmark. Videregivelse af data, der kan indebære en risiko for tortur eller anden umenneskelig behandling, skal dog ikke kunne videregives. Dette indebærer, at trafikdata vedrørende den nævnte gruppe, må analyseres med henblik på at vurdere, hvorvidt videregivelse opfylder de nævnte betingelser.

2. Lov om Center for Cybersikkerhed.

Den nyligt vedtagne lov definerer i modsætning til dens forgænger en sikkerhedshændelse som: " En hændelse, der negativt påvirker *eller vurderes* at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester. "Den oprindelige definition i L 197 (GovCert-loven) (2010-11 1. samling) § 3 lød: *"Sikkerhedshændelse:* Hændelse, der *påvirker* tilgængelighed, integritet eller fortrolighed af information eller tjenester på internettet. "Definitionen er altså betragteligt udvidet til nu også at omfatte *vurderede* hændelser. Centrets virksomhed er som

udgangspunkt ikke omfattet af persondataloven. Offentlighedsloven og forvaltningsloven finder i det væsentligste heller ikke anvendelse.

De data (såvel trafikdata som pakkedata), som centrets netsikkerhedstjeneste kommer i besiddelse af, kan bl.a. behandles når behandlingen vurderes at kunne bidrage væsentligt til Center for Cybersikkerheds muligheder for at sikre informations- og kommunikationsteknologisk infrastruktur, som samfundsvigtige funktioner er afhængige af (§§ 6 nr. 2 og 7 nr.2). *Behandling* af alle typer personoplysninger kan bl.a. finde sted ved begrundet mistanke om en sikkerhedshændelse jf. § 10 nr. 7. Tilsvarende gælder *videregivelse*. Videregivelse til udenlandske samarbejdspartnere kan dog kun finde sted for så vidt angår trafikdata eksempelvis navne, IP-adresser, betalingskorttransaktioner m.m.

Da Center for Cybersikkerhed er henlagt til FE, er der fri udveksling af oplysninger mellem netsikkerhedstjenesten og den øvrige del af efterretningstjenesten.
Retspolitisk Forening skal anbefale, at det overvejes, hvorvidt der er behov for den udvidede definition af en sikkerhedshændelse. Det bør tillige overvejes, hvorvidt der er behov for at undtage centrets virksomhed fra persondataloven og i stedet lade denne lov være gældende med de modifikationer, der følger af netsikkerhedstjenestens behov for effektivitet og samarbejde med danske og udenlandske myndigheder. Endelig forekommer det som et væsentligt spørgsmål, hvorvidt den givne begrundelse for placeringen under FE, synergieffekten, er tilstrækkelig fyldestgørende, når henses til behovet for at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af. Endelig bør det genovervejes, hvorvidt der er behov for de stærkt forlængede sletningsfriste eller, hvorvidt det er tilstrækkeligt at fastholde sletningsfristerne i GovCert-loven fra 2011.

3.Tilsynet.
Tilsynet med såvel forvaltningen af lovene om efterretningstjenesterne og lov om center for cybersikkerhed er henlagt til det nye tilsyn med efterretningstjenesterne, jf. § 16 i lov om Politiets Efterretningstjeneste. Dette tilsyn har kun beskedne beføjelser, og der er ikke nogen transparens i tilsynets virksomhed bortset fra en årlig redegørelse til forsvarsministeren.

Retspolitisk Forening skal anbefale, at tilsynet får mulighed for at give efterretningstjenesterne og Center for Cybersikkerhed pålæg vedrørende behandling af personoplysninger.

Endelig anbefaler foreningen, at der sker en generel kortlægning af omfanget af samarbejdet med udenlandske efterretningstjenester og IT-sikkerhedstjenester, herunder angivelser af omfanget af videregivne personoplysninger, herunder rådata. Kortlægningen skal tillige omfatte Center for Cybersikkerheds virksomhed fra oprettelsen i 2011 til ikrafttrædelsen af den nye lov.

København, den 28. august 2014

Bjørn Elmquist	Leif Hermann
Formand	Bestyrelsesmedlem