Retsudvalget
Folketinget, Christiansborg
1240 København K

IT-Politisk Forening
c/o Niels Elgaard Larsen
Århusgade 35, 1.
2100 København Ø

E-mail : bestyrelsen@itpol.dk
Web : http://www.itpol.dk

Dato : 20. februar 2013

Henvendelse fra IT-Politisk Forening om L 142 (bemærkninger til Justitsministeriets evaluering af sessionslogningen)

IT-Politisk Forening har skrevet et høringssvar om udkastet til lovforslag L 142. I den forbindelse var vi ikke opmærksom på at Justitsministeriet den 21. december 2012 har udarbejdet en redegørelse om diverse spørgsmål vedrørende logningsreglerne (REU alm. del bilag 125, "Notat om overimplementering af logningsdirektivet", også offentliggjort som bilag 2 til L 142). Redegørelsen blev ikke udsendt til høringskredsen den 21. december 2012.

I denne henvendelse til Retsudvalget vil vi gerne fremsende vores bemærkninger til især Justitsministeriets evaluering af sessionslogningen i den nævnte redegørelse.

Sessionslogningen er defineret i § 5 stk. 1 samt § 5 stk. 4-5 i logningsbekendtgørelsen, hvor stk. 4-5 er administrative lempelser af hovedreglen i stk. 1. Sessionslogningen er ikke en del af logningsdirektivet. Teleselskaberne anslår at 90% af de registrerede oplysninger efter logningsbekendtgørelsen kommer fra sessionslogningen.

Eksempler på politiets brug af internetlogning

Ved behandlingen af L 53 i folketingsåret 2011/12 fremlagde Justitsministeriet et notat med 10 eksempler på brugen af data indsamlet efter logningsbekendtgørelsen (Bilag 8 til L 53). Dette notat er oprindeligt udarbejdet til

EU Kommissionen. Ud af de 10 eksempler var 9 telelogning. Kun et eksempel var internetlogning, men internetlogning efter § 5 stk. 2 i logningsbekendtgørelsen, som handler om at spore kilden til en kommunikation (på grundlag af et udefra kommende IP-adresse efterforskningsspor), altså ikke sessionslogningen.

I den nye redegørelse har Justitsministeriet beskrevet tre eksempler på brugen af internetlogning. Det første eksempel i afsnit 5.4.1 er taget fra redegørelsen i L 53 bilag 8. Eksemplerne i afsnit 5.4.2 og 5.4.3 er derimod nye, og skal efter Justitsministeriets opfattelse vise politiets brug af sessionslogningen.

Det er imidlertid kun eksemplet i afsnit 5.4.3 som er sessionslogning efter § 5 stk. 1.

Afsnit 5.4.2 beskriver en sag med væbnede røverier, hvor politiet kunne kortlægge røvernes færden via lokaliseringsoplysninger fra deres mobiltelefon. Justitsministeriet skriver i redegørelsen

> *Sessionsdata indeholder i medfør af logningsbekendtgørelsen geografisk information, og gerningsmandens færden kan dermed kortlægges i videre omfang, end det ville have været muligt ved hjælp af historiske teleoplysninger, da telemasterne kun registrerer trafik, der genereres ved aktiv anvendelse af telefonen. Denne sessionslog-ning har således haft afgørende indflydelse på sagen.*

Den pågældende registrering har imidlertid ikke noget med sessionslogningen i § 5 stk. 1 at gøre. Logningsbekendtgørelsen § 5 stk. 1 kræver logning af IP adresser og portnumre, men der skelnes ikke mellem internettrafik fra faste linjer og mobiltelefoner, og der er ikke noget krav om logning af lokaliseringsdata.

Logningen i den beskrevne sag må være sket efter § 4 stk. 1 nr. 6, hvor lokaliseringsdata (masteoplysninger) skal registreres når der er kommunikation fra/til en mobiltelefon. Det gælder uanset om der er tale om samtaler eller datatrafik. Det er korrekt, som Justitsministeriet påpeger, at smartphones typisk genererer en masse ”automatisk” datatrafik, som fører til

mange flere registreringer af lokaliseringsoplysninger, men det har ikke noget med sessionslogningen i § 5 stk. 1 at gøre. Afsnit 5.4.2 er altså reelt telelogning, hvor politiet har brugt masteoplysninger (svarende til sagerne i afsnit 5.3, hvor politiet har brugt masteoplysninger i mindst halvdelen af sagerne).

Tilbage er sagen i afsnit 5.4.3, som er sessionslogning efter § 5 stk. 1 i logningsbekendtgørelsen. Der er tale om en sag om netbankindbrud for 100.000 kroner, hvor politiet ved hjælp af sessionslogningen har kunnet udelukke en borger fra mistanke. Den konklusion kunne politiet utvivlsomt være kommet til ved anden politimæssig efterforskning.

Under alle omstændigheder er vi i afsnit 5.4.3 meget langt fra terror og alvorlig voldelig kriminalitet. Da politiet selv har udvalgt sagerne til Justitsministeriets redegørelse, må det være rimeligt at konkludere, at der reelt ikke er efterforskningsscenarier i sager om alvorlig kriminalitet, hvor politiet har haft væsentlig nytte af sessionslogningen.

I den kvalitative del af redegørelsen med PET's erfaringer (afsnit 6) er det også telelogningen som fremhæves, mens sessionslogningen i ”meget begrænset omfang” har været inddraget i forbindelse med efterforskningen hos PET.

Justitsministeriets bemærkninger om tekniske udfordringer ved brugen af internetoplysninger

I afsnit 5 i redegørelsen kommer Justitsministeriet med nogle bemærkninger om tekniske udfordringer ved brugen af internetlogningen.

I afsnit 5.5.1.1 synes Justitsministeriet at mene, at det er et problem, at internetudbyderne kan nøjes med at logge hver 500. datapakke der indgår i en slutbrugers kommunikation. Justitsministeriet skriver på side 32-33 i redegørelsen:

> *Problemet med logningen er, at internetudbyderne, jf. bekendtgørelsens § 5, stk. 5, foretager registreringen af internetkommunikation på kanten til andre net i deres netværk, dvs. lige inden deres brugere sendes videre til de modtagende IP-*

adressers servere. Her registrerer de i overensstemmelse med bekendtgørelsens § 5, stk. 4, hver 500. pakke, der passerer serveren, men da datatrafikken på kantserveren er genereret af flere hundrede brugeres internetkommunikation, er det vilkårligt, hvilke brugeres data der logges i hver 500. pakke. På denne måde kan manglende fund af data fra en brugers IP-adresse hverken bruges til at be- eller afkræfte, om den pågældende rent faktisk har været aktiv på internettet i det pågældende tidsrum, og den foretagne logning er hermed som udgangspunkt i praksis uanvendelig i politiets efterforskning, når bortses fra de 'heldige' tilfælde, hvor den pågældende brugers internetkommunikation tilfældigvis er blevet fanget i en logget datapakke.

Der skal ikke ret meget internettrafik til for at generere 500 pakker, hvorefter en pakke statistisk set vil blive registreret efter § 5 stk. 4. I langt de fleste tilfælde vil politiet være "heldig" at der sker en registrering. At der kun registreres oplysninger om hver 500. pakke kan ikke være en reel begrænsning i forhold til at konstatere om en person er "aktiv på internettet".

Vi finder det også nærmest absurd, at Justitsministeriet indirekte ønsker registrering af hver eneste datapakke, hvilket vil føre til skønsmæssigt mindst 400 gange så mange registreringer af borgerne (og i øvrigt være teknisk umuligt for internetudbyderne), og i samme redegørelse beskriver politiets IT-mæssige problemer med at håndtere de nuværende datamængder (afsnit 5.5.2).

Bemærkningerne i afsnit 5.5.1.2 i redegørelsen må handle om sporing af kilden til en kommunikation, altså § 5 stk. 2 i logningsbekendtgørelsen, selv om Justitsministeriet prøver at blande sessionslogningen ind i billedet. Det problem som beskrives øverst på side 34 må være carrier-grade NAT, hvor flere kunder deler en offentlig IP adresse (typisk fordi der er mangel på IPv4 adresser). Hvis politiet i en ekstern serverlog finder en IP adresse, kan denne ikke nødvendigvis spores til en enkelt internetkunde, hvis internetudbyderen anvender carrier-grade NAT.

Logningsdirektivets artikel 5 stiller i øvrigt alene krav om registrering af den tildelte IP adresse. Der er ikke i

direktivet noget krav om portregistrering eller sessionsregistrering.

IT-Politisk Forenings konklusion

Vi vil afslutningsvist fremhæve denne bemærkning i Justitsministeriets redegørelse

> *Implementeringen af logningen blev imidlertid gennemført på en sådan måde, at den stort set blev uanvendelig, hvilket stod klart for politiet, da man første gang ønskede at gøre brug af sessionslogning i forbindelse med efterforskningen af en straffesag.*

De danske internetudbydere har implementeret sessionslogningen efter kravene i bekendtgørelsen, og den valgte implementering er udtryk for hvad der er teknisk muligt. Med stigningen i trafikmængderne er det ikke blevet nemmere at lave sessionslogning i 2013 sammenlignet med 2006. Samtidig er det på ingen måde klart at Justitsministeriets ikke nærmere beskrevne ”idealer” om sessionslogningen ville have gjort nogen forskel, jævnfør vores kommentarer ovenfor.

Efter at have lavet en evaluering af sessionslogningen, som den med rimelighed kan implementeres i praksis, er Justitsministeriet altså kommet til den konklusion, at den er ”stort set uanvendelig for politiet”. Efter fem års sessionslogning, med en anslået udgift på et par hundrede millioner kroner, kan politiet kun fremkomme med et enkelt eksempel hvor sessionslogningen har spillet en vis rolle (sagen med netbankindbrud).

Den eneste logiske konsekvens af denne evaluering må være at afskaffe sessionslogningen, som IT-Politisk Forening har anbefalet i vores høringssvar.