JUSTITSMINISTERIET
Politi- og Strafferetsafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 18. marts 2016
Kontor: Sikkerhedskontoret
Sagsbeh: Niels Dam Dengsøe Petersen
Sagsnr.: 2016-0030-4236
Dok.: 1892993

Hermed sendes besvarelse af spørgsmål nr. 325 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 26. februar 2016. Spørgsmålet er stillet efter ønske fra Pernille Skipper (EL).

Søren Pind

/

Lars Solskov Lind

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 325 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren redegøre for, jf. Rigspolitichefens udtalelser til medierne, hvordan den foreslåede sessionslogning adskiller sig fra den tidligere, og hvorfor den dermed ifølge rigspolitiet skulle blive mere effektiv?”

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Rigspolitiet, der har oplyst følgende:

> ”Rigspolitiet kan indledningsvis oplyse, at sessionslogning er et begreb, der dækker over registrering og opbevaring af oplysninger om internettrafik, dvs. oplysninger om kommunikationsspor. Det omfatter navnlig oplysninger om, hvilken IP-adresse der kommunikerede med hvilken IP-adresse, samt hvor og hvornår denne kommunikation fandt sted. Sessionslogning indeholder ikke oplysninger om selve kommunikationsindholdet, som f.eks. indholdet på en hjemmeside, som besøges.
>
> Reglerne om logning findes i bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen). Ved bekendtgørelse nr. 660 af 19. juni 2014 ophævede Justitsministeriet reglerne om sessionslogning. De øvrige regler i logningsbekendtgørelsen er fortsat gældende.
>
> Ophævelsen af reglerne om sessionslogning i 2014 skal ses i lyset af, at det i praksis havde vist sig at være svært for politiet at anvende de data, som udbyderne som led i sessionslogningen gemte vedrørende internettrafik, ligesom oplysninger fra sessionslogning kun blev anvendt af politiet i begrænset omfang.
>
> Dette skyldtes navnlig, at mange udbydere havde implementeret logningsbekendtgørelsens bestemmelser om logning af internettrafik således, at de gemte data ikke kunne identificere datatrafikken for én bestemt slutbruger. Logningen blev reelt gennemført som stikprøver, og det var således helt tilfældigt, om de loggede data indeholdt oplysninger vedrørende en bestemt slutbruger, som var af interesse for politiet.
>
> Hvis der ikke var logget nogen oplysninger om en mistænkt, kunne det godt betyde, at den pågældende ikke havde haft

nogen kommunikation. Men det kunne også betyde, at der – fordi der alene var tale om stikprøver – ved et tilfælde ikke var blevet logget nogen oplysninger om kommunikationen.

Nogle udbydere havde implementeret logningsbekendtgørelsens regler om sessionslogning på en måde, som bedre understøttede politiets ønsker om at kunne identificere kommunikation fra en bestemt slutbruger, og i disse tilfælde kunne politiet bruge informationen efterforskningsmæssigt.

Samlet set betød dette, at de daværende regler om sessionslogning kun var af begrænset nytte for politiet, og at nytteværdien for politiet i høj grad var afhængig af, hvilken udbyder, der havde gennemført logningen.

Problemerne med den tekniske udformning af den daværende ordning ændrer imidlertid ikke på, at sessionslogning vil være et særdeles vigtigt redskab for politiet, hvis ordningen bliver udformet på en måde, der understøtter politiets behov.

Efter Rigspolitiets opfattelse er vigtigheden af at have en velfungerende ordning til logning af internettrafik endvidere stigende.

Der er to hovedårsager hertil. For det første ændrer kriminalitetsbilledet sig i disse år i takt med den teknologiske udvikling i samfundet, således at den traditionelle kriminalitet falder, mens kriminaliteten på nettet stiger.

Stigningen sker både inden for netbedragerier og misbrug af betalingskort og for de mere avancerede og komplicerede kriminalitetstyper som hacking. Der kan i den forbindelse henvises til Rigspolitiets Strategiske Analyse 2015, side 67-74 (www.politi.dk/da/ompolitiet/virksomhedenpolitiet/strategisk_analyse_2015/).

I sådanne sager er politiets efterforskningsmuligheder helt afhængig af, at der kan findes spor af den datakommunikation, som har været et led i udførelsen af forbrydelsen.

Mens et indbrud i et hus eller en anden "traditionel" forbrydelse vil efterlade en lang række fysiske spor i form af fingeraftryk, DNA, måske videomateriale og udsagn fra vidner, som har været i nabolaget, så efterlader et hacking-angreb eller digital deling af børneporno alene digitale spor. Lagres disse spor ikke, er politiet reelt nærmest uden efterforskningsmuligheder.

Den anden hovedårsag til, at det bliver mere og mere vigtigt for politiet at have en velfungerende logningsordning er, at den

grundlæggende tænkning bag de nuværende logningsregler efter Rigspolitiets opfattelse udfordres af en parallel teknologisk udvikling, som vanskeliggør politiets efterforskning af enhver form for kriminalitet, herunder også den "traditionelle" som f.eks. narkokriminalitet, sædelighedsforbrydelser, terror mv.

Efter de nuværende logningsregler lagres der således oplysninger om traditionel telefoni mellem fastnettelefoner eller mobiltelefoner. Reglerne er indført for at give politiet mulighed for – efter forelæggelse for en dommer – at få historiske oplysninger om, hvilke telefonnumre, som har kommunikeret med hinanden, og dette har traditionelt været et særdeles vigtigt efterforskningsværktøj inden for en lang række af de mere alvorlige kriminalitetsformer.

Med udbredelsen af smartphones og kommunikation mellem computere, f.eks. ved brug af Skype, flyttes kommunikation imidlertid i stigende grad fra traditionel telefoni – som er omfattet af logningsforpligtelsen – til internetbaseret kommunikation, som i dag ikke er omfattet af logningen.

Dette betyder, at også de efterforskningsmuligheder, som den nuværende logningsbekendtgørelse har til formål at give politiet, løbende udhules. Inden for en kortere årrække må det således forventes, at reglerne om logning af telefoni i den nuværende udformning vil være af særdeles begrænset værdi for politiet.

Samlet set vil den beskrevne udvikling i væsentlig grad forringe politiets muligheder for at efterforske kriminalitet, og på denne baggrund har Rigspolitiet anbefalet Justitsministeriet at genindføre regler om logning af internettrafik i en form, hvor logningen reelt vil være anvendelig i indsatsen med efterforskning og strafforfølgning af strafbare forhold.

Rent praktisk vil dette efter Rigspolitiets opfattelse kunne ske ved, at det i logningsbekendtgørelsen bestemmes, at opsamlingen af oplysningerne skal kunne knyttes til en bestemt slutbruger (IP-adresse). Det var som nævnt ovenfor et af hovedproblemerne ved den tidligere gældende ordning, at dette kun i et vist omfang var muligt.

Konkret foreslår Rigspolitiet, at der for hver enkelt datasession for hver slutbruger opsamles en række oplysninger på udbyderens net om internettrafikken, herunder navnlig afsendende og modtagende IP-adresse samt tidspunkt og lokation.

De opsamlede oplysninger ville f.eks. kunne se sådan ud:

Afsender IP	**Modtager IP**	**Transport-protokol**	**Afsendende Portnummer**	**Modtagende Portnummer**	**Volumen (bytes)**	**Tidspunkt start**	**Tidspunkt slut**
6.6.6.6	1.2.3.4	TCP	13423	22	2003232	7/3-2016, 12:24:23.433	7/3-2016, 12:54:51.231
1.2.3.4	5.6.7.8	TCP	63423	80	1924823	7/3-2016, 12:25:23.823	7/3-2016, 12:54:37.251
6.6.6.6	1.2.3.4	TCP	3431	22	4883290	9/3-2016, 15:34:38.329	9/3-2016, 16:27:23.834

Pålægges teleudbyderne at opbevare disse oplysninger, vil logningen efter Rigspolitiets opfattelse være et særdeles vigtigt værktøj til brug for politiets efterforskning og strafforfølgning af ikke kun it-kriminalitet eller it-faciliteret kriminalitet, men også mere traditionelle forbrydelser som f.eks. terror, drab, røveri, voldtægt og brandstiftelse.

Som det fremgår af skemaet ovenfor, foreslår Rigspolitiet ikke, at der som led i sessionslogningen lagres oplysninger om indholdet af kommunikationen, men alene oplysningerne om, hvilke IP-adresser, der har været i kontakt med hinanden på hvilke tidspunkter og under anvendelse af hvilke tekniske protokoller og porte.

De blotte oplysninger herom vil imidlertid – lige som de oplysninger om, hvilke telefonnumre der har været i kontakt med hinanden, som lagres efter de "klassiske" logningsregler – være særdeles vigtige oplysninger i en lang række efterforskninger og efter Rigspolitiets opfattelse udgøre et meget effektivt efterforskningsredskab.

Afslutningsvis bemærkes, at Rigspolitiet – ud over de ovenfor beskrevne regler om sessionslogning – har foreslået, at teleudbyderne pålægges at opbevare såkaldte lokationsdata i form af oplysninger om, hvilke mobilmaster der bruges til kommunikationen. En sådan pligt findes i dag i relation til traditionelle opkald og sms-beskeder på mobiltelefoner, men ikke i relation til internetkommunikation.

> Lokationsdata er særdeles anvendelige i efterforskningen af en lang række forskellige forbrydelser, og en modernisering af reglerne, således at de ikke kun omfatter traditionel kommunikation til og fra mobiltelefoner, men også internetbaseret kommunikation, vil indebære en styrkelse af politiets efterforskningsmuligheder."

Justitsministeriet kan endvidere oplyse, at Justitsministeriet har afholdt møder med en række store udbydere og interesseorganisationer inden for tele- og internetbranchen. På møderne er der blevet etableret en nyttig og konstruktiv dialog om udformningen af fremtidens logningsregler.

På den baggrund finder Justitsministeriet, at den gode dialog med udbyderne bør fortsætte, således at en ny model både i tilstrækkelig grad tilgodeser politiets behov, og samtidig ikke pålægger udbyderne uacceptable økonomiske byrder.