JUSTITSMINISTERIET
Politi- og Strafferetsafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 18. marts 2016
Kontor: Sikkerhedskontoret
Sagsbeh: Niels Dam Dengsøe Petersen
Sagsnr.: 2016-0030-4244
Dok.: 1893057

Hermed sendes besvarelse af spørgsmål nr. 333 (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. 333 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren redegøre for, om sessionslogning - i den nye og gamle udgave - er anvendelig, hvis der bruges eksempelvis VPN, satellitforbindelse, XMPP eller ZRTP?”

Svar:

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

> ”Rigspolitiet kan oplyse, at man i forbindelse med sessionslogning efter såvel de tidligere regler som den af Rigspolitiet foreslåede ordning, jf. herved Rigspolitiets samtidige bidrag til besvarelsen af spørgsmål 325 (Alm. del) til Retsudvalget, i princippet kan opstille to forskellige hovedkategorier:
>
> 1. Kommunikation direkte mellem slutbrugerne. Til denne kategori hører i en vis udstrækning f.eks. Skype, Facetime og WhatsApp. Oplysninger om disse slutbrugeres IP-adresser mv. vil i sig selv kunne være værdifulde for efterforskningen.
>
> 2. Kommunikation fra slutbruger A til en server og derfra (eventuelt igennem et netværk af servere) til slutbruger B. Til denne kategori hører bl.a. VPN-forbindelser samt TOR-netværket.
>
>   I forhold til kategori 2 afhænger anvendeligheden af sessionslogning af flere faktorer. Der vil således være forskel på, om det er en kendt aktør, som kontrollerer leddene mellem slutbruger A og slutbruger B, ligesom der vil være forskel afhængigt af, om denne aktør er indstillet på at efterkomme en retskendelse. Der vil ligeledes være forskel på, om de servere, som trafikken ledes igennem, er placeret i Danmark eller i udlandet.
>
>   Loggede oplysninger vil imidlertid i alle tilfælde – men i varierende omfang – kunne være af værdi i forbindelse med en efterforskning, også i de situationer, hvor det ikke er muligt for politiet at identificere slutbruger B.
>
>   I disse situationer vil de loggede oplysninger kunne danne grundlag for politiets videre tilrettelæggelse af efterforskningen, herunder til brug for beslutning om eventuel brug af mere målrettede efterforskningsmetoder.
>
>   I forhold til de i spørgsmålet nævnte teknologier kan det mere specifikt oplyses, at der også fastholdes oplysninger om efterladte kommunikationsspor ved brug af VPN-forbindelser. Dis-

se oplysninger kan som ovenfor nævnt i varierende grad være anvendelige i forhold til politiets efterforskning.

XMPP (Extensible Messaging and Presence Protocol) er en efterhånden mindre anvendt protokol for kommunikationstjenester på internettet. Kommunikation via en sådan tjeneste vil falde ind under kategori 2, og anvendeligheden af loggede oplysninger vil være afhængig af dels den konkrete implementering af protokollen, dels af hvem der udbyder den specifikke kommunikationstjeneste.

Satellitforbindelser adskiller sig ikke fra anden kommunikation over internettet på en måde, som er relevant for sessionslogning. Kommunikation i kategori 1 vil f.eks. stadigvæk være i kategori 1, selvom den underliggende kommunikationsteknologi er en satellitopkobling.

ZRTP (Zimmermann Real-time Transport Protocol) er en protokol til kodeudveksling, dvs. at den alene er relevant for indholdet af kommunikationen og ikke for kommunikationssporene. Rigspolitiets forslag om at indføre sessionslogning vedrører alene kommunikationssporene og ikke indholdet af kommunikationen, og brugen af ZRTP har derfor ikke betydning for anvendeligheden af sessionslogning."