JUSTITSMINISTERIET

Folketinget
Europaudvalget
Christiansborg
1240 København K
DK Danmark

Dato: 10. oktober 2023
Kontor: Politikontoret
Sagsbeh: Emil Lykke Gregersen
Sagsnr.: 2023-06585
Dok.: 2999855

Besvarelse af spørgsmål nr. 2 til KOM (2022) 0209 fra Folketingets Europaudvalg

Hermed sendes besvarelse af spørgsmål nr. 2 til KOM (2022) 0209, som Folketingets Europaudvalg har stillet til justitsministeren den 26. september 2023. Spørgsmålet er stillet efter ønske fra Alex Ahrendtsen (DF).

Peter Hummelgaard

/

Maria Carlsson

Slotsholmsgade 10
1216 København K.

T +45 7226 8400

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 2 til KOM (2022) 0209:

> ”I forlængelse af drøftelsen på mødet i Europaudvalget den 15. september 2023 bedes ministeren uddybe, hvordan regeringen på den ene side vil sikre, at online-tjenesteudbydere effektivt kan anvende ”end to end”-kryptering, samtidig med at "end to end"-kryptering skal være omfattet af den kommende forordning og dermed af et muligt opsporingspåbud. Herunder bedes ministeren svare på, om dette ikke vil nødvendiggøre såkaldte bagdøre i krypteringen, der netop strider imod selve idéen med ”end to end”-kryptering.”

Svar:

Kommissionen har med forslaget til forordning om regler til forebyggelse og bekæmpelse af seksuelt misbrug af børn lagt op til et teknologineutralt og fremtidssikret regelsæt, der ikke på forhånd udelukker bestemte teknologier. Forslagets anvendelsesområde omfatter således ”end-to-end”-kryptering, som er en krypteringsteknologi, der krypterer data, således at kun afsender og modtager kan læse dem.

Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) og Det Europæiske Databeskyttelsesråd (EDPB) har i forbindelse med fremsættelsen af forordningsforslaget afgivet fælles udtalelse nr. 04/2022 af 28. juli 2022. Der bliver i udtalelsen bl.a. rejst bekymring om forslagets indvirkning på mulighederne for at opretholde ”end-to-end”kryptering. Det fremgår bl.a. af udtalelsen, at der med forslaget skal sikres en balance mellem samfundets behov for at have sikre og private kommunikationskanaler og bekæmpelsen af misbrug heraf. Med henblik på at præcisere, at der med forordningen ikke lægges op til at umuliggøre ”end-to-end”-kryptering, foreslås det af EDPS og EDPB, at det udtrykkeligt fremgår af forslaget, at intet i forordningen skal fortolkes som et forbud mod eller en svækkelse af kryptering.

Fra dansk side har det været en vigtig prioritet, at ”end-to-end”-kryptering ikke udelukkes fra forslagets anvendelsesområdet. Det skyldes, at en udelukkelse af bestemte teknologier, herunder ”end-to-end”-kryptering, vil kunne udhule forslagets formål, da gerningspersoner i givet fald vil kunne skjule sig bag krypterede tjenester. Dette skal også ses i lyset af, at det er Rigspolitiets erfaring, at seksuelt misbrug af børn online ofte foregår via tjenester, som netop benytter sig af ”end-to-end”-kryptering.

Regeringen anerkender den væsentlige sikkerhedsforanstaltning, som "end-to-end"-kryptering udgør for at beskytte privat kommunikation og personoplysninger mod uautoriseret adgang og misbrug. Med henblik på at sikre, at muligheden for at benytte sig af "end-to-end"-kryptering ikke svækkes, arbejder regeringen sammen med en række medlemslande for, at det – som foreslået af EDPS og EDPB – udtrykkeligt fremgår af forordningsteksten, at intet i forordningen kan fortolkes sådan, at forordningen forbyder, kræver deaktivering af eller umuliggør "end-to-end"-kryptering, eller skal forstås som et incitament til eller en hindring for at bruge bestemte teknologier.

Efter forordningsforslaget kan en udbyder af en "end-to-end"-krypteret tjeneste, der skal efterkomme et opsporingspåbud, frit vælge, hvordan opsporingen foretages, herunder hvilken teknologi udbyderen ønsker at benytte sig af. Der gælder efter forslaget alene krav om, at teknologierne bl.a. på effektiv vis skal være i stand til at påvise "kendt" eller "ukendt" materiale eller forsøg på kontakt med børn. Forordningsforslaget pålægger således ikke udbydere at benytte sig af bestemte teknologier eller andet opsporingsværktøj, som vil kunne svække IT-sikkerheden.