

Yttrande över Utkast till lagrådsremiss: Datalagring och tillgång till elektronisk information Ju2024/02286

Södertörns tingsrätt har granskat utkastet utifrån de intressen som tingsrätten har att beakta. Tingsrätten har följande synpunkter.

Anpassningsskyldighet för allmänt tillgängliga NOIK

I tingsrättens yttrande 2023-10-26 (dnr TSN 2023-208) över utredningens slutbetänkande framhölls att en potentiell konsekvens av att införa en anpassningsskyldighet för allmänt tillgängliga NOIK är en försvagad totalsträckekryptering. Tingsrätten har även efterfrågat närmare överväganden kring detta i det fortsatta lagstiftningsarbetet.

En totalsträckekryptering är per definition inte åtkomlig för leverantören. Efter att ha tagit del av utkastet är det för tingsrätten oklart hur tillhandahållare av NOIK ska kunna uppfylla anpassningsskyldigheten utan att bygga in sådana bakdörrar som försämrar eller omöjliggör totalsträckekryptering. I utkastet sägs samtidigt att det är av vikt att totalsträckskrypterade tjänster alltjämt kan användas (s. 88 i utkastet). Det är en otillfredsställande lösning att denna centrala och principiella frågeställningen enligt utkastet ”i slutändan [blir] en fråga för rättstillämpningen och praxis att avgöra” (s. 88 i utkastet).

Det är oklart vad en anpassningsskyldighet som medför att HAK kan verkställas i förhållande till NOIK mer konkret innebär. Utredningen har funnit att anpassningsskyldigheten innebär en skyldighet för tillhandahållare av allmänt tillgängliga NOIK att tillhandahålla meddelanden i läsbar form. En frågeställning som inte behandlas i utkastet är om tillhandahållarna av kommunikationstjänsterna bör ha en skyldighet att förhindra en förmedling av meddelanden som krypterats genom en tredjepartsapplikation och som tillhandahållaren inte kan få tillgång till i klartext (jfr resonemanget i SOU 2023:22 s. 412 ff.). Om så skulle vara fallet innebär detta en betydande inskränkning i allmänhetens möjlighet till säker elektronisk kommunikation eftersom det i praktiken innebär ett förbud mot krypterad kommunikation. Om i stället motsatsen skulle vara fallet riskerar den föreslagna reformen att bli verkningslös eftersom den lätt kan kringgå. Saken bör beröras i den fortsatta beredningen.

Som påpekas i konsekvensanalysen (avsnitt 10.1) innebär förslaget en risk för den personliga integriteten, för svenska företag och organisationer, samt för att tillhandahållare helt slutar verka i Sverige. Vidare kan det ifrågasättas

om efterlevnaden av en eventuell anpassningsskyldighet genom sanktionsförelägganden är effektiv. Legitima globala aktörer kan dra sig ur den svenska marknaden, medan oseriösa aktörer i tredje land kan avstå från att följa skyldigheten med begränsade risker. Risker att tillhandahållare underlåter att följa en stats krav på att avslöja användares hemliga elektroniska kommunikation är ur ett globalt perspektiv inte en ny fråga. Många länder, t.ex. Kina och Iran, har valt olika blockeringsmetoder för att förhindra sina medborgares krypterade kommunikation som sker genom tillhandahållare som inte är åtkomliga för ländernas rättsskipning. Det är svårt att förstå hur Sverige med t.ex. rättslig hjälp skulle lyckas bättre än andra länder. I utkastet anges att risken för att reglerna inte efterlevs av tillhandahållare inte utgör ett tillräckligt starkt skäl för att avstå från att genomföra förslaget (s. 78 i utkastet). Förslaget, så som det nu är utformat, riskerar alltså att generellt minska säkerheten i kommunikationen för legitima intressen utan att uppnå eftersträvad brottsbekämpande effekt. Det kan därför ifrågasättas om förslaget uppfyller proportionalitetsprincipen.

I handläggningen av ärendet har chefsrådmannen Anders Larsson, rådmannen Michael Mackiewicz och tingsfiskalen Philip Stålhandske, föredragande, deltagit.

Anders Larsson

Philip Stålhandske