Finansdepartementet, fi.remissvar@regeringskansliet.se

Kopia till fi.ofa.dis.remisser@regeringskansliet.se

Stockholm den 3 februari 2026

Remissvar över promemorian Nya regler mot bedrägerier och annat vilseledande genom elektroniska kommunikationer (Fi2025/02192)

Hi3G Access AB (Tre) får lämna följande synpunkter i rubricerat ärende, fortsättningsvis kallat Förslaget. Synpunkterna ansluter till det av TechSverige ingivna remissvaret men utvecklar några av synpunkterna däri, i avsnittet kallat ”Tydlig ansvarsfördelning och rättssäkra ramar i den digitala infrastrukturen”.

Av Förslaget framgår att: ”*Den tillhandahållare som omfattas av skyldigheten behöver kontrollera om den information som den har tillgång till ger anledning att anta att ett elektroniskt meddelande överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare. Valet av uttrycket har anledning att anta innebär att kravet ställs relativt lågt. Det ska dock finnas konkreta omständigheter som indikerar att meddelandet överförs som ett led i ett bedrägeri eller annat vilseledande. En sådan kontroll kan som utgångspunkt ske med automatiserade medel. Kontrollen måste vara förenlig med reglerna om behandling av trafikuppgifter och integritetsskydd i 9 kap. LEK.”*

Tre anser att det krävs en betydligt högre grad av konkretion avseende vilka faktiska omständigheter i en operatörs verksamhet som innebär att ett elektroniskt meddelande överförs för att bedra eller vilseleda en vidare krets av mottagare än vad som framgår av Förslaget, innan en skyldighet att i realtid stoppa elektroniska meddelanden kan införas.

Vilka elektroniska meddelanden kan stoppas baserat på trafikuppgifter?

Som framgår av Förslaget ska elektroniska meddelanden blockeras redan vid en misstanke om (försök till) bedrägeri, samtidigt som blockeringen ska ske utan kontroll av innehållet i meddelandet. Tre kan inte se att det går att stoppa vissa typer av bedrägerier utan någon form av kontroll av innehållet. Detta gäller bl.a. avseende Förslagets exempel om spridning av desinformation, vilseledande budskap och utskick av sms innehållande falska länkar. Med andra ord är det mycket svårt eller t.o.m. omöjligt att genom trafikanalys, mönsterigenkänning och kontroll av metadata förstå att det troligtvis rör sig om ett brott i dessa fall.

En utbredd åtgärd som kan användas för att stoppa t.ex. utskick av sms innehållande skadliga länkar är blockerande filter. Som framgår av PTS rapport[1] efterfrågas både i Sverige och andra EU-länder tydligare regler kring vad som är tillåtet för filtrering och skanning av innehåll i meddelanden. I några EU-länder har sådana möjligheter införts.[2] Tre anser att det behöver klargöras hur Förslaget förhåller sig till denna åtgärd.

När det gäller t.ex. wangiri-samtal och blockering av Sender-ID går det däremot normalt att analysera ovan nämnda risker genom mönster och trafikanalys. Även åtgärden att blockera spoofade samtal, dvs. samtal via nationella nummer som kommer in via ett internationellt gränssnitt, är ett sådant exempel. Blockeringen kräver inte några subjektiva bedömningar eller indikationer om bedrägeri utan samtal via nationella nummer ska som utgångspunkt inte komma från utlandet.

Vidare har branschen tagit fram en åtgärd för rapportering av bluff-sms (7726), som bygger på att användarna själva rapporterar in t.ex. misstänkta bedrägerier.

Sammanfattningsvis måste Förslaget, om det ska kunna genomföras, vara begränsat till situationer där avsändarens avsikt att bedra eller vilseleda en vidare krets av mottagare tydligt kan slutledas baseras enbart på trafikuppgifter och trafikmönster. Det är i dagsläget möjligt avseende framförallt wangiri-samtal, spoofade samtal och vid en användning av meddelanden med Sender-ID.

Tre tillstyrker därför också lagförslaget att PTS ska få föra ett samlat register över uppgifter om avsändarnamn (alfanumeriska nummer eller Sender-ID) för sms-meddelanden för s.k. Application2Person (A2P) men anser att registrering ska bygga på frivillighet, såsom tidigare föreslagits av PTS[3].

Nödvändigt med kompletterande föreskrifter

Enligt Förslaget (4 kap. 12 § LEK) ges PTS mandat att meddela föreskrifter om skyldighetens omfattning. Som Tre ser det innebär Förslaget att föreskrifter är en nödvändighet och bemyndigandet för PTS bör således göras obligatoriskt.

Föreskrifterna bör utgå från vissa specifika problemsituationer, såsom dem som angivits ovan. Föreskrifterna om spoofade samtal kan nämnas som ett fungerande exempel. Blockerings-åtgärden arbetades fram under en längre tid, inom ramen för ett samarbete mellan operatörerna och PTS. Kraven på operatörerna var också inledningsvis en vägledning, men blev senare föreskrifter. I praktiken fungerar blockeringsåtgärden avseende mobilsamtal tack vare en teknisk lösning som några av operatörerna finansierat och upprättat och som alla berörda operatörer kan ansluta sig till.

[1] PTS-ER 2024:31 s. 35.
[2] A. a. s. 37.
[3] A. a. s. 9.

Ovan nämnda tydlighet krävs för att inte legitima elektroniska meddelanden ska stoppas, p.g.a. en rädsla hos operatörerna att göra fel och träffas av sanktioner. Tre anser det vidare viktigt att tillämpningen av lagstiftningen blir enhetlig mellan operatörerna; så att användarna ges samma grundskydd oberoende av operatör och inte skillnader i tillämpningar mellan operatörerna utnyttjas av bedragare. Dessutom riskerar skillnader i trafikanalyser m.m. kopplat till säkerhetsarbetet att straffa dem som håller en hög säkerhetsnivå. Även om operatörernas förutsättningar, skillnader i tjänsteutbud och tekniska miljö skiljer sig åt bör därför en enhetlig tillämpning eftersträvas.