Finansdepartementet
fi.remissvar@regeringskansliet.se
fi.ofa.dis.remisser@regeringskansliet.se

Stockholm den 26 januari 2026

Telenor Sverige AB:s svar i remiss av promemoria Nya regler mot bedrägerier och annat vilseledande genom elektroniska kommunikationer, Fi2025/02192

Telenor Sverige AB instämmer i den grundläggande bedömningen att det är nödvändigt att agera för att minska antalet bedrägerier och annan brottslig verksamhet riktat mot användare av elektroniska kommunikationer. Telenor har dock invändningar mot det förslag som presenteras i promemorian och menar att förslaget inte utan vidare analys och komplettering bör omsättas i lag.

De åtgärder som introduceras måste inte bara vara tydliga och effektiva, utan måste också vara proportionerliga. Proportionaliteten ska bl.a. bedömas utifrån vad som är rimligt att kräva av olika aktörer i värdekedjan. När det gäller bedrägerier och annan brottslighet som riktas mot användare av elektroniska kommunikationstjänster ska det framhållas att dessa kan begås genom tekniska metoder som är eller bör vara otillåtna. Här finner vi brott mot nummer- och adresseringsregler, såsom manipulering av a-nummer eller sändaridentiteter. Sådana metoder kan hindras genom teknisk analys och blockering eller filtrering, såsom nuvarande blockering av samtal som inkommer från utlandet med svenskt a-nummer (PTS anti-spoofingföreskrifter).

Men bedrägerier och annan brottslig verksamhet kan också ske genom legitimt bruk av elektroniska kommunikationer där det är själva innehållet eller uppsåtet som är brottsligt. För att i realtid hindra sådant olagligt innehåll att komma fram krävs en stor tydlighet kring vad som ska blockeras, hur det ska gå till och vem som ansvarar för vad.

Operatörer av elektronisk kommunikation ska enligt gällande regelverk inte övervaka eller analysera trafiken för andra syften än att tjänsten ska fungera och för fakturering och avräkning. Operatören ska inte avkrävas något ansvar för det innehåll som dess kunder skickar eller tar emot (s.k. mere conduit). Filtrering eller blockering får endast ske om det finns en tydlig laglig grund, t.ex. efter beslut av domstol eller behörig myndighet.

Promemorians förslag utmanar i vissa delar dessa grundläggande principer, som finns fastslagna i regelverk som endast i mycket begränsad utsträckning medger undantag, inbegripet e-Dataskyddsdirektivet, e-Handelsdirektivet och Förordningen om digitala tjänster (DSA).

Det är viktigt att det råder stor tydlighet kring vilka förfaranden som ska anses bedrägliga eller som av annan anledning ska hindras från att nå fram. Även om det är tydligt vilka förfaranden som är bedrägliga så uppkommer dock även frågan om vilken grad av misstanke som ska krävas för att kommunikationen ska blockeras.

Promemorian talar om att det ska finnas ”anledning att anta” vilket får förstås som att det långt ifrån är säkerställt att ett brottsligt förfarande är för handen. Sannolikheten blir med nödvändighet olika stor beroende på omständigheterna i varje enskilt fall och det förefaller som svårt eller omöjligt för tillhandahållarens att göra denna bedömning på tillräckligt säkra grunder i varje fall. Givet att bedömningen behöver göras i realtid dygnet runt årets alla dagar kommer det inte vara möjligt med enskilda bedömningar, utan blockeringsbeslutet måste i stället vila på automatisering som utgår från på förhand uppställda generella regler.

Det får inte läggas på tillhandahållaren av nummerbaserade kommunikationstjänster att ställa upp dessa regler. Om förslaget ska bli verklighet måste det genom föreskrifter och vägledning framgå exakt vilka kriterier som ska vara uppfyllda. Att endast hänvisa till att operatören har ”anledning att anta” är otillfredsställande, då operatören inte har möjlighet att bilda sig någon uppfattning i de enskilda fallen. Risken för att legitim kommunikation hindras är vidare stor vid automatiserad blockering som baseras på generella regler. Enligt Telenors mening har dessa aspekter inte analyserats i tillräcklig utsträckning, särskilt vad gäller trafikfallet samtal. Att i realtid blockera ett inkommande samtal för att förhindra brottsligt innehåll eller uppsåt, utan att riskera att legitima samtal blockeras, torde i praktiken vara så svårt att det inte framstår som proportionerligt att kräva.

I promemorian sägs att blockeringen bör utformas på ett sätt som minimerar risken för att andra än de avsedda elektroniska meddelanden blockeras, samtidigt som att kravet på att omständigheterna ska tala för att det rör sig om sådana förhållanden inte får vara så högt ställt att skyldigheten förlorar sitt syfte. Det sägs inget om hur detta ska åstadkommas, vilket gör att det inte heller går att göra den nödvändiga proportionalitetsavvägningen. Promemorian resonerar kring att det kan uppstå ”avvikande trafikmönster i tillhandahållarens system” utan att gå närmare in på vilka system som avses eller vilka volymer eller andra kännetecken som ska anses avvikande. Det överlämnas till operatören själv att ta ställning till.

Promemorian påstår vidare att kravet inte innebär en skyldighet att övervaka samtliga elektroniska meddelanden som tillhandahållaren överför. Däremot behöver tillhandahållaren införa rutiner för att regelbundet kontrollera om det finns omständigheter som aktualiserar skyldigheten. Återigen anges endast ”avvikande trafikmönster” som en grund för att operatören ska ha anledning att anta att innehållet utgör bedrägeri eller vilseledande. Det finns ingen beskrivning av hur detta ska kunna ske i realtid för inkommande samtal, men det framhålls att endast den omständigheten att det rings upprepade samtal inte ska leda till ett antagande om att samtalet är bedrägligt eller missledande. Det ges däremot inget exempel på en omständighet som bör leda till sådant antagande. Ändå krävs att operatörerna inrättar sin verksamhet för att kunna blockera samtalen utifrån den information som finns tillgänglig och att införa lämpliga kontrollåtgärder. Enligt Telenors mening bygger kravställningen på alltför lösa grunder för att kunna omsättas i lagstiftning. Vad Telenor känner till har promemorians förslag tagits fram utan samråd eller kontakter med berörda tillhandahållare, vilket är en brist i sig.

Promemorian anger att det för att upptäcka avvikande trafikmönster kan behöva behandlas uppgifter som visar att ett visst telefonnummer genomför ett stort antal misslyckade uppringningar eller samtal med mycket kort varaktighet under en kort tid. Men det anges inte om ett sådan mönster är tillräckligt för att det ska finnas anledning att anta att samtalet är bedrägligt eller missvisande. Det anges också att uppgifter om ett samtals geografiska ursprung, varaktighet och antal kan ge anledning att anta att samtalet utgör ett wangirisamtal. Men det resoneras inte kring möjligheten att detta mönster även kan finnas för legitima samtalsförsök. Även om ett stort antal upprepade samtalsförsök skapar misstankar så är det en utmaning att i realtid sätta gränser. Hur många upprepningar krävs innan blockeringen verkställs?

När det gäller SMS finns enligt Telenors mening ett större utrymme för realtidsanalys av avvikelser än när det gäller inkommande samtal. Abonnenter har möjlighet att uppmärksamma sin operatör på misstänkta bedrägerier genom att vidarebefordra meddelandet till 7726. Det finns på marknaden ett antal leverantörer av brandväggar mot spam-SMS som använder AI för att flagga upp misstänkta SMS. Det ska dock framhållas att utan verifiering genom stickprov på innehållet i inkommande massutskick av SMS blir det oftast svårt att med tillräckligt stor sannolikhet slå fast att innehållet är bedrägligt och skyddet blir därför inte så effektivt som det annars kunnat vara. Telenor noterar Polismyndighetens svar i denna del och den synpunkt som myndigheten anför vad gäller integritetsaspekten med att ta del av innehåll i massutskick av SMS som misstänks vara brottsliga.

Det saknas en internationell utblick i promemorian, vilket är anmärkningsvärt med tanke på de insatser som gjorts på området i andra nordiska länder. Telenor har större utrymme att agera mot skadliga SMS i Norge och Finland än vad som föreslås i promemorian. Det är också utformat som möjligheter snarare än skyldigheter, vilket Telenor förordar även för Sverige. Om operatörerna ges tydlighet och flexibilitet gällande möjliga säkerhetsåtgärder finns grogrund för innovationer där konkurrensen driver på för säkrare kundupplevelser. Det är många gånger effektivare än otydliga och vagt beskrivna skyldigheter som kräver tolkning genom skarp tillsyn och rättsliga avgöranden.

Det ska i sammanhanget också framhållas att EU-kommissionens förslag till Digital Networks Act (DNA) innehåller förslag till harmoniserade regler för att bekämpa online bedrägerier, som inkluderar blockering av nummer och tjänster. Det finns enligt Telenors mening anledning att analysera hur dessa tvingade regler kommer att utformas innan promemorians förslag omsätts i lag.

Övrigt

Telenor står till regeringens förfogande om det uppkommer behov av ytterligare uppgifter. Telenor åberopar inte sekretess för lämnade uppgifter.

Telenor Sverige AB

Martin Sjöberg
Bolagsjurist