

Promemoria

Nya regler mot bedrägerier och annat vilseledande genom elektroniska kommunikationer

Promemorians huvudsakliga innehåll

Denna promemoria innehåller förslag som syftar till att motverka att elektroniska kommunikationstjänster används för att genomföra bedrägerier eller vilseleda mottagare på något annat sätt.

Det föreslås att tillhandahållare av allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster inte ska överföra ett elektroniskt meddelande om de har anledning att anta att meddelandet överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare. Åtgärder som vidtas med anledning av denna skyldighet får inte innebära en granskning eller annan behandling av innehållet i ett elektroniskt meddelande. För att skapa förutsättningar för åtgärder för kontroll av avsändarnamn för sms ska regleringsmyndigheten få föra ett register över anmälda avsändarnamn för sms. Att registrera avsändarnamn i registret ska vara frivilligt. Vidare föreslås att regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter i anslutning till förslagen. Bestämmelserna utgör delvis ett nytt genomförande av artikel 97.2 av Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation.

De nya reglerna föreslås träda i kraft den 1 augusti 2026.

Innehållsförteckning

1	Lagtext	3
1.1	Förslag till lag om ändring i lagen (2022:482) om elektronisk kommunikation	3
1.2	Förslag till förordning om ändring i förordningen (2022:511) om elektronisk kommunikation	5
2	Ärendet	8
3	Användningen av elektroniska kommunikationstjänster för bedrägeri	8
4	Möjligheterna att hindra meddelanden av skäl som rör bedrägeri eller annat missbruk av tjänsten är begränsade	10
5	En skyldighet att inte överföra elektroniska meddelanden i vissa fall	12
6	Post- och telestyrelsen ska få föra register över avsändarnamn för sms-meddelanden	18
7	Behandling av uppgifter om elektroniska meddelanden	21
8	Ikraftträdande	26
9	Konsekvenser	27
9.1	Konsekvenser om ingen åtgärd vidtas	27
9.2	Konsekvenser för tillhandahållare av allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster	27
9.3	Konsekvenser för Post- och telestyrelsen	28
9.4	Konsekvenser för rättsväsendet	29
9.5	Konsekvenser för enskilda och samhället i övrigt	29
9.6	Övriga konsekvenser	30
10	Författningskommentar	31

1 Lagtext

1.1 Förslag till lag om ändring i lagen (2022:482) om elektronisk kommunikation

Härigenom föreskrivs i fråga om lagen (2022:482) om elektronisk kommunikation

dels att 9 kap. 27 § ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 4 kap. 12 § och 9 kap. 6 a §, av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

4 kap.

12 §

En tillhandahållare av en allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst ska inte överföra ett elektroniskt meddelande om den har anledning att anta att meddelandet överförs

1. som ett led i ett bedrägeri, eller

2. i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om skyldighetens omfattning.

9 kap.

6 a §

Trafikuppgifter får behandlas om uppgifterna behövs vid åtgärder som krävs för att fullgöra skyldigheten i 4 kap. 12 §. Uppgifterna får behandlas endast i den utsträckning och under den tid som är nödvändig för ändamålet. De ska där efter genast utplånas.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

1. vilka uppgifter som får behandlas enligt första stycket, och

2. hur länge uppgifterna får behandlas innan de ska utplånas.

Utöver vad som anges i 1–3 och 31 §§ får inte någon annan än berörda användare ta del av eller på något annat sätt behandla uppgifter i ett elektroniskt meddelande som överförs i ett allmänt elektroniskt kommunikationsnät eller med en allmänt tillgänglig elektronisk kommunikationstjänst, eller trafikuppgifter som hör till detta meddelande, om inte någon av användarna har samtyckt till behandlingen.

Detta hindrar inte

1. lagring som är automatisk, mellanliggande och tillfällig, om den är nödvändig för överföring av ett elektroniskt meddelande, eller sådan lagring i den utsträckning som den är nödvändig för driften av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst,

2. att andra får tillgång till innehållet i ett elektroniskt meddelande, om innehållet ändå är allmänt tillgängligt, om tillgången ges endast för att effektivisera den fortsatta överföringen till andra mottagare samt om uppgifterna om vem som har begärt att få informationen utplånas, eller

3. att någon i en radiomottagare avlyssnar eller på något annat sätt, genom att använda en sådan mottagare, får tillgång till ett radiobefordrat elektroniskt meddelande som inte är avsett för denne eller för allmänheten.

Utöver vad som anges i 1–3, 6 a och 31 §§ får inte någon annan än berörda användare ta del av eller på något annat sätt behandla uppgifter i ett elektroniskt meddelande som överförs i ett allmänt elektroniskt kommunikationsnät eller med en allmänt tillgänglig elektronisk kommunikationstjänst, eller trafikuppgifter som hör till detta meddelande, om inte någon av användarna har samtyckt till behandlingen.

Denna lag träder i kraft den 1 augusti 2026.

1.2 Förslag till förordning om ändring i förordningen (2022:511) om elektronisk kommunikation

Härigenom föreskrivs i fråga om förordning (2022:511) om elektronisk kommunikation

dels att 1 kap. 2 § ska ha följande lydelse,

dels att det ska införas åtta nya paragrafer, 4 kap. 9–15 §§ och 9 kap. 2 a §, och närmast före 4 kap. 10 § en ny rubrik av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 kap.

2 §¹

Denna förordning är meddelad med stöd av

– 1 kap. 9 § lagen (2022:482) om elektronisk kommunikation i
fråga om 1 kap. 6 §,

– 1 kap. 10 § i samma lag i fråga om 1 kap. 7 §,

– 1 kap. 11 § i samma lag i fråga om 1 kap. 8 §,

– 1 kap. 13 § i samma lag i fråga om 1 kap. 9 b och 9 c §§,

– 2 kap. 1 § i samma lag i fråga om 2 kap. 2 §,

– 3 kap. 4 § i samma lag i fråga om 3 kap. 26 §,

– 3 kap. 10 § i samma lag i fråga om 3 kap. 3 §,

– 3 kap. 22 § i samma lag i fråga om 3 kap. 4 §,

– 3 kap. 24 § i samma lag i fråga om 3 kap. 5 och 27 §§,

– 3 kap. 28 § i samma lag i fråga om 3 kap. 27 §,

– 4 kap. 1, 3 och 10 §§ i samma lag i fråga om 4 kap. 7 §,

– 4 kap. 12 § i samma lag i

fråga om 4 kap. 9 §,

– 5 kap. 44 § i samma lag i fråga om 5 kap. 9 §,

– 7 kap. 1, 5, 14, 16, 21, 33 och 35–38 §§ i samma lag i fråga
om 7 kap. 2 §,

– 7 kap. 21 § i samma lag i fråga om 7 kap. 3 §,

– 8 kap. 1 och 3 §§ i samma lag i fråga om 8 kap. 4 och 5 §§,

– 8 kap. 4–6 §§ i samma lag i fråga om 8 kap. 4 §,

– 9 kap. 5 § i samma lag i fråga om 9 kap. 1 §,

– 9 kap. 6 § i samma lag i fråga om 9 kap. 2 §,

– 9 kap. 6 a § i samma lag i

fråga om 9 kap. 2 a §,

– 9 kap. 11 § i samma lag i fråga om 9 kap. 3 §,

– 9 kap. 29 § i samma lag i fråga om 9 kap. 12 §,

– 9 kap. 30 § i samma lag i fråga om 9 kap. 13 §,

– 8 kap. 11 § regeringsformen i fråga om 2 kap. 2 §,

3 kap. 28 §, 4 kap. 8 §, 7 kap. 4 §, 8 kap. 6 §, 9 kap. 9, 11

och 12 §§ och 11 kap. 1 §, och

– 8 kap. 7 § regeringsformen i fråga om övriga bestämmelser.

¹ Senaste lydelse 2024:190.

4 kap.

9 §

Post- och telestyrelsen får meddela ytterligare föreskrifter om omfattningen av skyldigheten att inte överföra ett elektroniskt meddelande enligt 4 kap. 12 § lagen (2022:482) om elektronisk kommunikation.

Register över avsändarnamn för sms-meddelanden

10 §

Post- och telestyrelsen får med hjälp av automatiserad behandling föra ett register över uppgifter om anmälda avsändarnamn för sms-meddelanden.

Post- och telestyrelsen får meddela föreskrifter om

- 1. vilka uppgifter som ska ingå i registret, och*
- 2. vad en anmälan till registret ska innehålla.*

11 §

Post- och telestyrelsen får behandla personuppgifter i registret för att föra en aktuell förteckning över anmälda avsändarnamn för sms-meddelanden.

Post- och telestyrelsen är personuppgiftsansvarig för behandling av personuppgifter i registret.

12 §

Tillhandahållare av allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster ska ha direktåtkomst till uppgifterna i registret.

13 §

En förteckning över anmälda avsändarnamn för sms-meddelanden ska hållas tillgänglig på Post- och telestyrelsens webbplats.

14 §

Post- och telestyrelsen ska ta ut en handläggningsavgift av den som anmäler ett avsändarnamn för sms-meddelanden för registrering i ett sådant register som avses i 10 §.

Post- och telestyrelsen ska ta ut en årlig avgift av den som har ett avsändarnamn för sms-meddelanden registrerat.

15 §

Post- och telestyrelsen får meddela föreskrifter om storleken på de avgifter som får tas ut enligt 14 §.

9 kap.

2 a §

Post- och telestyrelsen får, i fråga om behandling av trafikuppgifter enligt 9 kap. 6 a § lagen (2022:482) om elektronisk kommunikation, meddela föreskrifter om

- 1. vilka uppgifter som får behandlas, och*
- 2. hur länge uppgifterna får behandlas innan de ska utplånas.*

Denna förordning träder i kraft den 1 augusti 2026.

2 Ärendet

Regeringen beslutade i december 2023 att ge Post- och telestyrelsen (PTS) i uppdrag att föreslå åtgärder för att förhindra spoofing och andra tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier (Fi2023/03206). PTS redovisade myndighetens arbete med uppdraget i en promemoria och en rapport. Promemorian Delredovisning – att motverka tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier (23-31716) överlämnades i maj 2024. Rapporten Att motverka tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier, PTS-ER 2024:31, överlämnades i december samma år.

Denna promemoria innehåller förslag på bestämmelser som syftar till att förhindra förfaranden där elektroniska kommunikationstjänster används för bedrägerier eller annat vilseledande av en vidare krets av mottagare. Bestämmelserna utgör delvis ett nytt genomförande av artikel 97.2 av Europaparlamentets och rådets direktiv (EU) 2018/172 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation, i fortsättningen benämnt kodexen för elektronisk kommunikation.

3 Användningen av elektroniska kommunikationstjänster för bedrägeri

Bedrägerier där elektroniska kommunikationstjänster används är en utbredd företeelse som får konsekvenser för den som drabbas. Förekomsten av bedrägerier genom elektroniska kommunikationstjänster påverkar även förtroendet för tjänsterna och för den information som överförs genom dem.

Tillvägagångssättet varierar men kännetecknas av kontaktsökande samtal och sms-meddelanden (sms). Den som blir uppringd eller tar emot ett sms vilseleds om identiteten hos den som ringer eller skickar meddelandet.

Samtal för att inleda kontakt och bygga upp förtroende inför genomförandet av bedrägerier benämns vishing. Syftet kan vara att förmå mottagaren av samtalet att föra över pengar eller lämna ifrån sig uppgifter som gör det möjligt för den andra parten att t.ex. få tillgång till ett bankkonto. Vishingsamtal kombineras ofta med manipulering av det uppringande telefonnumret, s.k. spoofing. Begreppet spoofing kan även användas i vid bemärkelse som benämning på olika slags bedrägerier som sker via telefon eller andra elektroniska kommunikationstjänster som sms och e-post. Det förekommer också att slutanvändare vilseleds genom s.k. wangirisamtal. Med wangirisamtal avses att den som ringer upp lägger på efter bara en signal i syfte att få den som har blivit uppringd att ringa tillbaka, ofta till ett nummer med förhöjd samtalsavgift, exempelvis ett utlandssamtal eller en betalteletjänst.

Förfaranden med kontaktskapande sms med vilseledande avsändaruppgifter kallas för smishing. För att öka trovärdigheten bakom sådana sms används ofta avsändarnamn som liknar eller är identiskt med det som

används av en välkänd avsändare, t.ex. en paketdistributör, bank eller myndighet. Avsändarnamn för sms kallas också SMS Sender ID. Sms:et kan innehålla telefonnummer till en falsk kundtjänst eller en länk som leder till vilseledande annonser, lösenordsfiske eller installation av skadlig programvara i syfte att inhämta personuppgifter eller andra uppgifter från mottagarens terminalutrustning. Vid sms-bedrägerier används ofta tekniska lösningar som möjliggör att samma meddelande skickas samtidigt till ett stort antal mottagare, s.k. applikation till person (A2P). A2P-sms innebär att sms skickas via t.ex. en onlineplattform. Den som tillhandahåller en tjänst för att skicka sådana meddelanden kan benämnas tillhandahållare av sms-aggregatörstjänster. Enligt PTS rapport är bedrägerier som genomförs med stöd av bl.a. sms, meddelandeappar och e-post för närvarande den vanligaste formen av bedrägerier via elektroniska kommunikationstjänster.

Den kartläggning som PTS har gjort inom ramen för regeringsuppdraget visar att det under 2023 polisanmälades ca 29 000 telefonbedrägerier. Den sammanlagda brottsvinsten av de här bedrägerierna uppgick till 708 miljoner kronor, vilket var en ökning med 13 procent jämfört med föregående år. Uppgiften avser såväl samtals- som sms-bedrägerier. Kartläggningen visar vidare att inte alla bedrägerier anmäls. Enligt PTS rapport anger 41 procent av företagare att de inte anmäler något brott, medan 22 procent anger att man endast anmäler vissa brott. Kostnaderna för näringslivet till följd av alla typer av bedrägerier beräknades 2023 till 4,5 miljarder kronor. Bland privatpersoner slår bedrägerier genom elektroniska kommunikationstjänster hårt mot framför allt äldre personer och leder ofta till negativa psykosociala konsekvenser.

Såväl myndigheter som privata aktörer har gjort insatser för att motverka förekomsten av bedrägerier genom elektroniska kommunikationer. PTS redogör i sin rapport för både frivilliga åtaganden och bindande regler som har genomförts helt eller delvis för att motverka spoofing i vid bemärkelse. Dessa åtgärder omfattar informationskampanjer, frivillig registrering av avsändarnamn, filtrering och blockering av samtal och sms samt föreskrifter och allmänna råd som PTS har meddelat (se vidare avsnitt 4). Tillhandahållare av elektroniska kommunikationstjänster har bl.a. lanserat ett gemensamt sms-kortnummer, 7726, dit sms som mottagaren misstänker utgör bedrägerier kan vidarebefordras. Tillhandahållarna kan därefter dela informationen med varandra och agera samlat mot bedrägerier genom sms.

De åtgärder som har vidtagits har haft viss effekt. Enligt PTS blockerar tillhandahållarna 40 000–50 000 samtal med manipulerade nummer varje dygn. Enligt Polismyndighetens statistik minskade brottsvinsterna från vishing- och smishing-bedrägerier med 40 procent 2024 jämfört med 2023. Trots åtgärderna är bedrägerier genom elektroniska kommunikationstjänster fortfarande vanligt förekommande.

4 Möjligheterna att hindra meddelanden av skäl som rör bedrägeri eller annat missbruk av tjänsten är begränsade

Lagen (2022:482) om elektronisk kommunikation (LEK) syftar till att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer. Lagen syftar även till största möjliga utbyte för alla av elektroniska kommunikationstjänster sett till urvalet samt till deras pris, kvalitet och kapacitet (1 kap. 1 § LEK). Syftet ska uppnås främst genom att konkurrensen och den internationella harmoniseringen främjas (prop. 2021/22:136 s. 109). Att slutanvändare har tillgång till säkra och effektiva elektroniska kommunikationstjänster innebär bl.a. att användare ska kunna nå varandra. Det kommer till uttryck bl.a. i 4 kap. 10 § LEK där det framgår att den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst ska se till att slutanvändare kan nå samtliga nummer inom Europeiska ekonomiska samarbetsområdet (EES). Skyldigheten gäller dock under vissa förutsättningar. Det ska vara ekonomiskt genomförbart och numret i fråga ska inte vara ett nummer som enbart har ett nationellt syfte. Den uppringda slutanvändaren ska inte heller av kommersiella skäl ha valt att begränsa nåbarheten från vissa geografiska områden.

Möjligheten för tillhandahållare av elektroniska kommunikationstjänster att avstå från att överföra ett elektroniskt meddelande är begränsad. Med överföring av ett elektroniskt meddelande avses exempelvis att koppla fram ett samtal eller leverera ett sms. Av 4 kap. 11 § LEK framgår att Konsumentombudsmannen i vissa fall får ålägga tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster att hindra användares tillgång till ett nummer eller till en tjänst. Med tjänst avses en tjänst som nås via ett nummer vars sifferstruktur saknar geografisk betydelse. En sådan tjänst är typiskt sett en betalteletjänst. Med nummer avses samtliga nummer inom EES. Ett sådant beslut får fattas om numret eller tjänsten marknadsförs på ett sätt som är otillbörligt eller innebär att väsentlig information utelämnas.

Bestämmelsen i 4 kap. 11 § LEK genomför artikel 97.2 i kodexen för elektronisk kommunikation. Bestämmelsen i artikel 97.2 infördes ursprungligen i Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om samarbete mellan de nationella tillsynsmyndigheter som ansvarar för konsumentskyddslagstiftningen (ändringsdirektivet). Den genomfördes i svensk rätt genom 7 kap. 9 a § lagen (2003:389) om elektronisk kommunikation (prop. 2010/11:115 s. 112–118 och 186–188). När kodexen för elektronisk kommunikation genomfördes ansågs det inte ha kommit fram skäl att implementera bestämmelsen på något annat sätt än vid det tidigare genomförandet. Bestämmelsen fördes därför över till den nya lagen utan ändringar i sak (prop. 2021/22:136 s. 178 och 429).

Syftet med 4 kap. 11 § LEK har varit att kunna hindra bedrägerier eller missbruk vid tillhandahållandet av betalteletjänster som leder till oväntat dyra telefonräkningar. Av förarbetena framgår att det, när bestämmelsen infördes, var ett relativt vanligt problem att konsumenter som använde betalteletjänster upplevde att de hade lurats in i en prenumeration på en tjänst när de endast hade avsett att beställa en enstaka tjänst. Ett annat vanligt problem var att en tjänst debiterades trots att konsumenten hade uppfattat att den var gratis. Vidare kunde det vara svårt för en konsument att säga upp en prenumeration på innehållstjänster. Det var ofta inte fråga om bedrägerier, utan många av problemen handlade om företag som agerade i gråzonen. En gemensam nämnare för dessa var att det fanns brister, otydlighet eller bedräglighet när det gällde bl.a. avtal och prisinformation när en konsument beställde en tjänst. Problemen rörde således i huvudsak marknadsföringen av nummer och tjänster (prop. 2010/11:115 s. 113–118). Konsumentombudsmannen har såvitt känt inte meddelat några beslut med stöd av 4 kap. 11 § LEK.

Telekområdgivarna, som ger opartisk och kostnadsfri vägledning till konsumenter om abonnemang för tv, telefoni och bredband, hanterar sedan 2022 även klagomål om betalteletjänster. Anmälningarna avser enligt organisationens årsstatistik för 2024 t.ex. innehållstjänster som betalas genom engångsköp. Enligt statistikrapporten för 2022 mottog organisationen 7 550 klagomål avseende betalteletjänster det året. Under 2024 minskade antalet klagomål med ca 50 procent jämfört med året innan. Minskningen var troligen ett resultat av ändringar i den uppförandekod för mobila innehållstjänster som har utarbetats av Telekområdgivarna, branschorganisationen MORGAN och tillhandahållare av elektroniska kommunikationstjänster. Ändringarna innebär att det inte längre är förenligt med uppförandekoden att använda prenumerationstjänster för att förmedla mobila spel eller pristävlingar. Självregleringsåtgärder har alltså haft positiva effekter. Det finns dock fortfarande ett behov av bestämmelser som möjliggör ingripande från Konsumentombudsmannen i enlighet med 4 kap. 11 § LEK.

Med stöd av föreskriftsrätten som PTS ges i 4 kap. 7 § 1 och 9 kap. 2 § 1 förordningen (2022:511) om elektronisk kommunikation (FEK) har myndigheten meddelat föreskrifter (PTSFS 2024:2) för att förhindra samtal med manipulerade anropande telefonnummer. Av föreskrifterna framgår hur användningen av svenska telefonnummer ska kontrolleras innan ett samtal kopplas fram. Enligt föreskrifterna ska tillhandahållare av elektroniska kommunikationstjänster göra en kontroll av det anropande telefonnumret för att minimera risken för att samtal med manipulerade telefonnummer kopplas fram (se 4–6 §§). PTS har enligt 4 kap. 7 § FEK endast rätt att meddela föreskrifter om användningen av nummer i den nationella nummerplanen. Myndigheten saknar därmed möjlighet att meddela föreskrifter för att motverka bedrägerier via samtal med nummer från en internationell nummerplan. Eftersom 9 kap. 2 § FEK endast är tillämplig på talkommunikationstjänster har PTS inte heller möjlighet att meddela föreskrifter om behandling av uppgifter i samband med åtgärder för att motverka bedrägerier via sms.

5 En skyldighet att inte överföra elektroniska meddelanden i vissa fall

Promemorians förslag

En tillhandahållare av nummerbaserade elektroniska kommunikationstjänster ska inte överföra ett visst elektroniskt meddelande om den har anledning att anta att meddelandet överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela ytterligare föreskrifter om omfattningen av skyldigheten att inte överföra meddelanden. Post- och telestyrelsen ska ges rätt att meddela sådana föreskrifter.

Skälen för förslaget

En möjlighet att blockera tillgången till nummer eller tjänster i vissa fall

Det finns ett behov att vidta åtgärder för att motverka att elektroniska kommunikationstjänster används för bedrägerier eller annat vilseledande. Som redogörs för i avsnitt 4 finns det i dagsläget inte någon lagstiftning som möjliggör att bedrägerier genom elektroniska kommunikationstjänster kan förhindras på ett ändamålsenligt sätt. Med hänsyn till den ökning av förfaranden där elektroniska kommunikationstjänster används för bl.a. bedrägeri som har skett sedan kodexen för elektronisk kommunikation genomfördes finns det nu skäl att, med utgångspunkt i artikel 97.2 i samma direktiv, införa nya bestämmelser för att förhindra sådana förfaranden.

Av artikel 97.2 i kodexen för elektronisk kommunikation framgår bl.a. att medlemsstaterna ska säkerställa att nationella regleringsmyndigheter kan kräva av tillhandahållare av allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster att, från fall till fall, blockera tillgången till nummer eller tjänster. Sådan möjlighet ska finnas i de fall det är motiverat av skäl som rör bedrägeri eller missbruk. Regleringsmyndigheten ska i sådana fall också få kräva att tillhandahållare av elektroniska kommunikationstjänster håller inne intäkter från relevant samtrafik eller andra tjänster. Bestämmelsen omfattar endast tillgången till tjänster via icke-geografiska nummer inom unionen och nummer som tillhandahålls inom unionen, dvs. nummerbaserade tjänster. Bestämmelsen bör vara utgångspunkten för möjliga krav på åtgärder som kan riktas mot tillhandahållare av elektroniska kommunikationstjänster i syfte att motverka att deras tjänster används för bedrägeri eller missbruk.

Krav på åtgärder för att motverka bedrägerier och annat missbruk bör endast avse tillhandahållare av nummerbaserade interpersonella kommunikationstjänster

PTS kartläggning visar att bedrägerier och annat vilseledande genomförs även genom nummeroberoende interpersonella kommunikationstjänster. De tekniska förutsättningarna för att kontrollera elektroniska meddelanden som överförs genom nummeroberoende interpersonella kommunikations-

tjänster skiljer sig dock från möjligheterna att kontrollera nummerbaserade interpersonella kommunikationstjänster. Användningen av nummerberoende interpersonella kommunikationstjänster genererar exempelvis inte trafikuppgifter på det sätt som sker vid användningen av nummerbaserade tjänster. En kontroll av nummerberoende interpersonella kommunikationstjänster kan i stället t.ex. baseras på filtrering av innehåll.

Av 9 kap. 27 § LEK följer att, med vissa undantag, endast berörda användare får ta del av eller på något annat sätt behandla uppgifter i ett elektroniskt meddelande, om inte någon av användarna har samtyckt till behandlingen. Filtrering av innehållet i ett elektroniskt meddelande är därför inte tillåten annat än i fall där någon av användarna har samtyckt till behandlingen. Det är alltså möjligt för tillhandahållare av nummerberoende interpersonella kommunikationstjänster att, med användarens samtycke, filtrera meddelanden med utgångspunkt i meddelandets innehåll. Meddelanden som dirigeras bort filtreras ofta till s.k. skräppost som användaren av tjänsten kan kontrollera.

Bestämmelsen i artikel 97.2 i kodexen för elektronisk kommunikation bedöms bara avse förfaranden som aktualiseras vid tillhandahållandet av nummerbaserade interpersonella kommunikationstjänster. De möjligheter som tillhandahållare av nummerberoende interpersonella kommunikationstjänster har att vidta verkkningsfulla åtgärder med användarnas samtycke talar vidare emot att krav på åtgärder ställs till dem. Att gå utöver det som avses i artikel 97.2 i fråga om vilka typer av tjänster som bör omfattas av kraven bedöms därför inte som lämpligt. Ett förslag om krav på åtgärder för att motverka bedrägerier och annat missbruk bör mot denna bakgrund endast avse tillhandahållare av nummerbaserade interpersonella kommunikationstjänster.

Möjlighet till blockering i fall som rör bedrägeri eller missbruk

Artikel 97.2 i kodexen för elektronisk kommunikation tillåter en blockering av tillgången till nummer eller nummerbaserade tjänster endast i fall där det är motiverat av skäl som rör bedrägeri eller missbruk. Vilka omständigheter som ska anses utgöra bedrägeri eller missbruk utvecklas dock inte i direktivet. I skäl 254 nämns handlingar i samband med vissa betaltjänster som exempel.

När ändringsdirektivets bestämmelse genomfördes i den då gällande lagen (2003:389) om elektronisk kommunikation ansågs begreppen huvudsakligen ta sikte på s.k. betaltjänster, där problem hade identifierats. Som redogörs för i avsnitt 4 ansågs syftet med bestämmelsen vara att kunna hindra bedrägerier eller missbruk vid tillhandahållandet av betaltjänster som leder till oväntat dyra telefonräkningar. Direktivet bedömdes dock även omfatta förfaranden som inte innebär nyttjande av en tjänst. Ingripande ansågs också kunna ske exempelvis mot förfaranden där någon lockas eller luras att ringa ett utlands- eller satellitnummer med mycket hög taxa (prop. 2010/11:115 s. 112–118).

Betaltjänster förekommer fortfarande på marknaden för elektroniska kommunikationstjänster (se avsnitt 4). De tillvägagångssätt som beskrivs i PTS kartläggning utgörs dock huvudsakligen inte av vilseledande eller otillbörlig marknadsföring av tjänster till konsumenter. Det finns därför

skäl att nu återkomma till frågan om vilken typ av förfaranden som bör anses som bedrägeri eller missbruk i direktivets mening.

Bedrägeri enligt artikel 97.2 i direktivet får anses syfta på en sådan gärning som avses i 9 kap. 1 § första stycket brottsbalken, dvs. en situation där någon avsiktligt vilseleder någon annan att göra eller låta bli att göra något som innebär vinning för bedragaren och skada för den som vilseleds eller någon som är i den vilseleddes ställe. Även ringa respektive grovt bedrägeri enligt 9 kap. 2–3 §§ brottsbalken får anses omfattas av tillämpningsområdet för artikeln. Med hänsyn till syftet med artikeln får den vidare anses omfatta försök till sådana handlingar. Bedrägeri enligt direktivets mening kan därför exempelvis vara ett förfarande där någon skickar ett elektroniskt meddelande som uppmanar mottagaren att klicka på skadliga länkar eller lämna bank- eller personuppgifter, i syfte att ge avsändaren vinning och skada för mottagaren.

Missbruk får antas avse förfaranden där någon på ett sätt som inte omfattas av bedrägeri enligt ovan vilseleder slutanvändare för att nå otillbörlig vinning på dennes bekostnad. Wangirisamtal är ett exempel på ett sådant förfarande. Missbruk bedöms även omfatta handlingar som har för avsikt att vilseleda mottagaren på ett annat otillbörligt sätt, utan att det leder till skada för den som vilseleds. Det kan t.ex. vara sms i syfte att sprida desinformation, där avsändarnamnet är vilseledande så att det framstår som att det kommer från en viss myndighet eller att det är ett meddelande enligt lagen (2023:407) om viktigt meddelande till allmänheten.

I båda fallen bedöms artikel 97.2 i kodexen för elektronisk kommunikation även omfatta förfaranden där andra identifierare än nummer används, om det görs i samband med användning av en nummerbaserad interpersonell kommunikationstjänst. Det kan exempelvis vara i situationer där avsändarnamn för sms används i stället för nummer vid kommunikation med nummer i en nationell eller internationell nummerplan.

Blockering i samband med användning av nummerbaserade interpersonella kommunikationstjänster

Artikel 97.2 i kodexen för elektronisk kommunikation tillåter blockering av tillgången till nummer eller nummerbaserade tjänster i vissa fall. Med en sådan blockering avses att det genom spärrning eller på annat sätt blir omöjligt att nå numret eller tjänsten (prop. 2010/11:115 s. 187). Det kan, i fråga om nummerbaserade interpersonella kommunikationstjänster, likställas med att ett elektroniskt meddelande inte överförs, dvs. att ett samtal inte kopplas fram eller ett sms eller annat meddelande inte levereras.

En åtgärd i syfte att hindra en överföring av ett elektronisk meddelande bör inte föregås av ett förvaltningsbeslut

Direktivet bedöms sammanfattningsvis möjliggöra att det ställs krav på att den som tillhandahåller en nummerbaserad interpersonell kommunikationstjänst ska underlåta att överföra ett elektronisk meddelande om det är motiverat av skäl som rör bedrägeri eller missbruk.

Som framgår av PTS rapport är antalet samtal och sms som har samband med bedrägerier och annat vilseledande mycket omfattande. Den tekniska utvecklingen innebär att det är enkelt att manipulera telefonnummer och skicka sms med avsändarnamn som ser ut att komma från en betrodd

avsändare. För den som vill använda sig av sms i bedrägligt syfte är det enkelt att göra det genom att byta avsändaruppgifter.

För att krav i syfte att motverka användningen av elektroniska kommunikationstjänster för bedrägerier och annat vilseledande ska vara ändamålsenliga bör en blockeringsåtgärd vidtas med automatiserade medel i samband med att tillhandahållaren uppmärksammar ett misstänkt elektroniskt meddelande. En ordning där kravet på åtgärder för blockering föregås av ett förvaltningsbeslut av regleringsmyndighet i enlighet med artikel 97.2 i kodexen för elektronisk kommunikation blir därför inte ändamålsenlig.

Tillhandahållare av nummerbaserade interpersonella kommunikationstjänster ska inte överföra ett elektroniskt meddelande om de har anledning att anta att meddelandet överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare

En skyldighet att underlåta att överföra ett elektroniskt meddelande om det är motiverat av skäl som rör bedrägeri eller missbruk bör utformas på ett sätt som minimerar risken för att andra än de avsedda elektroniska meddelanden blockeras. Samtidigt får kravet på att omständigheterna ska tala för att det rör sig om sådana förhållanden inte vara så högt ställt att skyldigheten förlorar sitt syfte.

Av PTS kartläggning framgår att en av de vanligaste formerna av bedrägerier genom nummerbaserade elektroniska kommunikationstjänster för närvarande är bedrägerier genom sms. Det görs ofta genom att numret manipuleras eller att ett vilseledande avsändarnamn används. Merparten av dessa meddelanden är A2P-sms med avsändarnamn. Genom att avsändarnamnet liknar eller är identiskt med en betrodd aktör vilseleds mottagaren om meddelandets avsändare. Ett annat vanligt förekommande tillvägagångssätt är wangirisamtal. De kännetecknas av att tillhandahållaren under en kort tid överför stora volymer av samtal från utländska nummer som avslutas innan mottagaren har besvarat samtalet. De här typen av förfaranden rör ofta sms eller samtal som riktar sig till ett stort antal mottagare och lämnar spår i form av avvikande trafikmönster i tillhandahållarens system.

Att ställa krav på åtgärder i de fall där tillhandahållare har anledning att anta att ett meddelande överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare framstår som ett lämpligt och ändamålsenligt sätt att avgränsa de handlingar som bör förhindras. Det bör sammanfattningsvis införas en skyldighet för tillhandahållare av nummerbaserade interpersonella kommunikationstjänster att inte överföra ett elektroniskt meddelande om tillhandahållaren har anledning att anta att meddelandet överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare. En sådan skyldighet bör införas i LEK.

Den skyldighet som föreslås innebär inte att tillhandahållare av nummerbaserade interpersonella kommunikationstjänster åläggs en allmän 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 att inte överföra meddelanden. Åtgärder kan behöva vidtas om tillhandahållaren exempelvis uppmärksammar vissa avvikande

trafikmönster som ger anledning att anta att ett visst elektroniskt meddelande överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare. En förutsättning är alltså att det rör sig om avvikande trafikmönster som indikerar att meddelanden överförs med sådant syfte. Enbart omständigheten att någon ringer upprepade samtal innebär inte i sig att det rör sig om ett sådant avvikande trafikmönster som ger anledning att anta att överföringen görs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagaren. Inte heller att en avsändare skickar sms till en vidare krets av mottagare innebär i sig ett sådant avvikande trafikmönster.

I många fall är det tekniskt möjligt att med automatiserade medel genomföra en kontroll av omständigheter som kan aktualisera skyldigheten att inte överföra meddelanden. Ett exempel på automatiserade åtgärder för att förhindra bedrägerier och annat vilseledande är kontroller mot ett register över avsändarnamn som används vid A2P-sms. Tillhandahållaren kan genom automatiserad behandling kontrollera om avsändarnamnet är registrerat och, om så är fallet, om uppgifterna i registret överensstämmer med vissa av de uppgifter som tillhandahållare får tillgång till i samband med överföringen av ett meddelande. En sådan jämförelse kan exempelvis visa om uppgiften om avsändare av sms:et överensstämmer med den tillhandahållare av en sms-aggregatörstjänst som har angetts för avsändarnamnet i registret. Om uppgifterna inte stämmer överens får det anses finnas anledning att anta att ett meddelande överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare (se vidare avsnitt 6).

Ytterligare föreskrifter om skyldigheten att inte överföra elektroniska meddelanden

Utförningen av bestämmelsen om skyldigheten att i vissa fall inte överföra elektroniska meddelanden innebär att en tillhandahållare behöver avgöra vilken information som tillhandahållaren har eller får del av som kan ge 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. Tillhandahållaren måste även inrätta sin verksamhet så att åtgärder för att fullgöra skyldigheten vidtas med anledning av sådan information.

Olika tillhandahållare kan bedöma olika typer av kontrollåtgärder som lämpliga att vidtas med anledning av skyldigheten som föreslås. Åtgärderna kan exempelvis variera beroende på vilka tjänster som tillhandahållaren erbjuder eller om tjänsterna riktas mot konsumenter eller andra slutanvändare. En tillhandahållare av nummerbaserade interpersonella kommunikationstjänster som tillhandahåller telefonitjänster kan komma att behöva göra andra kontroller än den som tillhandahåller en sms-aggregatörstjänst. I vissa fall kan det dock vara motiverat att säkerställa att tillhandahållare som omfattas av skyldigheten genomför samma typ av kontrollåtgärder. Det kan vara fallet om det finns en risk för att variationen i de åtgärder som tillhandahållarna vidtar utnyttjas för att genomföra bedrägerier eller annat vilseledande. Den som avser att genomföra ett bedrägeri kan exempelvis välja att använda en viss tjänst eftersom den inte kontrolleras för ett visst förfarande. En reglering av sådana kontrollåtgärder som

tillhandahållare ska vidta blir så detaljerad och specifik för olika typer av tjänster att det lämpligen bör regleras i myndighetsföreskrifter. I lagen bör det därför införas ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare föreskrifter om omfattningen av skyldigheten att inte överföra elektroniska meddelanden. Rätten att meddela sådana föreskrifter bör ges vidare till PTS i egenskap av regleringsmyndighet och tillsynsmyndighet enligt lagen om elektronisk kommunikation (se 1 kap. 5 § FEK).

Alternativa lösningar

Den föreslagna skyldigheten innebär att tillhandahållaren får ett ansvar att avgöra vilka åtgärder som bör vidtas för att identifiera de elektroniska meddelanden där omständigheterna kring dem ger anledning att anta att de överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare. Tillhandahållaren behöver då bl.a. avgöra vilken information som den har del av vid tillhandahållandet av tjänsterna som kan ge anledning att anta att det rör sig om sådana meddelanden.

Det finns dock andra tänkbara sätt att utforma en skyldighet att vidta åtgärder för att blockera elektroniska meddelanden av skäl som rör bedrägeri eller annat vilseledande. Ett möjligt alternativ vore att reglera skyldigheten att blockera i lag på det sättet som nu föreslås men förena det med ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om på vilket sätt skyldigheten ska fullgöras. Skyldigheten att i vissa fall inte överföra ett elektroniskt meddelande skulle då endast få den innebörd som följer av de föreskrifter som regeringen eller den myndighet som regeringen bestämmer meddelar.

En skyldighet som preciseras i föreskrifter på annan nivå än lag innebär en större tydlighet för tillhandahållare om vilka åtgärder som behöver vidtas för att följa skyldigheten. För slutanvändare av tjänsten blir det tydligt vilken behandling som sker av de elektroniska meddelanden som de skickar eller mottar och i vilka fall ett meddelande inte ska överföras till mottagaren. En sådan lösning är dock mindre flexibel än en reglering som den som föreslås, där det överlämnas till tillhandahållarna på marknaden att själva utforma anpassningen av åtgärder med utgångspunkt i det de bedömer vara mest ändamålsenligt. Nya tillvägagångssätt för bedrägerier via elektroniska kommunikationstjänster uppkommer i rask takt. Det innebär att gällande föreskrifter snabbt kan bli utan verkan och nya föreskrifter behöver meddelas för att förhindra nya förfaranden. Därtill kommer att tillhandahållarna ofta har bäst förutsättningar att avgöra hur, inklusive med vilka tekniska lösningar, som meddelanden som har samband med bedrägeri eller annat vilseledande kan identifieras.

Ytterligare ett alternativ vore att inte reglera skyldigheten i lag utan utforma bestämmelsen som ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om åtgärder som tillhandahållare av nummerbaserade interpersonella kommunikationstjänster ska vidta för att förhindra att tjänsten används för bedrägeri eller annat vilseledande. Med stöd i ett sådant bemyndigande skulle föreskrifter kunna meddelas om såväl vilka åtgärder som tillhandahållare ska vidta för att identifiera meddelanden som har samband med bedrägeri eller

annat vilseledande som hur sådana meddelanden ska hanteras. I likhet med föregående alternativ är denna lösning mindre flexibel eftersom skyldigheten sannolikt skulle begränsas till specifika åtgärder som svårigen skulle kunna omfatta alla förfaranden som används för bedrägeri eller annat vilseledande. Det kan vidare ifrågasättas lämpligheten av att krav på åtgärder för blockering av elektronisk kommunikation ställs i föreskrifter på annan nivå än i lag. Utgångspunkten bör i stället vara att krav på åtgärder av så ingripande karaktär bör ställas i lag.

Den ordning som nu föreslås, som innebär en lagreglerad skyldighet att inte överföra elektroniska meddelanden i vissa fall, framstår mot denna bakgrund som mest lämplig och ändamålsenlig.

6 Post- och telestyrelsen ska få föra register över avsändarnamn för sms-meddelanden

Promemorians förslag

Post- och telestyrelsen ska få föra ett register över uppgifter om anmälda avsändarnamn för sms-meddelanden. Myndigheten ska få meddela föreskrifter om vilka uppgifter som ska ingå i registret och om vad en anmälan till registret ska innehålla.

Tillhandahållare av nummerbaserade interpersonella kommunikationstjänster ska ha direktåtkomst till uppgifterna i registret.

En förteckning över anmälda avsändarnamn för sms-meddelanden ska hållas tillgänglig på myndighetens webbplats.

Post- och telestyrelsen ska få behandla personuppgifter i registret i syfte att föra en aktuell förteckning över anmälda avsändarnamn för sms-meddelanden. Myndigheten blir personuppgiftsansvarig för behandling av personuppgifter i registret.

Post- och telestyrelsen ska ta ut en handläggningsavgift av den som anmäler ett avsändarnamn för sms-meddelanden för registrering och en årlig avgift av den som har ett avsändarnamn registrerat.

Skälen för förslaget

Ett register över uppgifter om avsändarnamn för sms-meddelanden

Som framgår av PTS kartläggning är smishing, dvs. kontaktskapande sms med vilseledande avsändaruppgifter, ett vanligt förfarande för bedrägerier genom elektroniska kommunikationer. Genom att meddelandet förses med ett avsändarnamn som liknar eller är likadant som det som används av en betrodd avsändare, t.ex. en paketdistributör, en bank eller en myndighet ökar meddelandets trovärdighet.

Det finns i dagsläget ingen reglering av hur avsändarnamn för sms får användas. Det innebär bl.a. att det inte finns någon enhetlig kontroll av vem som skickar sms med avsändarnamn. Det är därmed möjligt att använda ett avsändarnamn för sms som är identiskt med det avsändarnamn

som används av någon annan. Om mottagaren tidigare har fått andra meddelanden med samma avsändarnamn kan det medföra att sms från olika avsändare läggs till i samma sms-konversation i mottagarens sms-inkorg. Det gör det svårare för mottagaren att identifiera avsändaren av sms:et och skilja på olika meddelanden.

Enligt PTS kartläggning skickas det drygt 5,8 miljarder A2P-sms årligen. Sms med avsändarnamn används för att nå mottagare med exempelvis reklamutskick, leveransaviser, påminnelser om läkarbesök och information för tvåfaktorsautentisering, t.ex. vid köp och beställningar. Om en mottagare misstar ett sms med vilseledande eller felaktig information för ett korrekt meddelande kan det bl.a. få ekonomiska konsekvenser. Även den omvända situationen, att en mottagare uppfattar ett sms som ett försök till bedrägeri i fall då det inte är det, kan få konsekvenser för den enskilde. Det kan exempelvis leda till att en levererad vara inte hämtas ut från ett postombud eller att ett inbokat läkarbesök missas. Det är därmed av stor vikt att mottagare av sms med avsändarnamn kan lita på att informationen i sådana meddelanden är korrekt.

Av PTS rapport framgår vidare att ett antal tillhandahållare av elektroniska kommunikationstjänster har tagit fram en gemensam lösning för registrering av avsändarnamn för sms. Lösningen innebär att företag och andra aktörer kan anmäla det avsändarnamn de använder för sms-utskick och uppgift om vilken tillhandahållare av sms-aggregatörstjänster som hanterar utskicket till ett gemensamt register. Sms som inte kommer från den för företaget eller organisationen registrerade tillhandahållaren av sms-aggregatörstjänster överförs inte. Registret är dock inte offentligt. Det är därmed inte möjligt för en mottagare av ett sms att kontrollera om ett avsändarnamn är registrerat. Den gemensamma lösningen används vidare inte av alla tillhandahållare av elektroniska kommunikationstjänster.

Avsändarnamn för sms används i många länder. Av PTS rapport framgår att det i bl.a. Finland och Irland förs register över avsändarnamn av den nationella regleringsmyndigheten. De registrerade avsändarnamnen är offentliga. Även organisationen European Conference of Postal and Telecommunications Administrations (CEPT), där Sverige ingår, har tagit fram en rekommendation om hanteringen av avsändarnamn, som bl.a. förordar inrättande av register för avsändarnamn.

Ett sätt att motverka bedrägerier genom sms med vilseledande avsändarnamn kan vara att även i Sverige inrätta ett register över avsändarnamn för sms. Genom att införa en liknande lösning som den som har implementerats i andra länder begränsas också risken för att avsaknaden av reglering i Sverige leder till att aktörer som genomför bedrägerier genom elektroniska kommunikationstjänster särskilt riktar in sig på svenska slutanvändare. Det bör därför införas en möjlighet för PTS att föra ett sådant register. De registrerade avsändarnamnen bör vara offentliga så att mottagande slutanvändare kan verifiera autenticiteten av mottagna meddelanden. För att det ska vara enkelt för slutanvändare att kontrollera om ett avsändarnamn är registrerat bör en förteckning över anmälda avsändarnamn hållas tillgänglig på PTS webbplats.

Vilka uppgifter som ska ingå i en anmälan till ett sådant register regleras lämpligen i myndighetsföreskrifter.

Tillhandahållare bör ha direktåtkomst till uppgifterna i registret

De avsändarnamn som är registrerade bör vara tillgängliga på PTS webbplats. Om ett avsändarnamn är registrerat ska slutanvändaren kunna anta att avsändarnamnet i meddelandet har kontrollerats av tillhandahållaren som överförde meddelandet. En sådan kontroll omfattar både om avsändarnamnet är registrerat och om uppgifterna i registret stämmer överens med de trafikuppgifter om meddelandet som tillhandahållaren behandlar i samband med överföringen.

De kontroller som tillhandahållare av nummerbaserade interpersonella kommunikationstjänster gör mot ett register över avsändarnamn för sms ska kunna ske genom automatiserade medel. En sådan kontroll behöver utgå från korrekta uppgifter. Om kontrollen utförs baserat på inaktuella uppgifter kan det leda till att ett meddelande som borde ha överförts inte levereras eller att ett meddelande som borde ha hindrats överförs. Det kan exempelvis inträffa om den registrerade uppdaterar informationen i registret om vilken tillhandahållare av sms-aggregatörstjänster som är behörig att skicka sms med ett visst avsändarnamn. För att försäkra att tillhandahållarna vid varje tidpunkt har tillgång till aktuell information bör de ha direktåtkomst till uppgifterna i registret.

Anmälan till registret bör vara frivillig

Företag och andra aktörer kan komma att göra olika bedömningar av värdet av att registrera sina avsändarnamn för sms i ett register för kontroll vid överföring av sådana meddelanden. Större företag och aktörer, som skickar många sms med avsändarnamn och som i högre utsträckning drabbas av att deras avsändaruppgifter används på ett missvisande sätt, kan se ett stort värde i att registrera sina avsändarnamn i registret. En mindre organisation, vars uppgifter inte i samma utsträckning används för att genomföra bedrägerier eller annat vilseledande, kan göra en annan bedömning. Att registrera avsändaruppgifter för sms i ett register över avsändarnamn bör därför vara frivilligt.

Behandling av personuppgifter i registret

Registrering av avsändarnamn för sms kan innebära personuppgiftsbehandling. Ett avsändarnamn kan vara en personuppgift, exempelvis om ett firmanamn är detsamma som innehavarens personnamn. Det kan även finnas skäl att registrera en kontaktperson för varje registrerat företag eller organisation. Personuppgiftsbehandling kan därför vara nödvändig för att PTS ska kunna föra ett register över sådana avsändarnamn. Att föra ett sådant register som föreslås får anses vara en sådan uppdragsverksamhet som är motiverad av allmänt intresse (jfr prop. 2017/18:105 s. 57). Behandlingen av personuppgifter i registret är därmed nödvändig för att utföra en uppgift av allmänt intresse enligt artikel 6(1)(e) i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)). PTS ska vara personuppgiftsansvarig för de uppgifter som behandlas i registret.

Ett register över avsändarnamn för sms som gör det möjligt att identifiera abonnenten bakom ett visst avsändarnamn utgör en sådan allmänt

tillgänglig abonnentförteckning som avses i 9 kap. 17 § LEK. Innan personuppgifter om en abonnent som är en fysisk person tas in i förteckningen ska tillhandahållaren av förteckningen lämna abonnenten information om ändamålen med förteckningen och de sökfunktioner som finns (9 kap. 17 § LEK). För behandling av personuppgifter om en abonnent som är en fysisk person i en sådan förteckning krävs det samtycke från personen (9 kap. 18 § LEK).

De abonnenter som skickar sms med avsändarnamn är vanligtvis företag eller andra aktörer, dvs. juridiska personer. Registret förväntas därmed inte innehålla personuppgifter om abonnenter som är fysiska personer. Om sådana uppgifter skulle förekomma gäller kraven i 9 kap. 17 och 18 §§ LEK för behandlingen.

Rätt att ta ut avgift för handläggning av registrering och registerhållning

Att föra ett register över avsändarnamn för sms är förenat med kostnader för registerhållaren. Kostnader uppkommer för såväl hanteringen av anmälningar till registret som registerhållningen. För en ändamålsenlig och säker användning av registret över avsändarnamn för sms är det viktigt att de registrerade uppgifterna är korrekta och aktuella. Det kräver att registret hålls uppdaterat, vilket också är förenat med kostnader för registerhållaren. Företag och andra aktörer som registrerar sina avsändarnamn i registret får en fördel genom att de löper mindre risk för att deras namn och verksamhet utnyttjas i brottsligt syfte. De kostnader som registrering och registerhållningen i övrigt innebär bör mot denna bakgrund finansieras med avgifter.

Eftersom registreringen är tänkt att vara frivillig och avgifterna därmed inte är tvingande avser avgifterna en del av myndighetens uppdragsverksamhet. Regeringen har i sådana fall rätt att meddela föreskrifter om avgifterna. I föreskrifterna bör det regleras att PTS ska ta ut avgifter av den som anmäler ett avsändarnamn för sms för registrering. Avgifterna bör bestå av en handläggningsavgift och en årlig avgift. Handläggningsavgiften ska täcka myndighetens kostnader för handläggningen av registreringsärendet. De årliga avgifterna ska sammantagna täcka de kostnader som myndigheten, utöver kostnaden för handläggningen av registreringsärendet, i övrigt har med anledning av registret.

Avgifternas storlek behöver inte regleras i förordning, utan kan regleras i myndighetsföreskrifter. PTS bör därför få rätt att meddela sådana föreskrifter.

7 Behandling av uppgifter om elektroniska meddelanden

Promemorians förslag

En tillhandahållare av nummerbaserade interpersonella kommunikationstjänster ska få behandla trafikuppgifter för att fullgöra skyldigheten att inte överföra ett elektroniskt meddelande om den har anledning att

anta att meddelandet överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare.

En förutsättning för behandlingen ska vara att uppgifterna behövs vid åtgärder som krävs för att fullgöra skyldigheten. Uppgifterna ska få behandlas endast i den utsträckning och under den tid som är nödvändig för ändamålet. De ska därefter genast utplånas.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om vilka uppgifter som får behandlas och om hur länge det får göras innan uppgifterna ska utplånas.

Skälen för förslaget

Åtgärder för att fullgöra skyldigheten kräver behandling av vissa uppgifter

Den skyldighet att i vissa fall inte överföra elektroniska meddelanden som föreslås innebär att tillhandahållare av nummerbaserade interpersonella kommunikationstjänster behöver vidta åtgärder för att kontrollera om det finns omständigheter som medför att ett elektroniskt meddelande inte ska överföras. Sådana omständigheter kan uppmärksammas av tillhandahållaren på olika sätt.

Tillhandahållare av elektroniska kommunikationstjänster får som utgångspunkt inte behandla uppgifter om innehållet i ett meddelande. Av 9 kap. 27 § LEK följer nämligen att, utöver vad som anges i 1–3 och 31 §§ LEK, endast de berörda användarna får ta del av eller på något sätt behandla uppgifter i ett elektroniskt meddelande som överförs i ett allmänt elektroniskt kommunikationsnät eller med en allmänt tillgänglig elektronisk kommunikationstjänst, om inte någon av användarna har samtyckt till behandlingen. De åtgärder som en tillhandahållare vidtar för att fullgöra skyldigheten att i vissa fall inte överföra elektroniska meddelanden får därför utgå från annan information om meddelandet än dess innehåll. Under rubriken Förutsättningar för behandling av uppgifter om elektroniska meddelanden finns en närmare redogörelse för bestämmelsen och dess innebörd.

Tillhandahållare får exempelvis del av uppgifter om ett elektroniskt meddelande och om dess avsändare och mottagare i samband med överföringen av meddelandet. En uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande utgör enligt 1 kap. 7 § LEK en trafikuppgift. Begreppet trafikuppgift kan t.ex. omfatta uppgifter om uppringande och uppringt nummer, datum och tid för ett samtal och hur länge samtalet varade. Det kan också omfatta vissa lokaliseringsuppgifter som behandlas i samband med överföringen av ett elektroniskt meddelande. En lokaliseringsuppgift definieras i samma bestämmelse som en uppgift som behandlas i ett allmänt mobilt elektroniskt kommunikationsnät och som anger den geografiska positionen för en slutanvändares terminalutrustning eller en uppgift i ett allmänt fast elektroniskt kommunikationsnät om nätanslutningspunktens fysiska adress. Det kan exempelvis vara en uppgift om vilken cell (antenn på basstation) som terminalutrustning har kopplat upp sig mot (prop. 2018/19:86 s. 12).

Ytterligare en kategori av uppgifter om elektronisk kommunikation är uppgifter om abonnemang. Sådana uppgifter definieras inte, vare sig i nationell rätt eller i EU-rätten. Med uppgift om abonnemang avses bl.a. uppgifter om abonnentens nummer, namn, titel och adress. Avgörande för bedömningen av om en uppgift är en uppgift om abonnemang är om uppgiften identifierar abonnenten eller den registrerade användaren bakom ett visst nummer eller en viss adress (prop. 2018/19:86 s. 93 och prop. 1992/93:200 s. 310). Med abonnent avses enligt 1 kap. 7 § LEK den som ingått avtal med en tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster om tillhandahållande av sådana tjänster.

I syfte att upptäcka avvikande trafikmönster kan en tillhandahållare av interpersonella nummerbaserade kommunikationstjänster exempelvis behöva behandla uppgifter som visar att ett visst telefonnummer genomför ett stort antal misslyckade uppringningar eller samtal med mycket kort varaktighet under en kort tid. Sådana uppgifter utgör trafikuppgifter.

En tillhandahållare kan även få del av information om ett elektroniskt meddelande genom en kontroll i ett sådant register över avsändarnamn som beskrivs i avsnitt 6. Ett sms med avsändarnamn skickas i regel av en tillhandahållare av sms-aggregatörstjänster. För att granska om den avsändande tillhandahållaren har rätt att skicka meddelanden med det aktuella avsändarnamnet kan tillhandahållaren kontrollera avsändaruppgifterna i ett sådant register. Uppgifter om den avsändande tillhandahållaren av sms-aggregatörstjänster som behandlas i syfte att överföra meddelandet eller fakturera detta meddelande utgör trafikuppgifter enligt definitionen i 1 kap. 7 § LEK. En tillhandahållare av sms-aggregatörstjänster är i vissa fall en tillhandahållare av elektroniska kommunikationstjänster. Den som har ingått ett avtal med tillhandahållaren om användningen av sådana tjänster är därmed abonnent. Uppgifterna i registret som identifierar abonnenten bakom ett visst avsändarnamn utgör alltså uppgifter om abonnemang.

Åtgärder vid kontroll mot ett sådant register som avses ovan bedöms innebära en behandling av uppgifter om avsändaren av meddelandet (trafikuppgifter), typiskt sett en tillhandahållare av en sms-aggregatörstjänst. Åtgärderna innebär även en behandling av registrerade uppgifter om avsändarnamn för sms och uppgifter som identifierar abonnenten bakom ett sådant avsändarnamn (uppgifter om abonnemang).

De uppgifter som en tillhandahållare av nummerbaserade interpersonella kommunikationstjänster kan behöva behandla i samband med åtgärder för att fullgöra skyldigheten att inte överföra vissa meddelanden är sammanfattningsvis främst trafikuppgifter och i vissa fall även uppgifter om abonnemang.

Förutsättningar för behandling av uppgifter om elektroniska meddelanden

Bestämmelserna om behandling av trafikuppgifter och integritetsskydd finns i 9 kap. i LEK. Trafikuppgifter får, med vissa angivna undantag, enligt 1 § behandlas endast under den tid som de behövs för överföringen av ett elektroniskt meddelande. De ska därefter utplånas eller avidentifieras. Efter samtycke från den som uppgifterna rör får trafikuppgifter enligt 2 § behandlas för att tillhandahålla andra tjänster där uppgifterna behövs. Av

3 § följer vem som får utföra behandling av trafikuppgifter. I 4 § anges när begränsningarna i 1–3 §§ inte gäller. Enligt 4 § 4 gäller inte begränsningarna i den utsträckning som trafikuppgifterna är nödvändiga för att förhindra eller avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

I 9 kap. 27 § finns den grundläggande bestämmelsen till skydd för hemligheten för elektroniska meddelanden. Utöver det som anges i 9 kap. 1–3 och 31 §§ får endast berörda användare ta del av eller på något annat sätt behandla uppgifter i ett elektroniskt meddelande om inte någon av användarna har samtyckt till behandlingen. Detsamma gäller trafikuppgifter som hör till meddelandet. Från detta görs dock vissa undantag. Bestämmelsen hindrar inte lagring som är automatisk, mellanliggande och tillfällig, om lagringen är nödvändig för överföringen av ett elektroniskt meddelande. Sådan lagring är även tillåten i den utsträckning som den är nödvändig för driften av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Bestämmelsen hindrar inte heller att andra får tillgång till innehållet i ett elektroniskt meddelande om innehållet ändå är allmänt tillgängligt, om tillgången ges endast för att effektivisera den fortsatta överföringen till andra mottagare samt om uppgifterna om vem som har begärt att få informationen utplånas. Därtill undantas att någon i en radiomottagare avlyssnar eller får tillgång till ett radiobefordrat elektroniskt meddelande som inte är avsett för denne eller för allmänheten. Bestämmelsen gäller inte heller när tillhandahållare av nummeroberoende interpersonella kommunikationstjänster behandlar uppgifter i enlighet med Europaparlamentets och rådets förordning (EU) 2021/1232 av den 14 juli 2021 om ett tillfälligt undantag från vissa bestämmelser i direktiv 2002/58/EG vad gäller användning av teknik hos tillhandahållare av nummeroberoende interpersonella kommunikationstjänster för behandling av personuppgifter och andra uppgifter i syfte att bekämpa sexuella övergrepp mot barn på nätet.

Bestämmelserna i 9 kap. 1–4 och 27 §§ LEK genomför bestämmelserna i artikel 6 respektive artikel 5.1 och 5.2 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), i fortsättningen benämnt e-dataskyddsdirektivet. I artikel 15.1 i samma direktiv anges under vilka förutsättningar som medlemsstaterna får begränsa de rättigheter och skyldigheter som följer av bl.a. artiklarna 5 och 6. Sådan begränsning får göras genom lagstiftning när den i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för bl.a. förebyggande, undersökning, avslöjande av och åtal för brott.

Utöver de begränsningar i behandlingen av uppgifter om elektroniska meddelanden som följer av 9 kap. 1–4 och 27 §§ LEK föreskrivs det en tystnadsplikt i 9 kap. 31 § i LEK. Tystnadsplikten gäller bl.a. för den som tillhandahåller nummerbaserade interpersonella kommunikationstjänster. Den som i samband med tillhandahållande av en sådan tjänst har fått del av eller tillgång till vissa angivna uppgifter får inte obehörigen föra vidare eller utnyttja det han eller hon har fått del av eller tillgång till. Tystnadsplikten avser uppgift om abonnemang, innehållet i ett elektroniskt meddelande och annan uppgift som angår ett särskilt elektroniskt meddelande. I den senaste kategorin ingår trafikuppgifter.

Det bör införas bestämmelser som tillåter nödvändig behandling av trafikuppgifter vid åtgärder för att fullgöra skyldigheten att inte överföra elektroniska meddelanden i vissa fall

Den behandling av trafikuppgifter som beskrivs ovan antas bli nödvändig vid åtgärder för att identifiera elektroniska meddelanden som överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare. Behandlingen är som framgår ovan inte tillåten om inte bestämmelser som möjliggör den införs. Vidare ska sådana bestämmelser vara förenliga med de krav som ställs i artikel 15.1 i e-dataskyddsdirektivet.

Utgångspunkten är att uppgifterna behöver behandlas under en mycket kort tid i samband med att en överföring av ett elektronisk meddelande initieras av en avsändare eller ett uppringande nummer. För att en behandling av trafikuppgifter ska vara proportionerlig i förhållande till syftet bör den begränsas till den utsträckning och tid som är nödvändig för ändamålet. Uppgifterna bör därefter genast utplånas. Med att utplåna avses att uppgifterna ska förstöras så att de inte kan återskapas (jfr. prop. 2016/17:113 s. 19).

Införandet av en bestämmelse som möjliggör nödvändig behandling av uppgifter för att vidta åtgärder i syfte att förebygga bedrägerier och annat vilseledande av elektroniska kommunikationstjänster bedöms vara nödvändigt, lämpligt och proportionerligt för att förebygga en viss typ av brottsliga förfaranden (se avsnitt 5). En sådan lagstiftningsåtgärd är därmed att anse som förenlig med kraven som ställs i artikel 15.1 i e-dataskyddsdirektivet.

Det bör mot denna bakgrund införas en bestämmelse som ger tillhandahållare av nummerbaserade interpersonella kommunikationstjänster rätt att behandla trafikuppgifter för att fullgöra skyldigheten att inte överföra elektroniska meddelanden i vissa fall. En förutsättning för behandlingen bör vara att uppgifterna behövs vid åtgärder som krävs för att fullgöra skyldigheten. Uppgifterna bör få behandlas endast i den utsträckning och under den tid som är nödvändig för ändamålet. De bör därefter genast utplånas.

Begränsningar i hur uppgifter om abonnemang och trafikuppgifter får behandlas följer, som framgår ovan, även av 9 kap. 31 § LEK. Uppgifterna får enligt bestämmelserna inte obehörigen föras vidare eller utnyttjas av den som i samband med tillhandahållande av tjänsten har fått del av eller tillgång till uppgifterna. Den typ av behandling av uppgifter som antas behövas för att vidta åtgärder för att fullgöra skyldigheten bedöms inte innebära att uppgifterna förs vidare eller utnyttjas i den mening som avses i 9 kap. 31 § (jfr prop. 2021/22:136 s. 327–329 och 509–511, prop. 2002/03:110 s. 271–272 och 397 och prop. 1992/93:200 s. 162–164 och 310). Bestämmelsen hindrar därför inte den uppgiftsbehandling som bedöms som nödvändig för att fullgöra skyldigheten som nu föreslås.

PTS bör få meddela ytterligare föreskrifter om behandling av trafikuppgifter

Tillhandahållare av nummerbaserade interpersonella kommunikationstjänster föreslås endast få behandla de trafikuppgifter som behövs för att vidta sådana åtgärder som krävs för att fullgöra skyldigheten att i vissa fall

inte överföra ett elektroniskt meddelande. Behandling av trafikuppgifter för det syftet föreslås endast få ske i den utsträckning och under den tid som är nödvändig för ändamålet.

Skyldigheten att inte överföra ett elektroniskt meddelande kan innebära att tillhandahållaren inte ska koppla fram ett samtal. Det kan också innebära att en tillhandahållare inte ska leverera ett sms till den avsedda mottagaren. Skyldigheten omfattar med andra ord olika typer av elektroniska meddelanden. För att avgöra om ett meddelande ska överföras eller inte kan en tillhandahållare, som nämnts ovan, behöva behandla trafikuppgifter. Det kan behövas för att upptäcka sådana avvikande trafikmönster som ger anledning att anta att ett samtal utgör ett wangirisamtal. Det kan då röra sig om uppgifter om ett samtals geografiska ursprung och varaktighet och om ett stort antal liknande samtal genomförs i nära anslutning till varandra. Trafikuppgifter kan även behöva behandlas för att upptäcka avvikelser i förhållande till den information som har registrerats om ett visst avsändarnamn för sms. Vilka uppgifter som behöver behandlas varierar alltså beroende på vilken typ av elektroniskt meddelande som används för en viss kommunikation. Det kan även variera beroende på vilket förfarande som används för ett bedrägeri eller annat vilseledande. Behovet att behandla olika typer av uppgifter kan därmed skilja sig åt beroende på kommunikationsslag och förfarande.

Eftersom det finns skillnader både i fråga om vilka uppgifter som kan behöva behandlas och hur länge det kan behöva göras kan det finnas anledning att precisera den tillåtna behandlingen i föreskrifter. Det kan exempelvis avse vilka uppgifter som får behandlas i syfte att vidta åtgärder mot ett visst förfarande. Det kan också finnas skäl att ställa upp bortre tidsgränser för behandlingen för att upptäcka ett visst förfarande för bedrägerier eller annat vilseledande. Sådana bestämmelser meddelas lämpligen i myndighetsföreskrifter. Regeringen eller den myndighet som regeringen bestämmer bör därför få meddela föreskrifter om vilka uppgifter som får behandlas för att fullgöra skyldigheten att inte överföra vissa meddelanden och om hur länge uppgifterna får behandlas. Rätten att meddela sådana föreskrifter bör delegeras till PTS.

8 Ikraftträdande

Promemorians förslag

Författningsändringarna ska träda i kraft den 1 augusti 2026.

Skälen för promemorians förslag

Det är angeläget att åtgärder vidtas för att motverka bedrägerier och annat vilseledande genom elektroniska kommunikationstjänster. Förslagen i promemorian bör därför träda i kraft så snart som möjligt. Förslagen innebär att nya skyldigheter införs för tillhandahållare av nummerbaserade interpersonella kommunikationstjänster och kan kräva viss anpassning av tillhandahållarnas verksamheter. De anpassningar som behöver göras

bedöms dock vara av begränsad omfattning. Ett lämpligt datum för ikraftträdande bör mot denna bakgrund vara den 1 augusti 2026.

Lag- och förordningsändringarna bör tillämpas omedelbart efter ikraftträdandet. Det saknas behov av att införa särskilda övergångsbestämmelser.

9 Konsekvenser

9.1 Konsekvenser om ingen åtgärd vidtas

Att elektroniska kommunikationstjänster används för att genomföra bedrägerier och vilseleda på annat sätt är vanligt förekommande. De kontakter som PTS, inom ramen för regeringsuppdraget, har haft med regleringsmyndigheter i andra länder visar också att det är fråga om ett internationellt problem. Bedrägerier som genomförs genom elektroniska kommunikationstjänster har ofta ett gränsöverskridande element. Bedrägerierna drabbar också slutanvändare i olika länder. Enligt PTS rapport vidtas åtgärder för att motverka bedrägerier och annat vilseledande av och genom elektroniska kommunikationstjänster i flera länder. Arbete sker även inom ramen för de internationella samarbetsorgan där PTS deltar.

De åtgärder som har vidtagits i Sverige har hittills varit begränsade till vissa förfaranden, såsom samtal från utlandet med manipulerade svenska nummer. De rättsliga förutsättningarna för att vidta ytterligare åtgärder är i dagsläget begränsade. Det innebär att såväl myndigheter som tillhandahållare av elektroniska kommunikationstjänster saknar möjligheter att vidta åtgärder för att möta nya tillvägagångssätt för bedrägerier och annat vilseledande. Sms med vilseledande avsändarnamn är ett exempel på ett sådant tillvägagångssätt där det i dag saknas möjligheter att vidta effektiva åtgärder. Den omständigheten att åtgärder vidtas i andra länder för att stoppa sådana sms innebär att risken för att bedrägerier som riktas mot svenska slutanvändare ökar om inte åtgärder vidtas också i Sverige.

9.2 Konsekvenser för tillhandahållare av allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster

Förslagen innebär bl.a. en ny skyldighet för tillhandahållare av allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster att inte överföra ett elektroniskt meddelande om tillhandahållaren har anledning att anta att meddelandet överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare. Sådana tillhandahållare ska självmant göra de bedömningar och vidta de åtgärder som krävs för att uppfylla skyldigheten. Därutöver ska de följa de föreskrifter som PTS kan komma att meddela. Det kan medföra ett behov av att utveckla tekniska lösningar och anpassa bl.a. tekniska system och rutiner.

Utgångspunkten är att skyldigheten i första hand ska följas genom automatiserade förfaranden. Sådana förfaranden kan t.ex. innefatta en automatiserad behandling av trafikuppgifter eller automatiserad kontroll mot ett register över avsändarnamn för sms.

De tillhandahållare som omfattas av förslagen ska redan i dag verifiera samtal för att förhindra samtal med manipulerade anropande nummer enligt PTS föreskrifter (PTSFS 2024:2). Vissa tillhandahållare har också utvecklat en frivillig tjänst med en gemensam teknisk lösning för filtrering av avsändarnamn för sms med utgångspunkt i ett frivilligt register. Flera tillhandahållare har också system för att identifiera wangirisamtal. De tekniska lösningar som redan har implementerats borde, i vissa fall med viss anpassning, kunna användas för att fullgöra skyldigheten enligt förslagen. Sådan anpassning kan t.ex. avse kriterierna för filtrering. Förslagen borde mot denna bakgrund innebära begränsade kostnader för tillhandahållare av nummerbaserade interpersonella kommunikationstjänster.

9.3 Konsekvenser för Post- och telestyrelsen

Förslagen medför nya arbetsuppgifter för PTS. Myndigheten får meddela föreskrifter om bl.a. omfattningen av skyldigheten att i vissa fall inte överföra elektroniska meddelanden. Därutöver får PTS föra ett register över uppgifter om anmälda avsändarnamn för sms. Om ett sådant register inrättas kommer PTS att vara personuppgiftsansvarig för behandling av personuppgifterna i registret. Myndigheten ska då även hålla en förteckning för anmälda avsändarnamn för sms tillgänglig på sin webbplats och ge tillhandahållare som omfattas av skyldigheten direktåtkomst till vissa uppgifter i registret. Förslagen innebär vidare att det införs nya skyldigheter för tillhandahållare av nummerbaserade interpersonella kommunikationstjänster som omfattas av myndighetens tillsynsansvar.

PTS meddelar redan i dag föreskrifter med stöd av LEK. Myndigheten genomför även tillsyn av tillhandahållare av elektroniska kommunikationstjänster. De uppgifter som tillförs myndigheten i denna del är därmed sådana som myndigheten har kompetens och vana att genomföra. Omfattningen av de tillkommande uppgifterna kommer att bero bl.a. på de föreskrifter som PTS meddelar och den tillsyn som myndigheten beslutar att genomföra. Föreskrifts- och tillsynsarbetet ska finansieras genom de avgifter som myndigheten tar ut enligt 14 kap. 2 § LEK.

Om ett register över anmälda avsändarnamn inrättas kan det innebära att PTS behöver utveckla en teknisk lösning för registret som bl.a. möjliggör direktåtkomst för tillhandahållare av nummerbaserade interpersonella kommunikationstjänster. Det skulle kunna medföra kostnader för myndigheten. PTS har dock erfarenhet av snarlika uppgifter och av att inrätta register. Om PTS skulle inrätta ett register bedöms det därmed få begränsade konsekvenser för myndighetens verksamhet och organisation. Eventuella kostnader förenade med registret får finansieras av de avgifter som föreslås kunna tas ut för registrering av avsändarnamn och registerhållning. Övriga eventuella kostnader till följd av förslagen bedöms kunna hanteras inom befintligt anslag.

9.4 Konsekvenser för rättsväsendet

Förslagen syftar till att försvåra bl.a. brottslig verksamhet i form av bedrägerier genom elektroniska kommunikationstjänster. Sådana handlingar antas motverkas genom att tillhandahållare av allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster avstår från att överföra vissa elektroniska meddelanden. Att elektroniska meddelanden som kan antas överföras som ett led i ett bedrägeri inte överförs förväntas leda till färre anmälningar om sådan brottslighet. Det skulle innebära minskade kostnader för handläggning och utredning av ärendetypen inom Polismyndigheten, Åklagarmyndigheten och de allmänna domstolarna.

Förslagen innebär att PTS kommer att genomföra tillsyn av skyldigheten att inte överföra elektroniska meddelanden som överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare. Under 2024 meddelade de allmänna förvaltningsdomstolarna ett begränsat antal avgöranden till följd av överklaganden av PTS tillsynsbeslut. Det saknas skäl att anta att tillsynen över de föreslagna bestämmelserna skulle föranleda mer än ett fåtal förvaltningsbeslut som överklagas per år. Antalet överklagade beslut till följd av förslagen förväntas därför inte innebära mer än marginella kostnadsökningar för de allmänna förvaltningsdomstolarna. Kostnadsökningarna bedöms rymmas inom befintliga anslag.

9.5 Konsekvenser för enskilda och samhället i övrigt

Bedrägerier genom elektroniska kommunikationstjänster drabbar både företag och privatpersoner. Brottsoffren påverkas såväl ekonomiskt som psykosocialt, t.ex. i form av förlorat sparkapital och en minskad tilltro till den digitala utvecklingen. Bedrägerierna medför även stora kostnader för näringslivet. Att åtgärder enligt förslagen vidtas för att motverka att elektroniska kommunikationstjänster används för att genomföra bedrägerier förväntas därför få positiva samhällsekonomiska effekter.

Förslagen innebär att det överlämnas till tillhandahållarna att bestämma vilka åtgärder i den egna verksamheten som krävs för att uppfylla skyldigheten. Det kan finnas en risk att elektroniska meddelanden stoppas från att överföras trots att de inte överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare. Detta skulle i sådana fall kunna få negativa konsekvenser för enskilda och samhället i övrigt. Risken för att det skulle inträffa framstår dock som låg med hänsyn till tillgången till tekniska lösningar och automatiserade kontroller. Tillhandahållarna får inte heller vidta åtgärder som strider mot bestämmelserna om behandling av trafikuppgifter och integritetsskydd i 9 kap. LEK. Vidare kommer PTS att bedriva tillsyn över efterlevnaden av skyldigheten att i vissa fall inte överföra elektroniska meddelanden som nu föreslås. Myndigheten kommer därmed att kunna granska de förfaranden som används till följd av skyldigheten. Förslagen bedöms mot denna bakgrund vara proportionerliga.

Eftersom det inte kan uteslutas att även andra meddelanden hindras från att överföras skulle frågor om förhållandet till yttrande- och informationsfrihet kunna aktualiseras. Den eventuella inskränkning av dessa fri- och rättigheter som förslagen i detta avseende skulle kunna innebära bedöms dock vara proportionerlig i förhållande till syftet med förslagen (jfr 2 kap. 20 § första stycket 1, 2 kap. 21 §, 2 kap. 23 § regeringsformen och artikel 10 i Europakonventionen för de mänskliga rättigheterna och de grundläggande friheterna).

Förslagen innebär också att tillhandahållare, under vissa förutsättningar, får behandla trafikuppgifter för att fullgöra skyldigheten att i vissa fall inte överföra elektroniska meddelanden. Den ökade behandlingen av trafikuppgifter kan innebära en ökad risk för intrång i den personliga integriteten. Uppgifterna får dock endast behandlas i den utsträckning och under den tid som är nödvändig för ändamålet och ska därefter genast utplånas. Tillhandahållarna får vidare inte vidta åtgärder i strid med övriga regler om personuppgiftsbehandling och integritetsskydd i bl.a. 9 kap. LEK.

Förslagen förväntas motverka bedrägerier och annat vilseledande och därmed skydda enskilda från att bli utsatta för en viss typ av brottslighet. Förslagen bedöms alltså leda till en ökad trygghet för enskilda. Sammantaget anses förslagen innebära en rimlig avvägning mellan behovet av att motverka brottslighet och den enskildes rätt till skydd för sin personliga integritet.

Om ett register för avsändarnamn för sms inrättas kommer registret att finansieras genom att en anmälningsavgift och en årlig avgift tas ut från den som anmäler ett avsändarnamn för sms till registret. Det innebär i sådana fall en ökad kostnad för de företag och andra aktörer som väljer att anmäla avsändarnamn för sms. Anmälan till registret är dock frivillig. Kostnaden för registreringen bedöms vara proportionerlig i förhållande till de fördelar som anmälningen till registret kan innebära för företag och andra aktörer.

Förslagen innebär ingen inskränkning av den kommunala självstyrelsen. De innebär inte heller några förändringar av kommunala befogenheter eller skyldigheter eller av grunderna för kommunernas eller regionernas organisation eller verksamhetsformer.

9.6 Övriga konsekvenser

Förslagen bedöms inte medföra några konsekvenser för hållbarhet eller jämställdheten mellan män och kvinnor.

Förslagen står i överensstämmelse med EU-rätten.

10 Författningskommentar

Förslaget till lag om ändring i lagen (2022:482) om elektronisk kommunikation

4 kap.

12 § En tillhandahållare av en allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst ska inte överföra ett elektroniskt meddelande om den har anledning att anta att meddelandet överförs

1. som ett led i ett bedrägeri, eller

2. i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om skyldighetens omfattning.

Paragrafen, som är ny, innebär en skyldighet för vissa tillhandahållare att inte överföra ett elektroniskt meddelande om tillhandahållaren har anledning att anta att det överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare. Paragrafen genomför delvis artikel 97.2 i kodexen för elektronisk kommunikation tillsammans med 4 kap. 11 § LEK. Övervägandena finns i avsnitt 5.

Skyldigheten i *första stycket* att i vissa fall inte överföra ett elektroniskt meddelande riktar sig mot den som tillhandahåller en allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst. Vad som avses med elektroniskt meddelande och nummerbaserad interpersonell kommunikationstjänst definieras i 1 kap. 7 § LEK. Begreppet elektroniskt meddelande definieras som all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst. Information som överförs som en del av sändningar av ljudradio- och tv-program som är riktade till allmänheten via ett elektroniskt kommunikationsnät omfattas dock inte, om inte denna information kan sättas i samband med den enskilda abonnenten eller användaren av informationen (se prop. 2021/22:136 s. 407 och prop. 2002/03:110 s. 248–250 och 389–390). Avgränsningen till den som tillhandahåller en allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst innebär att bestämmelsen är tillämplig på samtal, sms och andra standarder för textmeddelanden, t.ex. mms och RCS-meddelanden. Bestämmelsen är däremot inte tillämplig på e-post eller text- eller röstmeddelanden som utbyts genom en webbaserad applikation som inte möjliggör kommunikation med nummer i en nationell eller internationell nummerplan.

Ett elektroniskt meddelande ska inte överföras om den som tillhandahåller den elektroniska kommunikationstjänsten har anledning att anta att meddelandet överförs som ett led i ett bedrägeri eller i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare. Att ett elektroniskt meddelande inte ska överföras innebär att det ska stoppas innan det når den avsedda mottagaren av meddelandet, dvs. att ett samtal inte kopplas fram eller att ett sms inte levereras. Med mottagare avses den slutanvändare som vid en överföring tar emot det elektroniska meddelandet. Slut användare definieras i 1 kap. 7 § som användare som inte tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunika-

tionstjänster. En slutanvändare kan därmed vara en konsument likaväl som ett företag, en organisation eller en offentlig aktör (se prop. 2021/22:136 s. 410 och prop. 2002/03:110 s. 361).

Vid tillämpningen av denna paragraf avser bedrägeri en handling som omfattas av bedrägeribrotten enligt 9 kap. 1 § första stycket och 2–3 §§ brottsbalken. Bestämmelsen omfattar även en handling som utgör ett led i ett försök till ett sådant brott. Någon kan t.ex. skicka sms i syfte att förmå mottagaren att klicka på skadliga länkar eller lämna bank- eller personuppgifter, vilket skulle leda till vinning för bedragaren och skada för mottagaren.

Bestämmelsen omfattar även annat vilseledande som inte är ett led i ett bedrägeri, förutsatt att det elektroniska meddelandet överförs i syfte att vilseleda en vidare krets av mottagare. Det innebär att meddelandet ska syfta till att vilseleda ett större antal mottagare. Flera elektroniska meddelanden som riktar sig till samma mottagare omfattas alltså inte. Inte heller omfattas elektroniska meddelanden som syftar till att vilseleda ett fåtal mottagare. Det kan både vara fråga om initierad överföring av ett och samma meddelande till ett stort antal mottagare och flera meddelanden där överföringen har initierats var för sig men där meddelandena ändå ingår i samma vilseledande förfarande.

Som exempel på elektroniska meddelanden som överförs i syfte att, på något annat sätt, vilseleda en vidare krets av mottagare kan nämnas förfaranden där en stor mängd personer lockas eller luras att ringa ett utlands- eller satellitnummer med mycket hög taxa, exempelvis wangirisamtal (jfr prop. 2021/22:136 s. 176–178 och 429 och prop. 2010/11:115 s. 112–118 och 186–188). Det kan t.ex. också vara fråga om sms som skickas till en vidare krets i syfte att sprida desinformation, där avsändarnamnet är vilseledande så att det framstår som att det kommer från en viss myndighet eller att det är ett meddelande enligt lagen (2023:407) om viktigt meddelande till allmänheten.

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 (se bl.a. prop. 2021/22:136 s. 499–502, 504, 507–509, prop. 2018/19:86 s. 91–98 och prop. 2002/03:110 s. 389–397). Enligt 9 kap. 6 a § får tillhandahållaren behandla trafikuppgifter i syfte att fullgöra skyldigheten att inte överföra vissa meddelanden enligt denna paragraf, se författningskommentaren till den paragrafen. Bestämmelserna i 9 kap. LEK innebär bl.a. att tillhandahållaren är förhindrad att granska innehållet i meddelandena. Kontrollen får därför grundas i andra omständigheter.

En tillhandahållare kan t.ex. ha 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 om det finns tecken på att det presenterade numret har manipulerats eller att avsändarnamnet är

vilseledande. Ett sådant tecken kan exempelvis vara att ett sms med avsändarnamn skickas från en annan tillhandahållare av sms-aggregatörs-tjänster än den som har registrerats för avsändarnamnet i ett register för avsändarnamn för sms. Vissa trafikmönster kan också ge tillhandahållaren anledning att göra ett sådant antagande. En förutsättning är att det rör sig om ett avvikande trafikmönster som indikerar att överföringen har initierats med ett bedrägligt eller vilseledande syfte. Enbart omständigheten att någon ringer upprepade samtal innebär inte i sig att det rör sig om ett sådant avvikande trafikmönster som ger anledning att anta att överföringen görs som i ett sådant syfte. Inte heller att en avsändare skickar sms till en vidare krets av mottagare innebär i sig ett sådant avvikande trafikmönster. Om tillhandahållaren däremot registrerar sådana avvikelser i trafikmönster som indikerar att ett meddelande exempelvis är ett wangirisamtal, har tillhandahållaren anledning att anta att omständigheterna är sådana att meddelandet inte ska överföras.

Bestämmelsen i *andra stycket* gör det möjligt att meddela ytterligare föreskrifter om omfattningen av skyldigheten att inte överföra elektroniska meddelanden som överförs som ett led i ett bedrägeri eller syftar till att, på något annat sätt, vilseleda en vidare krets av mottagare enligt första stycket. Det kan exempelvis avse föreskrifter att tillhandahållare ska kontrollera viss information i samband med överföringen av ett elektroniskt meddelande.

9 kap.

6 a § *Trafikuppgifter får behandlas om uppgifterna behövs vid åtgärder som krävs för att fullgöra skyldigheten i 4 kap. 12 §. Uppgifterna får behandlas endast i den utsträckning och under den tid som är nödvändig för ändamålet. De ska där- efter genast utplånas.*

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

- 1. vilka uppgifter som får behandlas enligt första stycket, och*
- 2. hur länge uppgifterna får behandlas innan de ska utplånas.*

Paragrafen, som är ny, gör det möjligt för tillhandahållare av nummerbaserade interpersonella kommunikationstjänster att behandla trafikuppgifter om det behövs för att fullgöra skyldigheten att inte överföra elektroniska meddelanden i vissa fall. Övervägandena finns i avsnitt 7.

Tillhandahållare av nummerbaserade interpersonella kommunikations-tjänster får enligt *första stycket* behandla trafikuppgifter om uppgifterna behövs vid åtgärder som krävs för att fullgöra skyldigheten att inte överföra elektroniska meddelanden enligt 4 kap. 12 §, se författningskommen-taren till den paragrafen. Begreppet trafikuppgift definieras i 1 kap. 7 § som en uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande (se prop. 2021/22:136 s. 322–325 och 411 och prop. 2002/03:110 s. 248–250 och 389–390).

I bestämmelsen regleras vidare i vilken omfattning som uppgifterna får behandlas. Behandlingen ska vara tillåten endast i den utsträckning och under den tid som är nödvändig för ändamålet. Det innebär att trafikuppgifter får behandlas i den utsträckning som det är nödvändigt för att vidta

åtgärder som krävs för att avgöra om det finns 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. Uppgifterna kan också behandlas om det exempelvis behövs för blockeringsåtgärden. Uppgifterna får inte behandlas för något annat ändamål än att vidta åtgärder för att fullgöra skyldigheten i 4 kap. 12 §. Efter den tillåtna behandlingen ska uppgifterna genast utplånas.

Andra stycket gör det möjligt för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om vilka uppgifter som får behandlas och om hur länge det får göras innan uppgifterna ska utplånas. Sådana föreskrifter kan exempelvis avse vilka trafikuppgifter som får behandlas vid olika typer av åtgärder och yttersta tidsgränser för behandlingen.

27 § Utöver vad som anges i 1–3, 6 a och 31 §§ får inte någon annan än berörda användare ta del av eller på något annat sätt behandla uppgifter i ett elektroniskt meddelande som överförs i ett allmänt elektroniskt kommunikationsnät eller med en allmänt tillgänglig elektronisk kommunikationstjänst, eller trafikuppgifter som hör till detta meddelande, om inte någon av användarna har samtyckt till behandlingen.

Detta hindrar inte

1. lagring som är automatisk, mellanliggande och tillfällig, om den är nödvändig för överföring av ett elektroniskt meddelande, eller sådan lagring i den utsträckning som den är nödvändig för driften av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst,

2. att andra får tillgång till innehållet i ett elektroniskt meddelande, om innehållet ändå är allmänt tillgängligt, om tillgången ges endast för att effektivisera den fortsatta överföringen till andra mottagare samt om uppgifterna om vem som har begärt att få informationen utplånas, eller

3. att någon i en radiomottagare avlyssnar eller på något annat sätt, genom att använda en sådan mottagare, får tillgång till ett radiobefordrat elektroniskt meddelande som inte är avsett för denne eller för allmänheten.

Paragrafen reglerar hur uppgifter i elektroniska meddelanden får behandlas. Övervägandena finns i avsnitt 7.

Paragrafen genomför artiklarna 5.1 och 5.2 i e-dataskyddsdirektivet (se prop. 2021/22:136 s. 507 och prop. 2002/03:110 s. 252–255 och 395–396). I *första stycket* läggs det till en hänvisning till 6 a § till följd av möjligheten till behandling av trafikuppgifter som införs i den paragrafen.