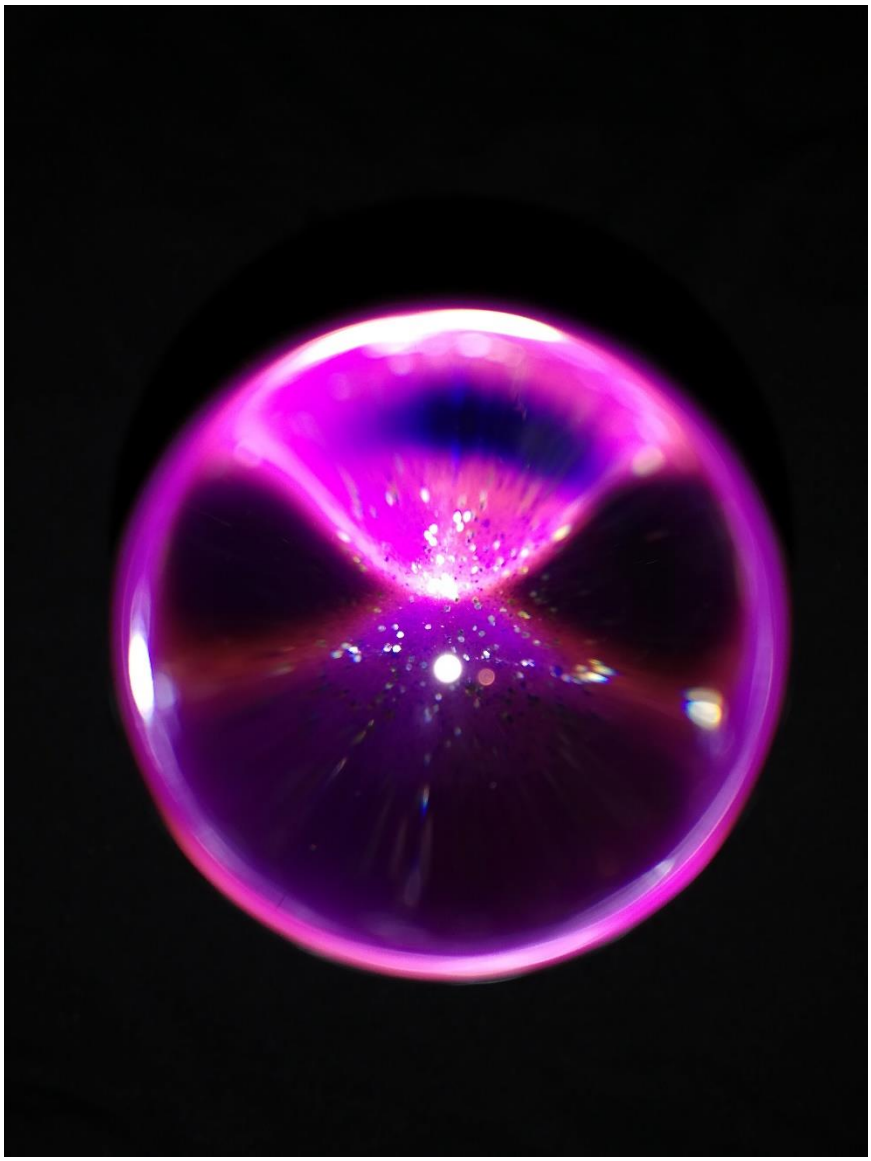
Delredovisning - Att motverka tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier

Regeringsuppdrag



PTS

Innehåll

1. Sammanfattning

PTS fick i december 2023 ett uppdrag[1] att kartlägga användningen av elektroniska kommunikationstjänster vid bedrägerier samt lämna förslag till åtgärder för att förhindra manipulering av telefonnummer, s.k. spoofing, och andra tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier.

I denna delredovisning fokuserar Post- och telestyrelsen (PTS) på att redovisa resultatet och slutsatserna av den kartläggning som hittills har genomförts. Dessutom redovisas befintliga regelverk och pågående åtgärder inom området. Vidare redovisas de avgränsningar PTS gjort av begreppet elektroniska kommunikationstjänster för att därmed ge inblick i vilka av dessa tjänster som myndigheten avser lämna åtgärdsförslag till i den kommande slutredovisningen.

PTS ser att bedragarna ändrar tillvägagångssätt mycket snabbt. När något förbjuds eller görs krångligare så ”flyttar” brottsligheten och använder sig av nya tekniska tillvägagångsätt eller andra typer av elektroniska kommunikationstjänster. Detta bidrar till svårigheter att vidta lämpliga rättsliga åtgärder för att hindra bedrägerier där elektroniska kommunikationstjänster är en del av händelsekedjan. PTS konstaterar att möjligheterna att inom myndighetens verksamhetsområde föreslå åtgärder mot olika typer av bedrägerier är begränsade till de fall där en elektronisk kommunikationstjänst utgör ett verktyg för bedragaren.

De bedrägerier som ses som de största problemen i dag är de som sker med stöd av någon form av elektroniska kommunikationstjänster, i vissa fall även genom sociala medietjänster och där e-legitimering, som t.ex. BankID, ingår i händelsekedjan, såsom;

- Bedrägerier med stöd av sms, meddelandeappar och e-post
- Telefonbedrägerier, inkl. wangirisamtal
- Kortbedrägerier
- Romansbedrägerier
- Investeringsbedrägerier

Ramar för uppdraget sätts genom definitionen av begreppet bedrägeri. PTS har därför valt att fokusera på sådana elektroniska kommunikationstjänster som kan

[1] Fi2023/03206.

användas som verktyg för brottet bedrägeri och som riktar sig direkt till slutanvändare.

Exempel på sådana tjänster är nummerbaserade talkommunikationstjänster, nummerbaserade sms, nummeroberoende tal- och meddelandetjänster (OTT[2]-tjänster) samt e-post.

Ett antal åtgärder har genomförts i Sverige för att förhindra samtal med manipulerade telefonnummer. PTS har i samverkan med operatörer och Telekområdgivarna tagit fram en vägledning[3] som vänder sig till operatörer. Vägledningen går i korthet ut på att stoppa internationella samtal till Sverige som utger sig att komma från svenska telefonnummer.

PTS har även, med stöd av befintliga bemyndiganden i förordningen (2022:511) om elektronisk kommunikation (FEK), tagit fram förslag till föreskrifter och allmänna råd som ersätter vägledningen. De föreslagna föreskrifterna kan förväntas träda ikraft i slutet av 2024. Som bemyndigandet är utformat gäller det dock endast för krav som ska ställas på en talkommunikationstjänst.

I kartläggningen har det framkommit att s.k. bluff-sms är ett av de vanligast förekommande verktygen för bedrägerier just nu. En stor del av problemen kring bluff-sms rör möjligheten att använda s.k. alfanumeriska avsändarnamn. PTS ser att det saknas uttryckliga bestämmelser som reglerar sms. PTS ser dock att en ändring av LEK och FEK skulle vara en möjlig väg att reglera detta område.

PTS kan konstatera att många länder i likhet med Sverige har vidtagit åtgärder eller planerar att genomföra åtgärder för att förhindra bedrägerier där PTS sektors tjänster används.

En annan slutsats av kartläggningen är att användningen av OTT-tjänster samt artificiell intelligens (AI) som hjälpmedel vid bedrägerier ser ut att öka och bli vanligare förekommande i framtiden.

Det kan slutligen noteras att det finns behov av ökad samordning vad gäller informationsspridning från myndigheter, organisationer och företag om bedrägerier och hur slutanvändaren kan minska risken att bli utsatt.

PTS ser att det inom ramen för uppdraget främst kan bli aktuellt att tillämpa lagen (2022:482) om elektronisk kommunikation.

[2] Over-the-top.
[3] Vägledning för tillhandahållare (pts.se)

2. Inledning

2.1 Uppdraget från regeringen

PTS fick i december 2023 ett uppdrag[4] att kartlägga användningen av elektroniska kommunikationstjänster vid bedrägerier samt lämna förslag till åtgärder för att förhindra manipulering av telefonnummer, s.k. spoofing, och andra tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier.

PTS ska senast den 31 maj 2024 delredovisa uppdraget till Regeringskansliet (Finansdepartementet) och senast den 31 december 2024 ska uppdraget slutredovisas.

2.2 Delredovisningens innehåll

I delredovisningen har PTS fokuserat på att beskriva den information som har framkommit under den kartläggning bland svenska aktörer som myndigheten hittills har genomfört.[5]

Kartläggningen inkluderar även en litteraturgenomgång av konsultstudier, utredningar, rapporter från bl.a. olika säkerhetsföretag verksamma inom sektorn elektroniska kommunikationer, lagtexter, och andra offentligrättsliga dokument av intresse för området.

Användningen av elektroniska kommunikationstjänster vid olika typer av bedrägerier kan spänna över ett brett spektrum av tjänster och PTS har därför gjort vissa avgränsningar som framgår av denna delredovisning.

PTS ska lämna förslag till åtgärder för att förhindra tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier. Av denna delredovisning framgår de åtgärder myndigheten har genomfört och för närvarande genomför kopplat till telefonbedrägerier genom ett pågående föreskriftsarbete.

[4] Fi2023/03206.

[5] Polismyndigheten, Konsumentverket, Svenska Bankföreningen, Tech Sverige, Brå, Telia Company, Tele2, Leissner Data, 3, Internetstiftelsen, Telekområdgivarna, Sinch och SKPF Pensionärerna.

Vidare berörs övergripande bedrägerier med hjälp av sms, vilket är ett område som särskilt lyfts fram i kartläggningen.

2.3 Elektroniska kommunikationstjänster enligt kodexen

Elektroniska kommunikationstjänster, som det är beskrivet i kodexen[6], är uppdelat i tre områden; internetanslutningstjänster, interpersonella kommunikationstjänster och tjänster som utgörs helt eller delvis av överföring av signaler. Beskrivningen nedan är inte fullständig utan exemplifierar några tjänster som är relevanta i det här sammanhanget.

- **Internetanslutningstjänster** – innefattar tjänster som ger tillgång till internet.
- **Interpersonella kommunikationstjänster** - är uppdelade i nummerbaserade- och nummeroberoende interpersonella kommunikationstjänster. De nummerbaserade tjänsterna är sådana som tillhandahålls genom ett telefonnummer som t.ex. traditionella telefonsamtal och sms, men även samtal via OTT-tjänster såsom t.ex. Microsoft Teams-telefon där kommunikationen kan göras med hjälp av telefonnummer. De nummeroberoende tjänsterna är sådana där kommunikationen sker utan inblandning av ett telefonnummer såsom e-post, OTT-tjänster för tal- och meddelandeappar som t.ex. Facebook Messenger och WhatsApp.
- **Tjänster som utgörs helt eller huvudsakligen av överföring av signaler** – under denna kategori hamnar t.ex. tjänster där maskiner kopplas samman med varandra (M2M/IoT-kommunikation) och rundradio.

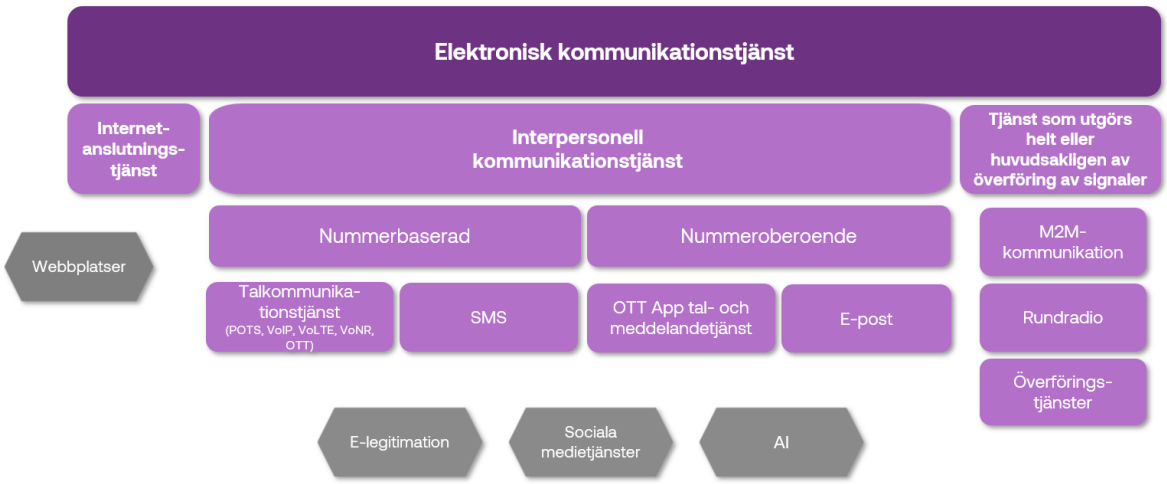
Tjänster i form av tillhandahållande av innehåll som överförts med hjälp av elektroniska kommunikationsnät och kommunikationstjänster eller tjänster som innebär utövande av redaktionellt ansvar över sådant innehåll är i artikel 2.4 i kodexen (EU) 2018/1972 undantagna från definitionen av elektronisk kommunikationstjänst. Rena innehållstjänster, som programverksamheten hos vissa programföretag för radio och tv och innehållstjänster som tillhandahålls via internet, och tjänster som innebär utövande av redaktionellt ansvar över sådant innehåll faller således utanför definitionen.[7]

Bestämmelserna i EU-direktivet har genomförts i svensk rätt genom lagen om elektronisk kommunikation. Av 1 kap. 7 § nämnda lag följer att definitionen av elektronisk kommunikationstjänst i lagen nära följer ordalydelsen i EU-direktivet.

[6] Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning)Text av betydelse för EES.
[7] Prop. 2021/22:136 s. 406.

En elektronisk kommunikationstjänst kan alltså vara av tre slag enligt ovan som delvis kan överlappa varandra. En grundläggande förutsättning är att tjänsten vanligen tillhandahålls mot ersättning. Tjänsten ska alltså tillhandahållas kommersiellt. Sker tillhandahållandet på rent ideell basis omfattas tjänsten inte av definitionen, t.ex. forskarnät eller andra nät inom universitetsvärlden. I vissa fall tillhandahålls kommersiella tjänster gratis till slutkunden. Det kommersiella inslaget manifesteras då på något annat sätt, t.ex. genom att tjänsten är reklamfinansierad. Kravet på tillhandahållande mot ersättning bör anses vara uppfyllt även i andra fall när tillhandahållaren får betalt av tredje part och inte av slutkunden, t.ex. om tillhandahållaren tjänar pengar på personuppgifter eller andra data som samlas in vid användningen av tjänsten.[8]

I bilden nedan illustreras även webbplatser, e-legitimation, sociala medietjänster och AI som inte anses utgöra elektroniska kommunikationstjänster men som ofta används i samband med bedrägerier med elektroniska kommunikationstjänster.



Figur 1: Elektroniska kommunikationstjänster enligt kodexen samt andra tjänster som inte omfattas (sexkantiga figurer).

[8] Prop. 2021/22:136 s. 406, se även skäl 16 i direktivet 2018/1972.

2.4 Vissa uttryck i delredovisningen

I denna redovisning använder myndigheten några uttryck som används av aktörerna utan att de direkt finns i PTS tillämpbara regelverk. Nedan beskrivs kort vissa uttryck som används i redovisningen.

Alfanumeriskt avsändarnamn för sms

Ett alfanumeriskt avsändarnamn för sms är en uppgift om avsändare, t.ex. ett varumärke eller en bank, som visas för mottagaren i form av bokstäver, siffror eller andra tecken. Dessa sms skickas via ett applikationskonto anslutet via en mobiloperatör, eller via en sms-aggregatör som erbjuder distribution till många mottagare i flera mobilnät. Avsändaren kan välja att ange avsändarnamn bestående av bokstäver och siffror ur teckenuppsättningen för sms. I vissa fall gäller en begränsning till tecknen 0-9 och a-Z. Ibland används även benämningen alfanumerisk avsändarID och den engelska termen SMS SenderID är också vanligt förekommande.

Bedrägerier

Begreppet bedrägeri har i denna rapport samma betydelse som i brottsbalken, se vidare i avsnitt 3.

Elektroniska kommunikationstjänster

Begreppet elektroniska kommunikationstjänster är definierat i 1 kap. 7 § lagen (2022:482) om elektronisk kommunikation (LEK).

Digitala tjänster

Uttrycket digitala tjänster används t.ex. i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen).

I rättsakten om en inre marknad för digitala tjänster (*Digital Services Act*, DSA)[9] används ordet förmedlingstjänst, vilket inkluderar även vissa elektroniska kommunikationstjänster.

OTT-tjänster

OTT-tjänster används i den här delredovisningen såsom Body of European Regulators for Electronic Communications (Berec) har definierat det i en rapport[10]

[9] Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG.

[10] *Report on OTT services*. Berec. https://www.berec.europa.eu/sites/default/files/files/document_register_store/2016/2/BoR_%2816%29_35_Report_on_OTT_services.pdf. Hämtat 2024-03-12.

med följande betydelse; ”innehåll, en tjänst eller applikation som tillhandahålls till slutanvändaren över det öppna internet”. Vissa typer av OTT-tjänster utgör en underkategori till kodexens begrepp nummeroberoende interpersonella kommunikationstjänster.

Phishing, smishing och vishing

Vid bedrägerier med inblandning av elektroniska kommunikationstjänster förekommer olika uttryck för de kontaktskapande momenten som tjänsterna används för, t.ex. phishing, smishing och vishing. Begreppen är ofta förekommande internationellt och har använts i rapporter från bl.a. Myndigheten för samhällsskydd och beredskap (MSB) och Brottsförebyggande rådet (Brå).

- Phishing (av Password fishing, lösenordsfiske) är en benämning av kontaktförsök via elektronisk kommunikation, huvudsakligen e-post, i bedrägligt syfte.
- Vishing (av Voice phishing) är en benämning på ett samtal för att inleda kontakt och bygga upp förtroende inför genomförande av bedrägerier. Det är inte ovanligt att den som ringer upp utger sig för att vara t.ex. polis eller kompis till barnbarn. Ofta kombineras förfarandet med manipulerat uppringande telefonnummer (spoofing) och ibland även med fysiska besök (fysisk vishing), oftast hos äldre personer.
- Smishing (av sms phishing, hädanefter bluff-sms) är en benämning på kontaktskapande bluff-sms som ofta förekommer som första kontakt. Bluff-sms kan innehålla telefonnummer till en falsk kundtjänst, eller en länk som leder till allt från mindre seriösa annonser till lösenordsfiske eller installation av skadlig programvara eller i syfte att inhämta personuppgifter. För att öka trovärdigheten bakom bluff-sms används ofta alfanumeriskt avsändarnamn som liknar eller imiterar en känd avsändare.

Spoofing

Begreppet spoofing används ibland i vid bemärkelse som benämning på olika slags bedrägerier som sker via telefon eller andra elektroniska kommunikationstjänster (t.ex. sms och e-post). I denna delredovisning begränsas innebörden av begreppet spoofing till telefonsamtal, där den som ringer upp manipulerar det telefonnummer som visas för den som blir uppringd. På så sätt kan den anropande abonnenten vilseleda den som blir uppringd, och få det att se ut som att samtalet kommer från någon annan än det faktiskt gör, t.ex. från en bank[11].

[11] https://www.europol.europa.eu/sites/default/files/documents/1_spoofed_bank_websites.pdf.

Wangirisamtal

Wangirisamtal[12] innebär att den som ringer upp lägger på efter bara en signal. Syftet är att få den som blivit uppringd att ringa tillbaka. Numret som ringer är ofta ett högkostnadsnummer (främst internationella telefonnummer) vilket gör det dyrt att ringa tillbaka. Olika röstmeddelanden läses ofta upp för att den som ringer tillbaka ska vara kvar i samtalet så länge som möjligt.

3. Bedrägerier genom elektroniska kommunikationstjänster

Den ekonomiska brottligheten utgör ett allvarligt samhällsproblem och enligt uppdraget till PTS är en av regeringens mest prioriterade frågor att motverka brottslighet. Bedrägerier är en allt viktigare finansieringskälla för den organiserade brottsligheten och regeringen anger i uppdraget att en central åtgärd är att motverka bedrägerier där elektroniska kommunikationstjänster används. Både den ökade digitaliseringen och globaliseringen är en förutsättning för många av bedrägerierna där elektroniska kommunikationstjänster används i allt större utsträckning, tillsammans med e-legitimeringstjänster.

Brottet bedrägeri regleras i 9 kap. 1-3 §§ brottsbalken. Av 9 kap 1 § brottsbalken framgår att den som medelst vilseledande förmår någon till handling eller underlåtenhet, som innebär vinning för gärningsmannen och skada för den vilseledde eller någon i vars ställe denne är, dömes för bedrägeri till fängelse i högst två år. För bedrägeri döms också den som genom att lämna oriktig eller ofullständig uppgift, genom att ändra i program eller upptagning eller på annat sätt olovligen påverkar resultatet av en automatisk informationsbehandling eller någon annan liknande automatisk process, så att det innebär vinning för gärningsmannen och skada för någon annan.

[12] https://www.europol.europa.eu/sites/default/files/documents/wangiri_final_2.pdf.

När ordet bedrägeri används i denna rapport är det den legala definitionen som avses. Genom definitionen begränsas arbetet till att omfatta just den typ av brottslighet som syftar till att vilseleda någon för egen vinning.

Bedrägerier som genomförs över elektroniska kommunikationsnät och tjänster kan ske på olika sätt, i olika nivåer i nätet och tjänsterna. För att elektroniska kommunikationstjänster ska fungera mellan mottagare och avsändare krävs för respektive tjänst i regel en standardiserad och särskild identitet i näten i båda leden hos båda parter, t.ex. telefonnummer, IP-adress m.m. för att kunna identifiera mottagaren och avsändaren. För flera elektroniska kommunikationstjänster saknas det inbyggda funktioner eller mekanismer för att säkerställa riktighet eller autenticitet i de behandlade uppgifterna, såsom den särskilda identiteten i näten för avsändare respektive mottagare i kommunikationen.

När det gäller olika bedrägerier som kan genomföras över elektroniska kommunikationstjänster är ett tillvägagångssätt att avsändarnamn, t.ex. såsom telefonnummer och IP-adresser, har manipulerats. En annan typ av bedrägeri med koppling till elektroniska kommunikationstjänster är att presentation av avsändaridentiteten har manipulerats gentemot mottagaren (t.ex. vid bluff-sms och samt nummerpresentation vid samtal i mobiltelefon). Ovanpå dessa typer av bedrägerier tillkommer en sista del av social manipulation som genomförs över sms, telefonsamtal, e-post etc. där mottagaren uppmanas att utföra något särskilt, exempelvis klicka på en länk, lämna personuppgifter eller legitimera sig med t.ex. BankID.

Det område där elektroniska kommunikationstjänster kan användas för bedrägerier är således stort och gör arbetet kring åtgärder för att förhindra sådana typer bedrägerier både omfattande och komplext.

De aktörer som PTS har intervjuat delar bilden av att tillvägagångssätten för bedrägerier kan ändras mycket snabbt. När något förbjuds eller blir krångligare att genomföra reagerar bedragarna snabbt och hittar andra lösningar.

I samtal med ett antal myndigheter och företrädare för flera olika operatörer och organisationer har det framkommit att de bedrägerier som ses som de största problemen i dag är bedrägerier som sker med stöd av någon form av elektroniska kommunikationstjänster, i vissa fall även genom sociala medietjänster, och oftast också tillsammans med e-legitimation som t.ex. BankID för att genomföra själva bedrägeriet. De vanligaste är, i fallande ordning:

- Bedrägerier med stöd av sms, meddelandeappar och e-post samt genom sociala medietjänster
- Telefonbedrägerier, inkl. wangirisamtal

- Kortbedrägerier
- Romansbedrägerier
- Investeringsbedrägerier

I flera av dessa bedrägerier ligger stora delar av brottet och tillvägagångsättet av naturliga skäl utanför PTS regleringsområde. Dock kan flera olika elektroniska kommunikationstjänster användas för att underlätta och bidra till framgång i bedrägeriet.

Några aktörer har framfört synpunkter om individens eget ansvar i samband med bedrägerier.

PTS kan konstatera att ett kommande stort problem kan utgöra s.k. AI-bedrägerier. I och med att det blivit mycket enklare att förfalska både röster, bilder och texter så att de blir ytterst lika originalen kommer bedragare att få ytterligare verktyg för att genomföra mycket svårgenomskådliga bedrägerier.

3.1 Bedrägeri via sms, meddelandeappar, e-post och sociala medietjänster

Vid dessa bedrägerier kontaktar bedragaren brottsoffret via sms, meddelandeappar, e-post eller sociala medier och lurar denne att genomföra en transaktion eller att lämna ifrån sig kort- eller personuppgifter.[13] Dessa bedrägerier har många likheter med telefonbedrägerierna.

När brottsoffren kontaktas kan det ske genom att bedragaren utger sig för att vara någon annan, t.ex. från banken eller från polisen, antingen genom att skicka sms eller e-post med snarlika eller kopierade e-postadresser eller via kapade sociala mediekonton. Avseende bluff-sms så finns i dag möjlighet att sända sms med falska alfanumeriska avsändarnamn, så att det ser ut som att sms:et kommer från t.ex. kundens bank. Idag är det enkelt att förfalska ett alfanumeriskt avsändarnamn i ett sms genom tjänster på nätet. Ett falskt alfanumeriskt avsändarnamn medför bl.a. att bluff-sms:et ser mer trovärdigt ut, men medför även att i den mottagande telefonen kommer själva sms:et att placera sig bland övriga icke manipulerade sms från t.ex. samma bank eller e-handelsföretag för att på så sätt ge sken av äkthet. Det förekommer också andra former av bluff-sms där bedragaren t.ex. utger sig för att vara mottagarens barn eller barnbarn som behöver pengar snabbt.

Bedragarens meddelanden innehåller ofta en länk eller ett telefonnummer som offret luras att klicka på eller att ringa till. Syftet är att antingen komma åt konto-, kort- eller

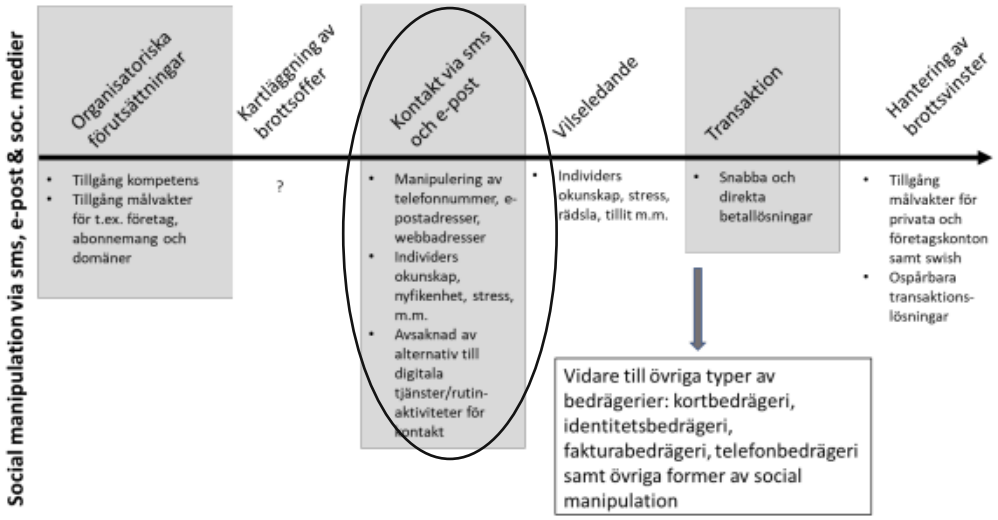
[13] Brå rapport 2023:11, *Bedrägerier mot privatpersoner*, s 27.

inloggningsuppgifter, eller att placera en skadlig kod på personens dator eller telefon för att senare få tag i t.ex. lösenord. Meddelandet kan även vara ett första steg i ett telefonbedrägeri eller ett kortbedrägeri.[14]

E-postmeddelanden med erbjudanden om belöningar[15] och vinster eller hot förekommer fortfarande, men har minskat i samband med bättre och förfinade spam-filter och större medvetenhet hos mottagarna. Även fakturabedrägerier förekommer och består i sin enklaste form av en e-postfaktura. Tidigare har fakturering av falska eller bedrägligt utformade tjänster till småföretag varit vanligt, ofta under semestertider. En uppmaning till betalning kan också kompletteras med personanpassad bakgrundshistoria, spoofade telefonsamtal, bluff-sms eller imitation av beslutsfattare (exempelvis chef eller firmatecknare). Internationellt har även imitation med hjälp av AI-genererade röster börjat förekomma och kan troligen förväntas öka även i Sverige. Betalning av bluffakturor sker ofta till ett s.k. målvaktskonto, där pengarna sedan överförs i flera steg för att försvåra spårning av betalningen.

Bedrägerier med falska fakturor i kombination med kartläggning av brottsoffer och i kombination med andra tjänster för att öka trovärdighet är potentiellt ett fortsatt problem.

[14] Brå rapport 2023:11, *Bedrägerier mot privatpersoner*, s 27.
[15] Går ofta under benämningen Nigeriabrev, https://www.minuc.se/id-stold/vad-ar-nigeriabrev.



Figur 2: Händelsekedja - bedrägeri via sms, meddelandeappar, e-post och sociala medietjänster.[16] Figur från Brå:s rapport med en ring, tillagd av PTS, som markerar i vilken del av händelsekedjan som elektroniska kommunikationstjänster används.

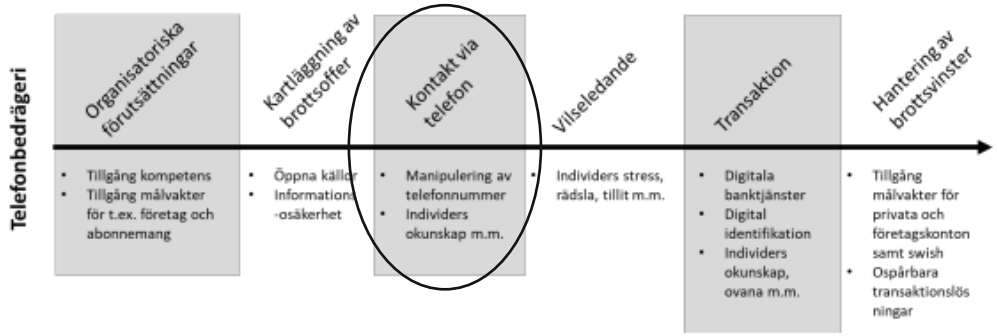
3.2 Telefonbedrägerier inkl. wangirisamtal

Vid telefonbedrägerier kontaktas brottsoffren via telefon, där personer luras att lämna ut känslig information som lösenord eller inloggningsuppgifter till t.ex. banken. Alternativt blir man lurad att logga in på sin bank och själv genomföra transaktionen till bedragarens konto. Bedragaren använder i vissa fall spoofade telefonnummer, dvs. numret ser ut att komma från banken, vilket ger brottsoffret en känsla av falsk säkerhet. Vad bedragaren säger för att lura offret att lämna ut den känsliga informationen varierar, men det kan t.ex. handla om att det skett transaktioner på offrets konto som inte är det brukliga. Gemensamt för bedragarna är dock att de skrämmer upp och stressar brottsoffret genom att påstå att det är bråttom och att offret snabbt måste vidta åtgärder för att inte lida skada och att bedragaren erbjuder sig att ”lösa” problemet. Bedragaren lurar offret att identifiera sig med t.ex. BankID eller bankdosan och logga in på sin bank samt att föra över pengar via Swish eller via en banköverföring.[17]

En särskild typ av telefonbedrägeri är s.k. wangirisamtal, som drabbar både slutanvändare och operatörer. Bedrägeriet består av samtal från telefonnummer med

[16] Brå rapport 2023:11, *Bedrägerier mot privatpersoner*, bilaga 4.
[17] Brå rapport 2023:11, *Bedrägerier mot privatpersoner*, s 25

hög samtalstaxa, främst från internationella telefonnummer, där samtalet avbryts innan den uppringda personen svarar. Tanken med detta är att den uppringda personen ska ringa tillbaka, antingen utan att inse att numret är ett dyrt internationellt samtal eller av misstag. Bedragaren får en intäkt av betalsamtal eller för terminering av samtrafik. Wangirisamtal kan kombineras med olika tekniker såsom falska svar, röstmeddelanden eller pausmusik för att förlänga samtalet. Bedrägeriet drabbar i första hand slutanvändaren, men upptäcks förmodligen inte så ofta av denne, men om det upptäcks så leder det ofta till att kostnaden avskrivs av operatören.



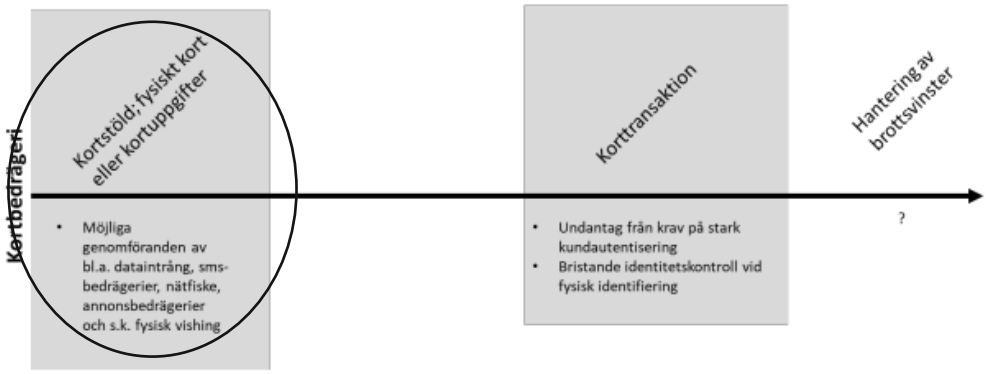
Figur 3: Händelsekedja – telefonbedrägerier.[18] Figur från Brå:s rapport med en ring, tillagd av PTS, som markerar i vilken del av händelsekedjan som elektroniska kommunikationstjänster används.

3.3 Kortbedrägerier

Kortbedrägerier är den vanligaste bedrägeritypen sett till antalet anmälda brott och de står för ca 40 % av alla anmälda bedrägerier 2022.[19] Grunden i ett kortbedrägeri är användningen av någon annan persons fysiska kredit- eller betalkort eller användning av kortuppgifter för att genomföra ett köp eller ett uttag.[20] Detta sker t.ex. genom att bedragaren ser över axeln på brottsoffret för att på så sätt få reda på koden och sedan stjäl kortet. Alternativt stjäls enbart kortet och det används till köp för lägre belopp där krav på kod saknas eller vilseleder offret att lämna ifrån sig både kort och kod. Vissa bedrägerier sker med enbart kortuppgifterna till köp på nätet. Dessa bedrägerier inleds vanligen med ett dataintrång mot t.ex. kortföretag eller mot privatpersonerna direkt genom t.ex. nätfiske, falska annonser i sociala medietjänster eller via sökmotorer som länkar till webbplatser som verkar seriösa. Kortuppgifterna säljs sedan vidare.[21] Under PTS intervjuer med olika aktörer har det framförts att antalet kortbedrägerier minskat efter införandet av EU:s andra betaltjänstdirektiv

[18] Brå rapport 2023:11, *Bedrägerier mot privatpersoner*, bilaga 4.
[19] Brå rapport s 21 och *Rapport om de dödliga bedrägerierna*, s 9.
[20] Polisen, *Rapport om de dödliga bedrägerierna*, s 9.
[21] Brå rapport 2023:11, *Bedrägerier mot privatpersoner*, s 31.

PSD 2, men att de nu är på väg att öka i antal igen och att kortköpen oftast görs på webbplatser utanför EU.

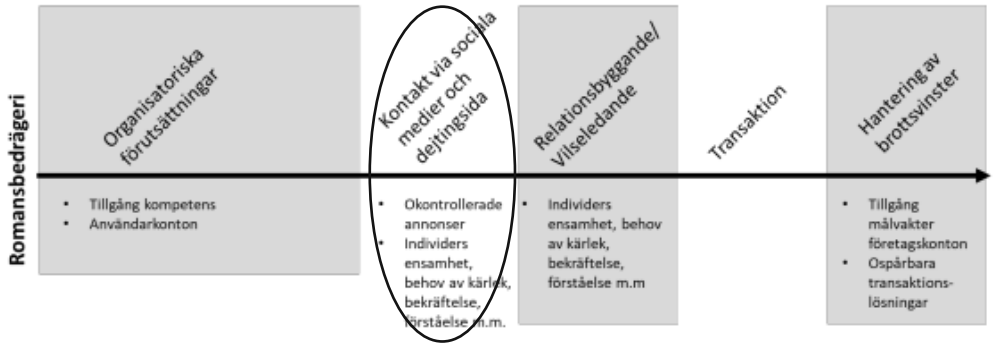


Figur 4: Händelsekedja - kortbedrägerier.[22] Figur från Brå:s rapport med en ring, tillagd av PTS, som markerar i vilken del av händelsekedjan som elektroniska kommunikationstjänster används.

3.4 Romansbedrägerier

Romansbedrägerier, s.k. *sol-och-vårande*, innebär att bedragaren inleder en kärleksrelation med offret med syfte att lura av denne pengar eller andra värdesaker. Romansbedrägerier sker främst via sociala medietjänster eller dejtingsidor och de är vanligtvis av internationell karaktär, t.ex. kan ett callcenter utomlands användas och att pengarna först går till ett målvaktskonto i Sverige för att sedan skickas utomlands via kontoöverföringar, betalningstjänster eller via Swish och uttag i kontanter.[23] Romansbedrägerier har få anmälningar, men brottsvinsterna är förhållandevis stora.[24]

[22] Brå rapport 2023:11, *Bedrägerier mot privatpersoner*, bilaga 4.
[23] Brå rapport 2023:11, *Bedrägerier mot privatpersoner*, s 28 f.
[24] Brå rapport 2023:11, *Bedrägerier mot privatpersoner*, s 8.

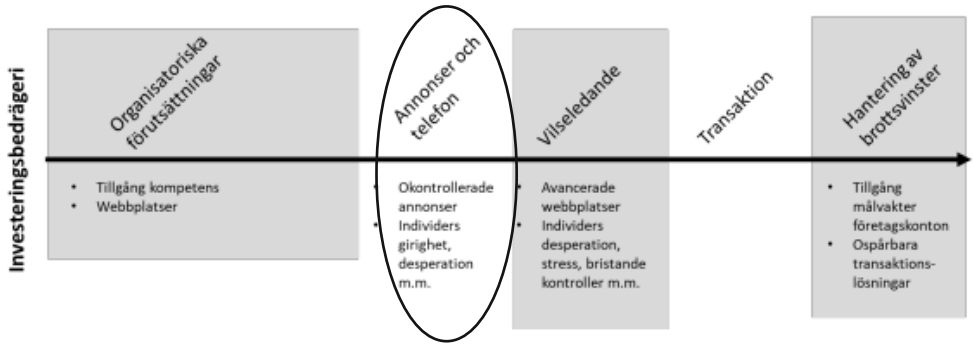


Figur 5: Händelsekedja – romansbedrägerier. Figur från Brå:s rapport med en ring, tillagd av PTS, som markerar i vilken del av händelsekedjan som elektroniska kommunikationstjänster används.

3.5 Investeringsbedrägerier

Investeringsbedrägerier går i korthet ut på att bedragaren vill få offret att investera i en påstått lönsam investering, t.ex. kryptovaluta. Brottets förberedande innehåller ofta ett upprättande av företag, webbplatser och annonser i syfte att skapa förtroende för produkten. Den viktigaste kontaktvägen är att det potentiella brottsoffret ser en annons för en finansiell produkt, klickar på länken och anmäler intresse.[25] Brotten genomförs med hjälp av t.ex. reklamannonser. Bedragarna ringer ofta från callcenter utomlands och offrets pengar går vanligtvis till utländska kryptoväxlar genom att brottsoffret vilseleds att betala till en elektronisk plånbok. Alternativt går betalningen till svenska företag som använder sig av penningmålvakter för att sedan skicka pengarna vidare till företag utomlands genom exempelvis osanna fakturor.[26] Investeringsbedrägerier har få anmälningar, men brottsvinsterna är förhållandevis stora.[27]

[25] Brå rapport 2023:11 *Bedrägerier mot privatpersoner*, s 29.
[26] Polisen, *Rapport om de dödliga bedrägerierna*, s 9 och Brå rapport 2023:11, *Bedrägerier mot privatpersoner*, s 30.
[27] Brå rapport 2023:11, *Bedrägerier mot privatpersoner*, s 8.



Figur 6: Händelsekedja - investeringsbedrägerier[28]. Figur från Brå:s rapport med en ring, tillagd av PTS, som markerar i vilken del av händelsekedjan som elektroniska kommunikationstjänster används.

3.6 Bedragarens förutsättningar

Organisatoriska förutsättningar skapas genom tillgång till kompetens och resurser. Dessa kan vara enskilda, eller mer organiserat i en callcenter-liknande organisation[29]. Trovärdighet byggs med inventering av material på externa webbplatser, kopiering och uppbyggnad av liknande webbplatser samt användarkonton på sociala medier och liknande. Målvakter rekryteras för att ta hand om betalningar eller att skapa abonnemang eller köpa domäner.

Kartläggning görs via öppna källor såsom nummerupplysning och upplysningstjänster med utgivningsbevis. Identitetskapning på t.ex. sociala medier görs för att kunna kartlägga eller utge sig för att vara någon för offret bekant person. Webbplatser och användarkonton skapas med inspiration från riktiga nyheter, personer och organisationer för att bygga en trovärdig historia.

3.7 Brottsvinster vid bedrägerier med elektroniska kommunikationstjänster

I analysen *Brottsvinsterna för bedrägeribrottsligheten 2022*[30] framgår att brottsvinsterna för olika former av telefonbedrägerier var 619 miljoner kronor år 2022. Under 2023 har det enligt polisen anmälts ca 29 000 telefonbedrägerier (då ingår både bedrägerier där brottet startat med ett telefonsamtal och där det startat med

[28] Brå rapport 2023:11, *Bedrägerier mot privatpersoner*, bilaga 4.
[29] Telefonbedrägerier är de gängkriminellas nio till fem-jobb (aklagare.se).
[30] Polismyndigheten, Brottsvinsterna för bedrägeribrottsligheten 2022, 2023-04-21, Dnr A232.846/2023.

ett sms) och brottsvinsterna uppgick till 708 miljoner kronor[31]. När det gäller bedrägerier beskrivs telefonbedrägerier som det allvarligaste problemet.[32] Det är inte ovanligt att dessa telefonbedrägerier genomförs med hjälp av s.k. spoofing.

Flera aktörer har framfört att det troligen finns ett underliggande mörkertal av bedrägerier där brottsoffer av olika anledningar väljer att inte anmäla brottet. Omfattningen på detta är okänd men talar för att Polisens siffra är lägre än det faktiska utfallet.

4. Summering av kartläggningen fram till idag – de vanligaste bedrägerierna med elektroniska kommunikationstjänster i Sverige

PTS konstaterar att möjligheterna att inom myndighetens verksamhetsområde föreslå åtgärder mot olika typer av bedrägerier är begränsade till de fall där en elektronisk kommunikationstjänst utgör ett nödvändigt verktyg för bedragaren. Det är svårare att med åtgärder kopplade till elektronisk kommunikation komma tillrätta med exempelvis romansbedrägerier, investeringsbedrägerier och kortbedrägerier, där den sociala kontexten och bedragarens sociala förmåga till manipulation är viktiga verktyg för bedragarna. Den typen av bedrägerier är svåra att skydda sig mot genom elektroniska lösningar.

I kartläggningen har det framkommit att det framför allt är telefonsamtal, sms och e-post men även sociala medietjänster som används där slutanvändare drabbas av bedrägerier. Detta har framförts av samtliga aktörer som PTS haft en dialog med. För att bedrägeri genom elektroniska kommunikationstjänster ska kunna genomföras är ofta den drabbades e-legitimation inblandad som en del i förfarandet. Det förekommer också att bedrägerier genomförs med hjälp av falska webbplatser. Annat som underlättar för bedragarna är all den enkelt tillgängliga personliga

[31] https://polisen.se/aktuellt/nyheter/nationell/2024/januari/anmalningarna-av-bedragerier-okade-under-2023--det-har-gor-polisen/ [Hämtad 2024-04-24].
[32] BRÅ, Bedrägerier mot privatpersoner Rapport 2023:11, s 7.

information som går att hitta på olika webbplatser med personlig information om t.ex. adress, ålder och hushållets storlek. Annat som nämnts av aktörerna som ett ökande problem är bedrägerier där man med hjälp av AI kan utge sig för att vara en person genom en förfalskad röst, och på så sätt lättare lura en familjemedlem.

Det har också framförts att det kan finnas behov av ökad samordning, eller nätverk, vad gäller informationsspridning från myndigheter, organisationer och företag, om bedrägerier och hur slutanvändaren kan minska risken att bli utsatt.

Några aktörer har även framfört synpunkter om individens eget ansvar i samband med bedrägerier.

PTS gör följande summering:

- Telefonsamtal, sms och e-post är vanligast förekommande elektroniska kommunikationstjänster som används i samband med bedrägerier
- Även e-legitimation, sociala medietjänster och falska webbplatser används i samband med bedrägerier
- Personlig information som finns tillgänglig publikt på internet är ett problem då bedragare utnyttjar det vid kartläggning av brottsoffer
- Problem med bedrägerier via nummeroberoende OTT-tjänster ökar
- Användning av AI som ett verktyg i samband med bedrägerier ökar
- Informationsspridning om bedrägerier och hur slutanvändare skyddar sig kan behöva samordnas.

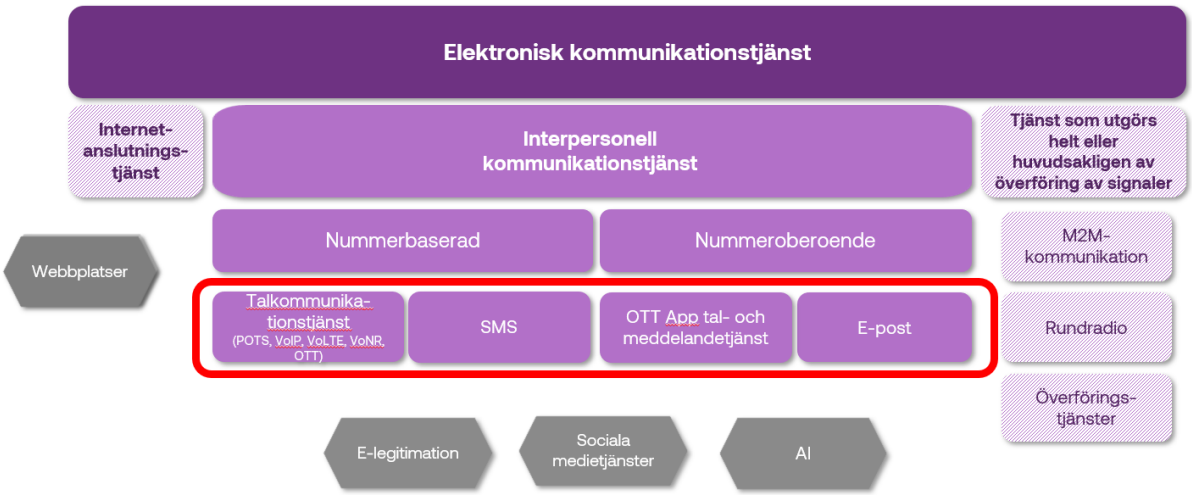
5. PTS gjorda avgränsningar i uppdraget

Ramar för uppdraget sätts genom definitionen av begreppet bedrägeri. PTS har därför valt att fokusera på sådana elektroniska kommunikationstjänster som kan användas som verktyg för brottet bedrägeri och som riktar sig direkt till slutanvändare. Därmed omfattas inte t.ex. M2M-kommunikation och internetanslutningstjänster.

PTS har utifrån resultatet av kartläggningen valt att i första hand fokusera på följande elektroniska kommunikationstjänster:

- Nummerbaserade talkommunikationstjänster
- Nummerbaserade sms
- Nummeroberoende OTT tal- och meddelandetjänster
- E-post

I bilden nedan illustreras elektroniska kommunikationstjänster och de avgränsningar som PTS har valt att göra. Rödmarkerade är de områden som PTS kommer att fokusera på i det fortsatta arbetet med uppdraget.



Figur 7: PTS avgränsning av elektroniska kommunikationstjänster i detta uppdrag. Tjänsterna inom det rödmarkerade området är de tjänster som PTS kommer att fokusera på i det fortsatta arbetet med uppdraget. Tjänster som inte utgör elektroniska kommunikationstjänster indikeras genom sexkantiga figurer.

Annat som har nämnts i kartläggningen är falska webbplatser, e-legitimation och sociala medietjänster som används som en del i bedrägerier. AI kan komma att bli ett frekvent använt hjälpmedel i samband med bedrägerier, men anses inte utgöra elektroniska kommunikationstjänster och hamnar därmed utanför uppdraget.

Avslutningsvis har det i mötena med operatörer framförts att det även förekommer bedrägerier riktade direkt mot deras verksamheter. Syftet kan vara att kringgå avräkning vid samtrafik av operatörstrafik, eller att få del av samtrafikintäkter eller

avgifter för t.ex. betalsamtal. Det rör sig i huvudsak om samtals- och meddelandetrafik men även om oönskad trafikbelastning i näten. Dessa bedrägerier drabbar även konsumenter eller företagskunder i form av direkta eller indirekta kostnader. Det förekommer också mer ”traditionella” bedrägerier, där någon mindre seriös aktör sluter avtal med en operatör och kan hämta ut hårdvara (telefoner, routrar och liknande) för att sedan försvinna utan att lämna tillbaka produkterna. PTS kommer inte att utreda bedrägerier direkt riktade mot operatörer inom ramen för detta uppdrag.

6. Befintliga regelverk och PTS mandat – vilka möjligheter finns att förhindra bedrägerier med elektroniska kommunikationstjänster?

PTS mandat att verka inom området för elektronisk kommunikation bestäms genom förordningen (2007:951) med instruktion för Post- och telestyrelsen och de olika rättsområden som nämns i den förordningen. Av instruktionen framgår att PTS har till uppgift att bl.a. främja tillgången till säkra och effektiva elektroniska kommunikationer, inbegripet att se till att samhällsomfattande tjänster finns tillgängliga, och att främja tillgången till ett brett urval av elektroniska kommunikationstjänster.

PTS är regleringsmyndighet och tillsynsmyndighet enligt LEK. PTS har även tillsynsansvar över s.k. betrodda tjänster, t.ex. e-legitimationer, där myndigheten tillämpar EU:s förordning 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner (eIDAS-förordningen)[33] och lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. PTS har också tillsynsansvar enligt lagen (2006:24) om nationella toppdomäner för Sverige på internet.

PTS är även Sveriges nationella samordnare för digitala tjänster och behörig myndighet för flertalet bestämmelser inom DSA. Rättsakten ska bidra till en korrekt

[33] *EU:s förordning 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG*.

fungerande inre marknad för förmedlingstjänster och säkerställa en förutsebar, säker och förtroendeskapande onlinemiljö, bl.a. genom att underlätta rapportering av olagligt innehåll på de förmedlingstjänster som berörs.

Givet att det finns flera underliggande funktioner i näten som behandlar identiteterna på flera olika nivåer i elektroniska kommunikationsnät och tjänster, kan eventuellt omfattande åtgärder behövas för att säkerställa riktighet och autenticitet av dessa.

Det pågår för närvarande ett arbete i EU för att harmonisera incidentrapportering och riskhanteringsåtgärder för att stärka cybersäkerheten inom EU enligt NIS2-direktivet[34]. Delbetänkandet *Nya regler om cybersäkerhet* (SOU 2024:18) föreslår att direktivet ska implementeras i svensk lag under 2025 genom en ny cybersäkerhetslag. Direktivet ställer tydligare krav på bl.a. riskanalyser och olika säkerhetsåtgärder i nätverks- och informationssystem. Det pågår även för närvarande informationsutbyten inom den europeiska cybersäkerhetsbyrån ENISA och mellan medlemsstaterna om vilka mandat som de olika medlemsstaterna har för att hantera bedrägerier som sker via elektroniska kommunikationsnät och elektroniska kommunikationstjänster, t.ex. bluff-sms. EU-kommissionen, ENISA och medlemsstaterna publicerade den 21 februari 2024 en rapport gällande cybersäkerhet och motståndskraft i infrastruktur och nätverk, där bl.a. rekommendationer och åtgärder mot bluff-sms nämns.[35]

Av ovanstående regelverk ser PTS att det inom ramen för uppdraget främst kan bli aktuellt att tillämpa lagen (2022:482) om elektronisk kommunikation.

6.1 Initial analys av tillämpliga regelverk

Lagen (2022:482) om elektronisk kommunikation (LEK)

LEK bygger till största delen på Europaparlamentets och rådets direktiv om inrättande av en europeisk kodex för elektronisk kommunikation[36] (Kodexen). Vissa bestämmelser i LEK har dock sitt ursprung i det s.k. e-dataskyddsdirektivet[37]. Varken i

[34] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet).

[35] Report on the cybersecurity and resiliency of the EU communications infrastructures and networks | Shaping Europe's digital future (europa.eu).

[36] Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation.

[37] 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).

kodexen, e-dataskyddsdirektivet eller i LEK finns några bestämmelser som uttryckligen tar sikte på att förhindra bedrägerier genom användandet av elektroniska kommunikationer. PTS har identifierat några befintliga bestämmelser i LEK som kan tillämpas i detta syfte.

Enligt 4 kap. 3 § LEK får nummer ur en nationell nummerplan användas endast efter tillstånd från regleringsmyndigheten. Ett tillstånd ska avse serier av nummer eller enskilda nummer. Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om tilldelning av nummer. Ett bemyndigande till PTS att meddela föreskrifter om nationella nummerplaner finns i 4 kap. 7 § förordningen (2022:511) om elektronisk kommunikation (FEK).

Enligt 9 kap. 6 § LEK får regeringen eller den myndighet som regeringen bestämmer i fråga om behandling av uppgifter för elektronisk kommunikation meddela föreskrifter om de krav som ska ställas på en talkommunikationstjänst som medger identifiering av det anropande eller uppkopplade telefonnumret, eller vidarekoppling.

I 9 kap. 2 § FEK ges PTS bemyndigande att meddela sådana föreskrifter.

Motsvarande bestämmelser saknas vad gäller andra typer av kommunikationstjänster. Om lagstiftarens avsikt hade varit att den generella bestämmelsen i 8 kap. 1 § om säkerheten i nät och tjänster skulle kunna tillämpas torde inte en särskild bestämmelse i 9 kap. 6 § för talkommunikationstjänster ha införts. Mot bakgrund av detta bedömer PTS att det i nuläget saknas tydligt lagstöd för att besluta om föreskrifter och att vidta ingripande åtgärder mot enskilda för andra typer av kommunikationstjänster än talkommunikationstjänster.

Förutom ovan nämnda bestämmelser i LEK finns även bestämmelser om säkerhet i nät och tjänster i 8 kap. LEK.

Enligt 8 kap. 1 § ska den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att på ett lämpligt sätt hantera risker som hotar säkerheten i nät och tjänster. Åtgärderna ska säkerställa en nivå på säkerheten i nät och tjänster som är lämplig i förhållande till riskerna. Åtgärder ska vidtas särskilt för att förebygga och minimera säkerhetsincidenters påverkan på användare och på andra nät och tjänster.

Uttrycket ”säkerhet i nät och tjänster” definieras i 1 kap. 7 § LEK som elektroniska kommunikationsnäts och elektroniska kommunikationstjänsters förmåga att vid en viss tillförlitlighetsnivå motstå händelser som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos näten eller tjänsterna, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som

erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster.

Så länge tjänsten ifråga förmedlar det innehåll som avsändaren skickar saknar PTS möjligheter att ingripa mot en operatör med stöd av bestämmelserna i 8 kap. LEK. Detta gäller även om uppgifterna som förmedlas (t.ex. ett angivet avsändarnamn) är falska.

PTS får enligt 8 kap. 4 § FEK meddela ytterligare föreskrifter om bl.a. säkerhetsåtgärder enligt 8 kap. 1 § LEK och har med stöd av bl.a. detta bemyndigande utfärdat föreskrifter och allmänna råd om säkerhet i nät och tjänster. Det finns idag inga särskilda krav i PTS befintliga säkerhetsföreskrifter på säkerställande av riktighet och autenticitet i enlighet med definitionen i 1 kap. 7 § LEK.

eIDAS-förordningen

Ett annat rättsområde där PTS idag har viss föreskriftsrätt är elektronisk identifiering och betrodda tjänster för elektroniska transaktioner (eIDAS-förordningen). eIDAS-förordningen är uppdelad i två delar, elektronisk identifiering och betrodda tjänster. Myndigheten för digital förvaltning (Digg) ansvarar för den del som hanterar elektronisk identifiering. PTS ansvarar för betrodda tjänster, vilket inkluderar elektronisk underskrift. PTS är också utpekad tillsynsmyndighet över reglerna i eIDAS-förordningen som rör betrodda tjänster. Under 2024 kommer eIDAS-förordningen att uppdateras, och diskussioner pågår om PTS tillsynsansvar kommer att breddas men fortfarande vara kopplad till elektronisk identifiering och betrodda tjänster.

PTS får enligt 2 § förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering meddela föreskrifter om:

1. krav för ackreditering av organ för bedömning av överensstämmelse,
2. hur bedömningar av överensstämmelse ska göras, och
3. rapportering av bedömningar av överensstämmelse.

PTS mandat att meddela föreskrifter sträcker sig alltså inte till själva användningen av tjänsterna och PTS har inte heller något tillsynsansvar i dessa delar.

6.2 Sammanställning av vidtagna och kommande åtgärder

I Sverige har ett antal initiativ tagits för att förhindra spoofing.

PTS vägledning om spoofing

PTS har i samverkan med operatörer och Telekområdgivarna tagit fram en vägledning[38] som vänder sig till operatörer. Vägledningen publicerades i november 2023 och utgår från att svenska telefonnummer ska användas i Sverige. Den innehåller rekommendationer om hantering av samtal med svenska telefonnummer som kommer in till Sverige från utlandet via ett internationellt samtrafikgränssnitt. Enligt PTS kartläggning kommer så gott som alla samtal med manipulerade nummer idag från utlandet. Genom att stoppa dessa samtal kan operatörerna hindra en stor del av de bedrägeriförsök som görs via telefonsamtal med manipulerade nummer.

Flera operatörer har börjat följa rekommendationerna och uppger att de fungerar bra. Operatörerna spärrar nu en stor mängd samtal med fasta nummer som kommer in till Sverige från utlandet. När det gäller mobilnummer krävs en lösning som kan kontrollera om abonnenten roamar utomlands eller inte vilket kräver ytterligare utvecklingsarbete. Operatörerna arbetar med att ta fram en sådan lösning. Vissa operatörer har också börjat spärra samtal med svenska mobilnummer där de själva kan kontrollera om numret roamar eller ej för sina egna abonnenter.

PTS förslag till föreskrifter och allmänna råd

PTS har parallellt med vägledningen arbetat vidare med att ta fram föreskrifter och allmänna råd som baseras på vägledningen. Sannolikt kan dessa börja gälla i slutet av 2024. De föreslagna föreskrifterna och allmänna råden innebär att vägledningen därmed har ersatts av såväl bindande regler (föreskrifter) som kompletterande rekommendationer (allmänna råd).

Förslaget till föreskrifter utgår från att svenska telefonnummer ska användas i Sverige. Det innebär att samtal med svenska telefonnummer som kommer in till Sverige via ett internationellt samtrafikgränssnitt ska spärras, så att de inte kopplas fram. När det gäller telefonnummer för mobiltelefonitjänster, M2M-kommunikation och mobila bredbandstjänster ska en kontroll först ske för att se om den svenska abonnenten roamar i ett annat land, och om så är fallet kan samtalet kopplas fram. De föreslagna bestämmelserna kommer att kräva en teknisk lösning för kontroll av roaming, som kommer att behöva tas fram och bekostas av operatörerna själva.

[38] Vägledning för tillhandahållare (pts.se).

Operatörernas spärrlista för vissa telefonnummer

Redan 2018 infördes genom ett gemensamt arbete mellan några operatörer, under ledning av Telekområdgivarna, en s.k. spärrlista där banker och andra företag kan registrera telefonnummer som företagen själva enbart använder för inkommande samtal. Om ett sådant nummer dyker upp i samtalstrafiken ska det därför inte kopplas fram. Listan används idag av de flesta stora operatörer.

Operatörernas frivilliga samarbete för att skydda alfanumeriska avsändarnamn (SMS SenderID protection)

Ett antal aktörer på marknaden har genom ett samarbete tagit fram en modell för att en organisation (t.ex. ett företag eller myndighet) ska kunna registrera sitt alfanumeriska avsändarnamn. Lösningen går ut på att organisationen som använder sms-utskick till sina kunder, kan registrera sitt alfanumeriska avsändarnamn hos den eller de aggregatörer som hanterar sms-utskick åt organisationen. Efter denna registrering underrättas operatörerna som därefter kan spärra sms med detta avsändarnamn om det inte kommer från rätt avsändare.

Operatörernas frivilliga samarbete för att rapportera bluff-sms

Flera operatörer har gått samman och tagit fram ett gemensamt sms-kortnummer, 7726, för att bättre kunna ta emot anmälningar om misstänkta bluff-sms och på så sätt motverka förekomsten av dessa. Kunden kan vidarebefordra misstänkta bluff-sms till sin operatör via 7726. Operatörerna kan därefter dela informationen och agera samtidigt på sådana sms. Tidigare har operatörerna haft egna sms-kortnummer dit kunderna har kunnat göra anmälningar men den nya lösningen ger operatörerna möjlighet att agera snabbare.

Operatörernas frivilliga arbete för att förhindra wangirisamtal

Förekomsten av wangirisamtal mot slutanvändare har avtagit dramatiskt under senare tid, då operatörer har tagit fram lösningar för detta. Genom att man analyserar trafiken och identifierar telefonnummer (främst internationella) som används vid wangirisamtal kan trafik till och från dessa nummer automatiskt blockeras under en tid.

6.3 E-legitimation och bedrägerier

Många bedrägerier går ut på att med hjälp av e-legitimation, t.ex. BankID, få offret att överföra pengar från sin bank till ett konto som bedragaren har tillgång till t.ex. via en målvakt.

BankID erbjuder både tjänsterna elektronisk identifiering och elektronisk underskrift, d.v.s. både inloggning och signering av tjänster. PTS tillsynsansvar idag berör enbart de betrodda tjänsterna, dvs. hantering av skapande, kontroller, validering och bevarande av elektroniska underskrifter. Kopplat till detta har PTS olika tillsynsmöjligheter beroende på om tjänsten är en så kallad icke kvalificerad betrodd tjänst eller en kvalificerad betrodd tjänst. BankID är en icke kvalificerad betrodd tjänst vilket gör att enbart händelsestyrd tillsyn kan göras och enbart mot de betrodda tjänsterna.

Inloggning med BankID har gradvis gjorts säkrare med t.ex. krav på att läsa en QR-kod från bankens inloggningssida. Detta görs för att säkerställa att inloggningen initieras av samma person som legitimerar sig. Sedan den 1 maj 2024 krävs "säker start" från rörlig QR-kod.

En tydlig skillnad jämfört med ett tidigare traditionellt besök i en fysisk banklokal är att det ur kundens perspektiv fortfarande är svårt att säkerställa äktheten hos personen som säger sig representera banken. Vanan att använda BankID i samband med telefonsamtal kan göra att man uppfattar kontakten som säker, trots att autentiseringen bara gjorts i en riktning.

Teknikutvecklingen har gjort att det skett en förskjutning från obehöriga till behöriga transaktioner, dvs. från att transaktionen görs utan kontoinnehavarens samtycke till de behöriga transaktionerna där kontoinnehavaren medverkar. Det innebär att brottsoffret själv genomför transaktionen och luras att föra över pengar till bedragarens konto.[39] Denna typ av bedrägeri har ökat avsevärt de senaste åren och det drabbar i huvudsak särskilt utsatta grupper såsom äldre och funktionsnedsatta och i vissa fall även små företag.

PTS har noterat att bankerna gör satsningar inom brottsförebyggande arbete[40] och ser att detta kan ha en positiv effekt för att motverka bedrägerier.

[39] Brå rapport 2023:11, *Bedrägerier mot privatpersoner*, s 26.
[40] Bankerna stärker kundskyddet mot bedrägerier ytterligare | Swedishbankers.

7. Initial internationell utblick

PTS kan konstatera att flera länder har i likhet med Sverige vidtagit åtgärder eller planerar att genomföra åtgärder för att förhindra bedrägerier. Framförallt handlar det om åtgärder för att motverka bedrägerier genom samtal med manipulerade telefonnummer och falska alfanumeriska avsändarnamn för sms.

Inom CEPT ECC WG NaN2[41] har en rekommendation tagits fram i syfte att vägleda medlemsstaterna kring åtgärder mot spoofing, ECC Recommendation (23)03[42], rekommendationen fastställdes i november 2023. Flera regleringsmyndigheter i europeiska länder har tagit fram åtgärder för att komma till rätta med spoofing på liknande sätt som denna rekommendation gör. Nu pågår ett arbete med att ta fram en rekommendation med förslag på åtgärder för att förhindra förfalskade alfanumeriska avsändarnamn för sms, *ECC Recommendation on Alphanumeric Sender ID for SMS*. Rekommendationen planeras bli klar för publicering i november 2024. PTS deltar aktivt i arbetet inom CEPT ECC WG NaN2 och har dialog med operatörer gällande det pågående arbetet med rekommendationen om Alphanumeric Sender ID. Inom CEPT och andra organisationer anordnas workshops inom området bedrägerier och elektroniska kommunikationer med lite olika inriktningar.

Finland är ett av de länder som har kommit långt i sitt arbete. Bl.a. har man infört åtgärder mot manipulerade finska nummer som kommer in från utlandet på liknande sätt som PTS rekommenderar i vägledningen som nämns i avsnitt 6.2. Finland har redan föreskrifter på plats för detta. Vidare har Finland också infört en möjlighet för företag att skydda sitt alfanumeriska avsändarnamn för sms för att på så sätt försäkra sig om att ingen annan avsändare kan använda samma identitet. Registrering av alfanumeriska avsändarnamn görs hos den finska regleringsmyndigheten Traficom efter vissa givna regler.

[41] CEPT (European Conference of Postal and Telecommunications Administrations) är en organisation som samlar regleringsmyndigheter inom post- och telekomsektorn I Europa. Inom CEPT finns ECC (Electronic Communication Committee), som I sin tur är indelat I ett antal arbetsgrupper, bl.a. Working Group NaN2.

[42] *Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers* - ECO Documentation (cept.org).

8. Problembeskrivning av bluff-sms

Många aktörer har uppgett att bluff-sms är ett av de vanligast förekommande verktygen för bedrägeriförsök. Eftersom det finns möjlighet att skicka sms med alfanumeriskt avsändarnamn, där ett varumärke eller företagsnamn visas i mottagarens nummerpresentation, finns idag möjlighet för bedragare att utge sig att vara en representant för en välkänd organisation. Sms är en etablerad tjänst och har med användningsområden som tvåfaktorsautentisering och leveransaviseringar upplevts som säker.

Den vanligaste formen av sms, person-till-person-meddelanden (P2P), är ett mindre problem i bedrägerisammanhang. Den största utmaningen är idag applikation till person-sms (A2P) med alfanumeriska avsändarnamn. Eventuella begränsningar av namn eller varumärken som alfanumeriska avsändarnamn kan bestå av är upp till aggregatörer och operatörer att avtala med slutanvändarna.

Sms med alfanumeriskt avsändarnamn regleras inte särskilt idag. Ett antal operatörer erbjuder ett visst skydd för registrerade namn för sms till sina egna kunder. Det finns i nuläget inte någon möjlighet för mottagaren att veta om ett namn är skyddat eller ej. Det går inte att svara på ett sådant sms. Det är oftast inte möjligt att blockera avsändare av dessa sms i mobiltelefonens adressbok. Om man tar emot ett bluff-sms med samma alfanumeriska avsändarnamn som tidigare visas de i samma flöde i adressboken, vilket förstärker intrycket av äkthet.

Begränsningen i antal tecken och möjligheten att sända sms via många olika aktörer gör att en generell spärrlista för sms med oregistrerade alfanumeriska avsändarnamn är utmanande. Generellt kan större organisationer ha många källor och leverantörer för sina utskick. Vissa alfanumeriska avsändarnamn kan även vara generiska och användas av många avsändare, som t.ex. ”Noreply”, "Blomsterbud", "Paketbud" eller "Resebokning".

I detta regeringsuppdrag har PTS fokuserat på bedrägerier i brottsbalkens mening. Det bör även noteras att manipulation av t.ex. alfanumeriska avsändarnamn för sms kan användas för andra ändamål än bedrägerier, men som ändå är vilseledande för mottagaren. Sms används vid vissa krissituationer som kommunikationskanal för massutskick till allmänheten. Detta sker genom Viktigt meddelande till allmänheten (VMA), där sms är en av flera kommunikationssätt som kan användas. Felaktiga eller bedrägliga sms kan i detta sammanhang användas för att skapa osäkerhet och

riskera att underminera förtroendet för denna viktiga funktion. Under våren inträffade en incident där ett bluff-sms, med angiven avsändare ”VMA”, skickades ut till ett flertal slutanvändare. I media beskrevs det som ett falskt VMA, men det bör betonas att det var ett vanligt bluff-sms som skickades till ett antal slutanvändare. Det var alltså inte fråga om att VMA-funktionen hade hackats och utnyttjats för att skicka ett falskt VMA. Uppmärksamheten ledde dock till att åtgärder vidtogs av bl.a. operatörer och SOS Alarm för att minska risken för liknande incidenter.

PTS har i andra arbeten tittat på ett alternativ till VMA-sms; "cell broadcast", vilket i likhet med sms skickar meddelanden till mobiltelefoner/terminaler. Dessa meddelanden sänds ut och visas för användaren på ett annat sätt än sms. Denna teknik bedöms idag av många som mer säkert än sms. Cell-broadcast är inte implementerat som en lösning i Sverige idag.

PTS kan sammanfattningsvis konstatera att en stor del av problemen kring bluff-sms rör möjligheten att använda alfanumeriska avsändarnamn. PTS bedömning är att det idag saknas uttryckliga bestämmelser i 9 kap LEK som reglerar identifiering av avsändare av sms. Bemyndigandet i 9 kap. 2 § FEK har använts för PTS föreskrifter som syftar till att förhindra bedrägerier som görs genom spoofade telefonsamtal. Som bestämmelsen i 9 kap. 6 § LEK är utformad är det dock endast möjligt att ställa krav på en *talkommunikationstjänst*. PTS har utifrån denna begränsning gjort bedömningen att det i dagsläget saknas möjlighet att föreskriva om regler för nummerpresentation av sms med stöd av 9 kap. LEK. PTS ser dock att en ändring av LEK och FEK som tillåter PTS att föreskriva motsvarande bestämmelser för presentation av avsändare av sms skulle vara en möjlig väg att reglera detta område.

9. Förkortningar

Följande förkortningar används i rapporten:

Förkortning	Uttydning
AI	Artificiell Intelligens
A2P	Application to Person
Berec	Body of European Regulators for Electronic Communications
DSA	Digital Services Act.
eIDAS	Electronic identification and trust services
FEK	Förordning om elektronisk kommunikation
IoT	Internet of Things
LEK	Lagen om elektronisk kommunikation
M2M	Machine to Machine
OTT	Over the Top
POTS	Plain Old Telephone Service
PSD 2	Payment Service Directive 2.
P2P	Person to Person
sms	Short message service
VMA	Viktigt meddelande till allmänheten
VoIP	Voice over IP
VoLTE	Voice over Long Term Evolution
VoNR	Voice over New Radio