Förvaltningsrätten i Stockholm,

115 76 Stockholm

Inges till Post- och telestyrelsen, Box 6101, 102 32 Stockholm
via e-post pts@pts.se

Stockholm den 28 januari 2022

Överklagande och begäran om inhibition

Klagande: Bahnhof AB ("Bahnhof"), Box 7702, 103 95 Stockholm

Motpart: Post- och telestyrelsen ("PTS"), Box 5398, 102 49 Stockholm

Överklagat beslut: PTS beslut 2022-02-18, ärende nr 21-10499

Saken: Föreläggande vid vite enligt 7 kap 5 § lagen (2003:389) om elektronisk kommunikation ("LEK") ; fråga om utlämnande av uppgifter om abonnemang.

Yrkanden

Bahnhof yrkar att förvaltningsrätten upphäver PTS beslut.

Bahnhof yrkar vidare att förvaltningsrätten – med stöd av 28 § förvaltningsprocesslagen - beslutar att föreläggandet tills vidare inte ska gälla.

Grunder

Grunderna åberopas i den rangordning som följer av numreringen.

1. Det saknas befogad anledning att utfärda ett föreläggande mot Bahnhof.

Bahnhof anser inte att det finns några konkreta omständigheter som motiverar PTS förläggande. PTS har i sitt föreläggande påstått att det "Av tillsynen framgår att Bahnhof vid flera tillfällen vägrat att lämna ut uppgifter om abonnemang till Polismyndigheten enligt 6 kap 22 § LEK när uppgifter om portnummer saknas i Polismyndighetens begäran" (sid 5). I föreläggande nämner dock PTS endast ett konkret ärende (sid 3) i vilket Bahnhof, efter att ha fått viss kompletterande information

av polisen, lämnat ut de begärda uppgifterna. Vilka de övriga ärendena är som PTS syftar på känner Bahnhof inte till.

Bahnhof kan inte se det på annat sätt än att PTS har utfärdat ett föreläggande mot Bahnhof p.g.a. av att Bahnhof i ett ärende begärt kompletterande information från polisen innan man lämnat ut begärda uppgifter. Bahnhof anser inte att det är tillräckliga skäl för en så ingripande åtgärd som ett vitesförläggande.

2. Föreläggande är inte tillräckligt preciserat.

Enligt föreläggande ska Bahnhof "säkerställa att de uppgifter om abonnemang gällande misstanke om brott som begärs av Polismyndigheten eller annan myndighet som ska ingripa mot brottet, lämnas ut även om underlag i form av portnummer saknas i samband med förfrågan". Bahnhof ställer sig frågande till vad PTS menar med "säkerställa". Bahnhof har lämnat ut uppgifter till polisen, bl.a. i det ärende som nämns i föreläggandet, vilket innebär att Bahnhof i och för sig har förmåga att ta fram de begärda uppgifterna. Det är oklart vilka övriga "säkerställande" åtgärder som PTS syftar på.

I rättsfallet HFD 2020 ref 28 har Högsta förvaltningsdomstolen ("HFD") fastställt vilka krav som ställs på utformningen av en myndighets vitesföreläggande för att detta ska ha någon rättsverkan, se punkterna 21-26 i HFD:s dom. Som exempel på krav som måste vara uppfyllda kan nämnas bl.a. att den som ett föreläggande riktar sig till måste få helt klart för sig vad som fordras för att det fastställda vitesbeloppet inte ska dömas ut och att vitet således måste vara knutet till en klart definierad prestation eller underlåtenhet. PTS föreläggande uppfyller inte kravet på precision eller något av de övriga kraven som räknas upp i HFD:s dom. PTS föreläggande kan därför inte ha någon rättsverkan och ska följaktligen upphävas.

3. Föreläggandet strider mot EU-rätten i fråga om skyddet för datalagrad information.

Föreläggandet avser uppgifter om abonnenter som har tilldelats s.k. NATade IP-adresser. Med NATade IP-adresser menas att flera abonnenter, oberoende av varandra, samtidigt delar på en och samma IP-adress. Teoretiskt kan drygt 65 000 abonnenter dela på en NATad IP-adress. Hur många abonnenter som i praktiken delar på en NATad IP-adress vid ett visst tillfälle är svårt att säga, men Bahnhof uppskattar att det normalt rör sig om mellan några tiotal upp till några hundratal. Bahnhof är enligt i enlighet med 6 kap 16a § LEK och 40 § förordningen (2003:396) om elektronisk kommunikation skyldig att laga användares IP-adress. I samband med tilldelning av NATade IP-adresser är Bahnhof i enlighet med PTS egna föreskrifter PTSFS 2019:2 även skyldig att lagra UDP- eller TCP-portnummer kopplat till användares IP-adress och spårbar tid för uppkopplingen. Lagringsskyldigheten är inte inskränkt till en viss kategori användare eller användare inom ett avgränsat geografiskt område utan gäller alla användare. Lagringen är med andra ord generell.

Som medlem i EU är Sverige skyldigt att följa EU:s rättsakter i form av bl.a. förordningar, direktiv och EU-domstolens domar. EU:s rättsakter har företräde framför svenska lagar och övriga författningar. Svenska lagar och författningar som strider mot EU-rätten får inte tillämpas. Svenska domstolar är vidare skyldiga att rätta sig efter EU-domstolens domar.

EU-domstolen har i flera domar t.ex. i det s.k. Tele2-målet C-203/15 och C-698/15 och senast i målet La Quadrature du Net m. fl C-511/18 m.fl. uttalat att generell lagring av trafik- och lokaliseringsuppgifter i princip strider mot det s.k. ePrivacy-direktivet 2002/58/EG jämfört med artiklarna 7, 8, 11 och 52.1 i EU:s stadga om grundläggande mänskliga rättigheter. Som ett undantag från denna princip har EU-domstolen i målet La Quadrature du Net i sitt beslut uttalat att en lagstiftning som föreskriver en generell och odifferentierad lagring av IP-adresser inte strider mot nämnda EU-rättsakter under förutsättning att lagringen sker i syfte att skydda nationell säkerhet, bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet.

LEK eller ovan nämnda följdförfattningar till LEK innehåller inga regler om att syftet med den generella lagringen av IP-adresser eller att åtkomsten till uppgifter om användare som använt en viss IP-adress skulle vara begränsad till viss form av allvarligare hot och grov brottslighet som EU-domstolen föreskriver.

Eftersom EU:s rättsakter är överordnade svenska författningar gäller kravet på att lagringen måste syfta till bekämpning av allvarligare säkerhetshot och grov brottslighet även när det gäller generell datalagring av IP-adresser som sker i Sverige, oavsett vad som framgår eller inte framgår av LEK och dess följdförfattningar. Om generell datalagring av IP-adresser endast får ske med angivna ändamål innebär det med nödvändighet att inte heller utlämning av uppgifter med stöd av generellt lagrade IP-adresser får ske annat än i syfte att bekämpa allvarlig brottslighet eller förhindra allvarliga säkerhetshot.

PTS föreläggande gäller uppgifter om abonnenter som har haft en viss IP-adress vid ett visst tillfälle. Ett utlämnande förutsätter alltså att det finns en lagrad IP-adress hos Bahnhof. De IP-adresser som finns lagrade hos Bahnhof är som tidigare nämnts sådana generellt lagrade IP-adresser som Bahnhof är skyldig att lagra enligt LEK och dess följdförfattningar. I enlighet med EU-domstolens ovan redovisade dom får Bahnhof inte åläggas att lämna ut generellt lagrade IP-adresser om det inte är fråga om att bekämpa grov brottslighet eller förhindra allvarliga säkerhetshot.

PTS föreläggande innehåller ingen begränsning om att de uppgifter som Bahnhof föreläggs att lämna till polisen ska avse bekämpning av grov brottslighet eller förhindrande av allvarliga säkerhetshot. Föreläggandet gäller således även annan mindre allvarlig brottslighet som den generella lagringen av IP-adresser inte får vara avsedd för i enlighet med EU-domstolens dom. Genom att inte innehålla några begränsningar till att endast gälla utlämning av uppgifter för att bekämpa grov brottslighet och allvarliga säkerhetshot strider PTS föreläggande således mot EU-rätten. Eftersom PTS föreläggande strider mot EU-rätten saknar föreläggandet rättsverkan. Det ska därför upphävas.

4. Föreläggandet strider mot EU-rätten i fråga om till vem lagrade uppgifter ska överlämnas.

I EU-domstolens dom i mål C-746/18, Prokuratuur, behandlar domstolen vilka krav som ska ställas på den myndighet som begär tillgång till generellt lagrade uppgifter, se särskilt punkterna 46-59 i domen. I sin dom anger domstolen att säkerställandet av att lagrade uppgifter används på ett rättssäkert sätt kräver en förhandskontroll av en domstol eller oberoende myndighet. Domstolen ansåg inte att en åklagare var tillräckligt oberoende för att utföra den förhandskontroll som krävdes.

Europadomstolen har i dom den 24 april 2018 i målet Benedik ./ Slovenien funnit att Slovenien kränkt en tilltalads rättigheter enligt art 8 i Europakonventionen genom en lag som tillät att slovensk polis kunde begära ut uppgifter om vem som haft en viss IP-adress utan ett föregående beslut av domstol.

Enligt PTS föreläggande ska Bahnhof lämna uppgifter till "Polismyndigheten eller annan myndighet som ska ingripa mot brottet". I föreläggandet finns inget villkor om att utlämnandet ska ske först efter att förhandskontroll gjorts av domstol eller annan oberoende myndighet.

Polismyndigheten som brottsutredande myndighet kan inte anses vara vare sig objektiv eller oberoende för att säkerställa att uppgifter om de personer som berörs behandlas på ett rättssäkert sätt. Enligt Bahnhof är det särskilt angeläget med en förhandskontroll av domstol mot bakgrund av att en begäran från polisen om uppgift om alla som haft en NATad IP-adress vid ett visst tillfälle kan innebära att Bahnhof tvingas lämna uppgifter om hundratals - och i teorin ännu fler - abonnenter, varav flertalet rimligen inte har något att göra med den brottslighet som polisen utreder. Här bör också observeras att antalet faktiska användare som berörs i praktiken är mycket större eftersom flera användare kan vara uppkopplade under ett abonnentnamn, t.ex. familjemedlemmar, gäster hos ett café med Internetuppkoppling, och medlemmar i bostadsrättsföreningar som erbjuder delat abonnemang. Bahnhof anser att ett utlämnande av lagrade uppgifter enligt föreläggandet utan förhandskontroll av domstol eller oberoende myndighet strider både mot EU-rätten och Europadomstolens praxis. Föreläggandet ska därför anses sakna rättsverkan och följaktligen upphävas.

5. Det strider mot proportionalitetsprincipen att Bahnhof ska tvingas lämna ut mängder med abonnentuppgifter i stället för att polisen anger portnummer.

Under alla förhållanden anser Bahnhof att PTS föreläggande strider mot proportionalitetsprincipen att Bahnhofs att lämna uppgift om alla kunder som använt en och samma IP-adress vid ett visst tillfälle eftersom det finns ett för alla parter enklare och mer rättssäkert tillvägagångssätt. Polisen kan nämligen i stället för att begära uppgifter om alla kunder som använt en NATad IP-adress ange i sin begäran vilket s.k. portnummer som använts av den användare man vill få uppgifter om.

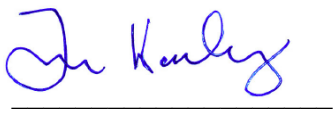
Som nämns i föreläggandet sid 6f har PTS utfärdat egna föreskrifter om att Bahnhof och andra Internetoperatörer ska lagra s.k. portnummer. Avsikten med lagringen av dessa portnummer är att identifiera enskilda användare som använt en NATad IP-adress för att på så sätt underlätta för polis att begränsa antalet uppgifter som var av intresse och dessutom underlätta operatörernas arbete att ta fram begärda uppgifter. En förutsättning för att portnummer på detta sätt skulle förenkla både för polis och operatörer var dock att polisen i en begäran om uppgifter kunde ange portnummer i anslutning till den NATade IP-adress som var av intresse. Som framgår av PTS konsekvensutredning, (se bilaga, sid 6) föregicks PTS föreskrifter om portnummer av samråd både med företrädare för polisen och vissa Internetoperatörer.

Av någon anledning som Bahnhof inte känner till så vill eller kan inte polisen uppge portnummer när man begär ut uppgifter om vilka personer som använt en NATad IP-adress. Tydligen känner inte heller PTS till vad anledningen är till att polisen inte lämnar uppgift om portnummer. Om polisen har svårigheter att ta fram uppgift om portnummer borde detta rimligen ha framkommit under de

samråd som PTS haft med polisen innan PTS föreskrifter om NAT-adresser utfärdades. PTS borde istället för att vitesförelägga Bahnhof begära en förklaring till polisens ovilja eller oförmåga att ange portnummer. Resultatet av PTS passivitet har nu istället blivit dels att Bahnhof och andra operatörer tvingats införa dyrbara system för lagring av portnummer som inte använts eftersom polisen inte uppger portnummer i sina förfrågningar, dels att Bahnhof och andra operatörer tvingas lägga ner ett betydande merarbete för att få fram de alla de uppgifter som polisen begär om de kunder som använt NATade IP-adresser, och dels det integritetsintrång som drabbar alla de kunder vars uppgifter måste lämnas till polisen trots att det absoluta flertalet inte har något med polisens utredning att göra. Så länge polisen har möjlighet att ange portnummer i sina framställningar är det mot ovanstående bakgrund oskäligt och onödigt att påtvinga Bahnhof att lämna ut uppgifter på det sätt som framgår av föreläggandet. Föreläggandet ska därför anses strida mot proportionalitetsprincipen och sakna rättsverkan och följaktligen upphävas.

Särskilda grunder för inhibitionsyrkandet

Bahnhof anser att bristerna i PTS föreläggande är så graverande att det finns en betydande grad av sannolikhet för att beslutet kommer att upphävas. Åtminstone framstår utgången som oviss. För Bahnhof innebär föreläggandet en betydande risk för skada beroende framför allt på föreläggandets otydlighet och att man tvingas lämna ut annars sekretessbelagd information i strid med EU-domstolens och Europadomstolens praxis. För berörda kunder hos Bahnhof finns risk för betydande skada bestående i det integritetsintrång det innebär att uppgifter lämnas ut i strid med EU-rätten och Europakonventionen. Någon motsvarande skada för PTS eller brottsbekämpande myndigheter om inhibition meddelas kan inte förutses. Det är ingen skada att svenska myndigheter måste följa klar och tydlig EU-rätt.



Jon Karlung, VD
Bahnhof AB

Bilaga

Nätsäkerhetsavdelningen

Konsekvensutredning avseende förslag till Post- och telestyrelsens föreskrifter om vilka andra uppgifter som ska lagras för att identifiera abonnent och registrerad användare vid användning av NAT-teknik

Post- och telestyrelsen

Postadress:
Box 5398
102 49 Stockholm

Besöksadress:
Valhallavägen 117 A
www.pts.se

Telefon: 08-678 55 00
Telefax: 08-678 55 05
pts@pts.se

Innehåll

1 Bakgrund

1.1 Inledning

Regeringen beslutade i februari 2017 att ge en särskild utredare i uppdrag att se över bestämmelserna om skyldigheten att lagra uppgifter om elektronisk kommunikation (s.k. datalagring) som gäller för leverantörer av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster samt de brottsbekämpande myndigheternas tillgång till sådana uppgifter (dir 2017:16). Syftet var bl.a. att anpassa det svenska regelverket om datalagring till EU-rätten såsom den uttolkats av EU-domstolen i den s.k. Tele2-domen[1].

Utredningen om datalagring och EU-rätten överlämnade i oktober 2017 delbetänkandet Datalagring – brottsbekämpning och integritet (SOU 2017:75) till regeringen. Utredningen lämnade flera förslag till ändringar bl.a. i lagen (2003:389) om elektronisk kommunikation (LEK) och i förordningen (2003:396) om elektronisk kommunikation (FEK).

I april 2019 överlämnade regeringen propositionen Datalagring vid brottsbekämpning – anpassningar till EU-rätten (prop. 2018/19:86) till riksdagen. I propositionen föreslår regeringen anpassningar av regleringen om lagring och tillgång till uppgifter om elektronisk kommunikation i brottsbekämpande syfte som syftar till att göra reglerna förenliga med EU-rätten på området.

Riksdagen beslutade den 19 juni 2019 att anta regeringens föreslagna lagändringar (bet. 2018/19:JuU27 och rskr. 2018/19:296). Regeringen har därefter den 27 juni 2019 beslutat om kompletterande förordningsändringar.

Lag- och förordningsändringarna träder huvudsakligen i kraft den 1 oktober 2019. Lagringsskyldigheten i 40 § första stycket 1 FEK avseende andra uppgifter som är nödvändiga för att identifiera abonnent och registrerad användare vid internetåtkomst träder dock i kraft den 1 april 2020.

Post- och telestyrelsen (PTS) får enligt 44 § FEK meddela närmare föreskrifter om vilka uppgifter som ska lagras enligt 40 § FEK.

Ändringen i 40 § första stycket 1 FEK har gjorts för att säkerställa att valet av tekniklösning hos internetleverantören inte ska omöjliggöra för de brottsbekämpande myndigheterna att spåra användaren bakom en ip-adress. På grund av brist på ip-adresser enligt den nuvarande huvudsakliga standarden (IPv4) använder många internetleverantörer sig av s.k. NAT[2]-teknik. Tekniken innebär att flera användare delar på en och samma publika ip-adress. I sådana fall räcker det inte att bara lagra användarens ip-adress för att det ska vara

[1] EU-domstolens dom den 21 december 2016 i de förenade målen C-203/15 och C-698/15.
[2] Network Address Translation

möjligt att identifiera abonnent och registrerad användare, utan även andra uppgifter behöver lagras.

Enligt Utredningen om datalagring och EU-rätten, kan det eftersom det är fråga om ett offentligrättsligt åliggande gentemot de lagringsskyldiga finnas en poäng i att mer tydligt ange exakt vilka uppgifter som ska lagras i författningstext. Eftersom den tekniska utvecklingen snabbt kan förändra förutsättningarna för vad som behöver lagras bör den exakta tekniska utformningen av lagringsskyldigheten fastställas i myndighetsföreskrifter utfärdade av PTS. Ramarna av föreskriftsrätten bör dock alltjämt finnas i lag och förordning.[3]

Det finns således en förväntan från lagstiftaren och regeringen om att PTS ska ta fram föreskrifter som förtydligar vilka uppgifter som ska lagras för att kunna identifiera abonnent och registrerad användare. Även hos internetleverantörer och brottsbekämpande myndigheter finns förväntningar om tydliggörande föreskrifter.

PTS ser således ett behov av att i föreskrifter förtydliga och klargöra vilka andra uppgifter som är nödvändiga att lagra för att identifiera abonnent och registrerad användare vid användningen av den teknik som i dagsläget används för att hantera bristen på ip-adresser, dvs. NAT-tekniken.

Den tekniska utvecklingen inom området går fort. PTS följer utvecklingen och har beredskap för att kunna se över föreskrifterna i den mån nya tekniska lösningar införs som ger upphov till att föreskrifterna kan behöva förändras.

Förslag till föreskrifter bifogas, se bilaga 1.

1.2 Rättslig reglering[4]

Den centrala bestämmelsen om lagringsskyldighetens omfattning finns i 6 kap. 16 a § LEK.

Enligt 6 kap. 16 a § LEK är den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § skyldig att lagra sådana uppgifter som avses i 20 § första stycket 1 och 3 som är nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut.

[3] SOU 2017:75 sid. 247.
[4] I dess lydelse fr.o.m. den 1 april 2020 (SFS 2019:497, SFS 2019:500 och SFS 2019:501).

Skyldigheten att lagra uppgifter omfattar uppgifter som genereras eller behandlas vid bl.a. internetåtkomst.

Av 38 § FEK följer att för att uppfylla lagringsskyldigheten i 6 kap. 16 a § LEK ska den lagringsskyldige lagra de uppgifter som anges i 39-40 §§.

Av 40 § FEK följer att när det gäller internetåtkomst ska följande lagras:
1. användares ip-adress och andra uppgifter som är nödvändiga för att identifiera abonnent och registrerad användare,
2. uppgifter om abonnent och registrerad användare,
3. datum och spårbar tid för på- och avloggning i tjänsten som ger internetåtkomst, och
4. uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten.
Om den som slutligt avskiljer kommunikationen till den enskilda abonnenten är någon som inte omfattas av 6 kap. 16 a § lagen (2003:389) om elektronisk kommunikation, ska första stycket 4 gälla för den som avskiljer kommunikationen till den som slutligt avskiljer kommunikationen till den enskilda abonnenten.

Av 16 kap. 16 d § första stycket, andra strecksatsen LEK följer att uppgifter som genereras eller behandlas vid internetåtkomst ska lagras i tio månader. Om uppgifterna identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten ska de dock lagras i endast sex månader.

2 Beskrivning av problemet och vad PTS vill uppnå

2.1 Problembild och syftet med föreskrifterna

Enligt 6 kap. 16 a § andra stycket LEK ska uppgifter som genereras och behandlas vid internetåtkomst lagras. I likhet med vad som gäller för telefonitjänst och meddelandehantering omfattar lagringsskyldigheten uppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan. Vid internetåtkomst finns det alltså enligt lagen en skyldighet att lagra uppgifter som gör det möjligt att identifiera abonnenten eller den registrerade användaren, t.ex. ip-adress och andra tekniska uppgifter som är nödvändiga för identifiering av abonnenten eller den registrerade användaren.

För utredningen av brott begångna över internet är sådana uppgifter om abonnemang, dvs. vilken person som innehar en specifik ip-adress eller annan unik användaradress vid varje tillfälle, enligt regeringen, den absolut viktigaste informationen. Sådan information är vidare, enligt regeringen, nödvändig för att kunna få fram identiteten på den som över internet t.ex. tillgängliggör barnpornografi eller upphovsrättsskyddat material, säljer narkotika och vapen, hotar och förtalar, tar kontakt med barn i sexuellt syfte eller gör dataintrång och andra digitala attacker mot privatpersoner, företag eller myndigheter. Nyttan av

uppgifterna är således enligt regeringen mycket stor. Det saknas dessutom i praktiken ofta andra möjligheter att identifiera en aktör på internet än genom uppgift om ip-adress i kombination med andra uppgifter om abonnemang.

På grund av brist på ip-adresser enligt den nuvarande huvudsakliga standarden (IPv4) har s.k. NAT-teknik kommit att användas av vissa internetleverantörer för att de tillgängliga ip-adresserna ska räcka för att koppla upp alla abonnenter. Tekniken innebär att flera abonnenter kan dela på en och samma publika ip-adress. Detta har inneburit att det inte är möjligt att ta reda på användaren bakom kommunikationen enbart genom att få del av vilken ip-adress som använts. Att valet av teknisk lösning hos internetleverantörerna är avgörande för om det går att spåra en brottsmisstänkt eller inte framstår enligt regeringen som orimligt och även oavsiktligt. Regeringen har därför genom ändringar i bestämmelsen i 40 § FEK beslutat att, utöver användares ip-adress, även andra uppgifter som är nödvändiga för att identifiera abonnent och registrerad användare ska lagras.[5]

Utredningen som legat till grund för regeringens författningsförslag betonar att en på så sätt utformad teknikneutral bestämmelse har fördelar även utifrån den lagringsskyldiges perspektiv, eftersom det blir tydligt att det finns en skyldighet att lagra uppgifter som möjliggör identifikation av abonnenten. Nackdelen är enligt utredningen att lagringsskyldighetens exakta omfattning inte går att utläsa direkt ur författning. Eftersom det är fråga om ett offentligrättsligt åliggande gentemot de lagringsskyldiga kan det därför enligt utredningen finnas en poäng i att mer tydligt ange exakt vad som ska lagras[6].

Utredningen anför vidare att, eftersom den tekniska utvecklingen snabbt kan förändra förutsättningarna för vad som behöver lagras, bör den exakta tekniska utformningen av lagringsskyldigheten fastställas i myndighetsföreskrifter.

Regeringen har, i enlighet med utredningens förslag, förtydligat PTS bemyndigande i 44 § FEK så att PTS får meddela närmare föreskrifter om vilka uppgifter som ska lagras enligt 40 § FEK. Med stöd av denna bestämmelse föreskriver PTS vilka uppgifter som ska lagras vid internetåtkomst enligt 40 § första stycket 1. FEK. Genom föreskrifterna, se bilaga 1, klargörs lagringsskyldighetens närmare omfattning.

2.2 Möten med berörda organisationer

PTS har haft möten med brottsbekämpande myndigheter, internetleverantörer och andra tjänsteleverantörer för att få en bild av de olika tekniska lösningar som används samt vilka uppgifter som är nödvändiga att lagra för att identifiera en abonnent i samband med användningen av NAT-teknik. Mötena som har hållits har varit med representanter från följande aktörer: Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Telia Company AB, Tele2 Sverige

[5] Se prop. 2018/19:86 sid. 43 ff och SFS 2019:501.
[6] Se SOU 2017:75 sid 247 ff.

AB, Telenor Sverige AB, Hi3G Access AB, Bahnhof AB, Netett Sverige AB, Stadsnätsföreningen, Viasat, Ownit Broadband AB, Verizon Sweden AB, Maintrac, Finansiell id teknik (Bankid) och Blocket.

Vid mötena har framkommit att internetleverantörerna använder sig av olika tekniska lösningar. Samtliga internetleverantörer som PTS träffat har påtalat vikten av att kunna matcha uppgifterna som lagras med information som de brottsbekämpande myndigheterna har tillgång till för att det ska vara möjligt att identifiera en abonnent. Det gör att det också ställs krav på att de brottsbekämpande myndigheterna har ett fullgott underlag vid förfrågningar. Mot bakgrund av vad som framkommit i samband med mötena kan PTS konstatera att det finns ett behov av att ta fram föreskrifter som förtydligar lagringsskyldigheten i samband med användningen av NAT-tekniken. Nedan redovisas utförligare vad som framkommit i samband med möten med internetleverantörerna och övriga aktörer.

2.3 Tilldelning av IP-adresser

Med ip-adress avses en adress som används för identifiering och kommunikation mellan två datorer på internet med hjälp av Internet Protocol-standarden (IP). För att kommunicera med IP behöver en dator minst en ip-adress. Enheter av olika slag t.ex. datorer, smarta telefoner och bredbandroutrar kan konfigureras av användaren att använda en fast (statisk) ip-adress eller att automatiskt (dynamisk) ta emot en ip-adress. Dynamisk tilldelning är den vanligaste metoden för konsumentutrustning. Varje lokalt nätverk har i regel tjänsten DHCP[7] för dynamisk tilldelning av ip-adresser. En enhet som använder DHCP efterfrågar en ip-adress när den slås på eller ansluter till ett nytt nätverk. En server som delar ut ip-adresser med hjälp av DHCP på ett nätverk svarar med att erbjuda enheten att låna en ip-adress under en viss angiven tid. Tiden för att låna en ip-adress kan variera mellan ett par timmar upp till flera veckor. I vissa situationer behåller en enhet sin ip-adress mycket längre än så. I t.ex. fibernätverk till bostäder är det vanligt att bredbandsroutern behåller samma ip-adress från internetleverantören i flera år. Om enheten kopplar ner och ansluter på nytt senare får den ofta samma ip-adress igen eftersom DHCP-servern kommer ihåg vilken hårdvara som haft vilken ip-adress, även om lånet gått ut. Den nu rådande versionen av standarden, IPv4, ger utrymme (har en adressrymd) för maximalt 4 294 967 296 unika ip-adresser (2^{32}). Vissa av dessa adresser (delmängder av adressrymden) är reserverade för särskilda ändamål. Övriga adresser är utdelade till olika organisationer och det finns inga fler adresser att få.

Den ip-adress som en internetleverantör tilldelar en smarttelefon eller en bredbandrouter när den ansluts till ett ip-nätverk kan användas för att nå internet. I normala fall, dvs. när NAT-teknik inte används är en sådan ip-adress publik, dvs. den är unik och kan nå, och nås över, hela internet.

[7] Dynamic Host Configuration Protocol

I ett sådant fall kan brottsbekämpande myndigheter i samband med brottsutredningar relativt enkelt identifiera vem som använt en ip-adress. Ett enkelt scenario är att någon har lämnat ett elektroniskt spår efter sig i form av en ip-adress i en loggfil på en webbserver någonstans. Om internetleverantören lagrar uppgifter om varje gång en internetanvändare (abonnent) får en ip-adress tilldelad till sin utrustning med DHCP, kan polisen gå till internetleverantören med denna ip-adress och fråga vem (vilket abonnemang) som haft ip-adressen vid ett visst tillfälle. Vilken internetleverantör som har tilldelat en viss ip-adress, dvs. är innehavare av adressrymden, är publikt tillgänglig information. Om NAT-teknik inte används blir mängden lagrade uppgifter hos internetleverantören begränsad, eftersom adresserna tilldelas sällan. Matchningen av ip-adressen mot de lagrade uppgifterna blir okomplicerad.

2.4 Närmare om NAT-teknik och Carrier-Grade NAT

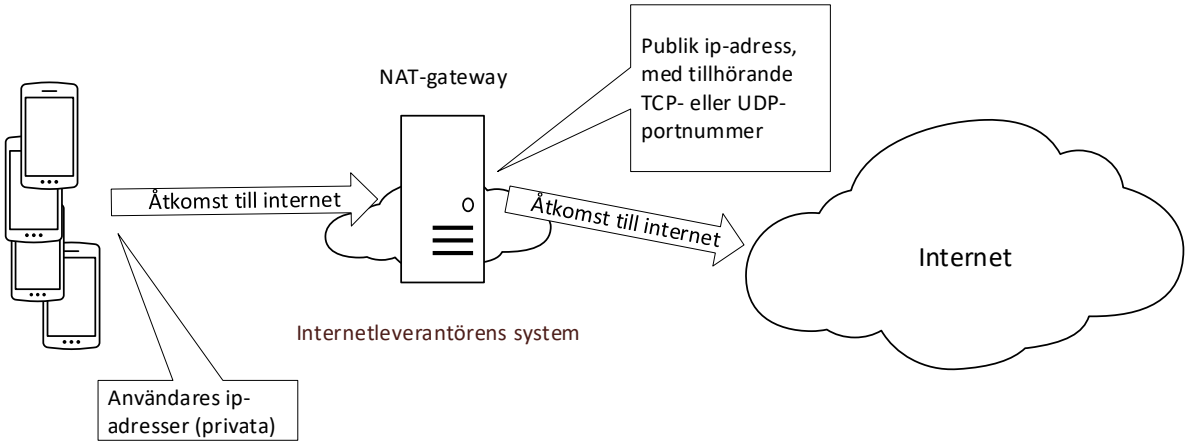
NAT-teknik är, som framgått ovan, en teknik som gör det möjligt att ansluta många datorer/terminaler till internet med användning av en eller några få gemensamma publika ip-adresser. NAT är en förkortning av Network Address Translation. NAT är en funktion som vanligen byggs in i en brandvägg eller router som ansluter ett lokalt nätverk till internet. I det lokala nätverket används ip-adresser reserverade för detta ändamål, som inte kan användas på det öppna publika nätet (s.k. privata adresser eller svarta adresser). NAT-tekniken används vanligen av privatpersoner och företag, som kopplar upp sitt lokala nätverk mot internet. På grund av bristen på IPv4-adresser så har emellertid NAT-teknik även kommit att användas av internetleverantörer, för att de tillgängliga ip-adresserna ska räcka till att koppla upp alla abonnenter. När internetleverantörer använder NAT kallas detta vanligen för Carrier-Grade NAT (CGNAT), även om termen NAT används vidare i detta dokument.

Eftersom en publik ip-adress i teorin kan delas av upp till 65 535 abonnenter (se nedan för förklaring) med privata ip-adresser, är det inte möjligt att identifiera abonnent och registrerad användare för kommunikationen med ledning av enbart den publika ip-adressen. Internetleverantörernas användning av NAT-teknik syftar alltså till att låta många internetanvändare dela på ett antal publika ip-adresser. Användare tilldelas ip-adresser från en adressrymd som inte är nåbar från internet (de privata ip-adresserna) och som internetleverantören därmed kan hantera fritt. Privata ip-adresser avsedda för CGNAT hör till en annan adressrymd än de ip-adresser som används för NAT hos privatpersoner och företag för att undvika adresskonflikter men funktionen är densamma.

Användarnas internettrafik passerar alltid utrustningen som utför NAT, vanligen någon form av gateway hos internetleverantören. Denna gateway står då mellan användarna och internet och har ett antal publika ip-adresser på sin ”internetsida”, som delas mellan användarna på ”insidan” av gatewayen. Avsändar-ip-adresserna översätts från privata till publika i gatewayen när trafiken passerar ut genom den.

En ”användare” i det här sammanhanget kan vara en enstaka smarttelefon eller bredbandsrouter hos en familj vars samtliga mobiltelefoner, datorer, musikspelare, smart-tv-apparater och annat uppkopplat använder samma internetabonnemang för att nå internet.

För att nå tjänster på internet, t.ex. webbservrar, upprättar webbläsare och andra klientprogram förbindelser i form av sessioner som normalt är av typen TCP[8] eller UDP[9]. För att gatewayen ska kunna hålla reda på användarnas förbindelser så tilldelas varje utgående förbindelse ett portnummer som i teorin kan ha ett värde från 1 till 65 535 (2^{16}-1), men i regel används inte de 1 024 lägsta, då de är s.k. reserverade portar. När svaret kommer tillbaka, från exempelvis en webbsida, så använder gatewayen portnumret för att hitta rätt privat ip-adress så att svaret kan skickas till rätt användare. Kopplingen mellan privat ip-adress, publik ip-adress och gatewayens tillhörande (publika) portnummer lagras i minnet på gatewayen så länge som en förbindelse varar, och är relevant bara under den tiden. Att visa förstasidan på en dagstidnings webbsajt genererar minst ett tiotal sådana förbindelser.



För att kunna härleda en publik ip-adress med portnummer till en privat ip-adress vid en viss tidpunkt behöver alltså fyra parametrar - privat ip-adress, publik ip-adress, portnummer och tid - lagras, för varje förbindelse. Hur ofta sådana förbindelser upprättas varierar beroende på användarmönster (fast internet, mobil etc.), men siffror som internetleverantörerna nämnt rör sig mellan 40 000 till 240 000 sessioner per dygn och enhet. En enhet kan vara en smarttelefon eller bredbandsrouter som i sin tur betjänar flera tiotals enheter hemma hos någon.

[8] Transmission Control Protocol
[9] User Datagram Protocol

Vid möten med berörda internetleverantörer har framkommit att det finns skillnader i hur NAT-tekniken har implementerats. Vissa internetleverantörer har relativt gott om publika ip-adresser och kan därför låta en mindre mängd användare, t.ex. 64 stycken, dela på en publik ip-adress vilket ger varje användare upp till 1 000 portar (64 000/64 = 1 000). Andra leverantörer kan ha färre publika ip-adresser, alternativt så många användare att varje ip-adress måste delas av många. Siffror över 60 000 har nämnts, d.v.s. nära den teoretiska maxgränsen på 65 535 användare. I övrigt ligger internetleverantörernas uppskattningar på mellan 64 och ca 3 000 användare per ip-adress.

Ett portnummer med tillhörande publik ip-adress tilldelas alltså varje förbindelse i samband med att den upprättas. Vilket portnummer en förbindelse får kan bestämmas då den upprättas men kan även, beroende på utrustning, tilldelas i block i förväg och kopplas till ip-adresserna. Då får en användare med en given privat ip-adress ett block portnummer med t.ex. 500 portar att disponera på en publik ip-adress. Blockstorleken kan anpassas vid behov efter användarnas trafikmönster så att nya block inte behöver tilldelas så ofta. Blocken behöver inte vara sammanhängande, utan kan vara spridda över det tillgängliga spannet portar. Möjligheten att tilldela portar i block kan minska mängden data som behöver lagras avsevärt, eftersom det då bara blir nödvändigt att logga när ett block tilldelas, jämfört med att logga varje gång en port används.

2.5 PTS sammanfattande bedömning

PTS bedömer, mot bakgrund av vad som beskrivits om tekniken i avsnitt 2.3-2.4 samt utifrån vad som framkommit vid de möten som PTS haft med inblandande aktörer, att det som behöver lagras för att kunna identifiera abonnent och registrerad användare när NAT-teknik används är privat ip-adress (användares ip-adress), korresponderande publik ip-adress med tillhörande portnummer, samt spårbar tidpunkt för tilldelning av portnumret. Med portnummer avses här portnumret som hör till den publika ip-adress som internetleverantörens NAT-gateway ger användarens förbindelse (alltså TCP- eller UDP-session). Den tidpunkt som ska lagras är tidpunkten för tilldelning av portnummer för en viss förbindelse alternativt tidpunkten för tilldelning av ett block portnummer i förväg. I föreskriften uttrycks detta som att den lagringsskyldige ska lagra uppgifter om publik ip-adress med tillhörande UDP- eller TCP-portnummer kopplat till användares ip-adress och spårbar tid för kopplingen.

Det bör i detta sammanhang också påpekas att det av förarbetena[10] framgår att inga uppgifter om destination t.ex. besök på webbplatser omfattas av lagringsskyldigheten. Sådana uppgifter är operatörerna skyldiga att förstöra om de inte har rätt att lagra dem för vissa egna ändamål.

[10] SOU 2017:75 sid. 248 och prop. 2018/19:86 sid. 43.

2.6 Kort om IPv6

Internet Protocol version 6 (IPv6) är avsett att ta över efter IPv4. IPv6 innebär att antalet tillgängliga ip-adresser ökar i enorm omfattning. På sikt kan därför övergången till IPv6 innebära att behovet av att hantera bristen på IPv4 adresser genom användningen av NAT-teknik minskar. Såvitt framkommit i samband med möten med internetleverantörer har man beredskap för och arbetar med frågor relaterade till övergången till IPv6 men den bedöms inte ske inom de närmaste åren. Under en övergångsperiod kommer dessutom IPv4 och IPv6 behöva användas parallellt för att användarna ska kunna adressera servrar som endast använder sig av IPv4. Vissa internetleverantörer tilldelar både IPv4- och IPv6-adresser till sina användare redan i dag, men samtliga internetleverantörer som PTS har varit i kontakt med uppger att IPv4-adresser kommer att behöva finnas kvar under överskådlig framtid. I princip kommer IPv4-adresser behöva användas av internetleverantörerna så länge som det finns servrar kvar på internet som bara kan nås med IPv4. Således kommer det att finnas ett behov av att i föreskrifter reglera vilka uppgifter som ska lagras vid användningen av NAT-teknik.

3 Alternativa lösningar och effekter om några föreskrifter inte kommer till stånd

PTS gör bedömningen att om inga föreskrifter tas fram riskerar tillämpningen att variera mellan olika lagringsskyldiga beroende på den tolkning som den berörda lagringsskyldige gör av den aktuella bestämmelsen. I en sådan situation skulle PTS i efterhand genom tillsyn och beslut i enskilda ärenden få försöka tillse en enhetlig tillämpning. Eftersom det förfarandet skulle ske över tid finns det en betydande risk att flertalet lagringsskyldiga då anpassat sina tekniska system utifrån de skyldigheter de bedömde förelåg när lagen trädde i kraft. Det skulle kunna innebära att större förändringar i rutiner och tekniska lösningar skulle behöva utföras när väl bestämmelsens tillämpning tydliggjorts genom tillsyn. Detta skulle kunna leda till större kostnader än om reglerna kring lagringsskyldigheten tydliggörs redan från början genom föreskrifter.

Det finns också en betydande risk att vissa lagringsskyldiga tolkar bestämmelserna på ett sådant sätt att de lagrar för få uppgifter så att syftet med bestämmelsen inte uppnås, d.v.s. att identifiering av abonnent eller användare inte kan ske med hjälp av de uppgifter som lagrats vilket påverkar möjligheterna att utreda och lagföra bl.a. grov brottslighet.

I en situation med oklar omfattning av lagringsskyldigheten kan också tänkas att lagring sker av uppgifter som inte ska och inte heller får lagras eller behandlas.

3.1 Proportionalitetsbedömning

Av förarbetena[11] framgår att endast sådana uppgiftskategorier vars information är påtagligt viktiga för brottsbekämpningen och som inte är möjliga att få del av genom en mindre ingripande åtgärd ska lagras. Både informationen och lagringen måste alltså vara nödvändiga. Lagringen får således enligt regeringen inte omfatta uppgifter som sällan eller aldrig inhämtas eller för vilka nyttan eller behovet inte är stort. Det är inte heller tillräckligt att den lagrade uppgiften allmänt sett är användbar eller bra att ha för de brottsbekämpande myndigheterna.

Såsom regeringen har betonat måste lagringen av uppgifter balanseras mot nyttan som de lagrade uppgifterna ger de brottsbekämpande myndigheterna. Endast uppgifter som är nödvändiga ska lagras. Det innebär enligt PTS bedömning att lagringen inte bör omfatta uppgifter som de brottsbekämpande myndigheterna inte har nytta av på grund av att de inte har tillgång till motsvarande uppgifter från aktuell webbplatsinnehavare.

Det är således av stor vikt att brottsutredande myndigheter har ett bra underlag. En konsekvens av att sessioner är så många och har så kort livslängd, är att en enskild session är svår att peka ut. Därför behövs en noggrann tidsangivelse för när en viss session har existerat från den som utreder ett brott. Även om ett portnummer ingår i underlaget (tillsammans med ip-adress) så kan en osäker tidsangivelse innebära att en abonnent eller registrerad användare felaktigt pekas ut, inte går att spåra alls, eller att en viss förfrågan kommer att avse väldigt många abonnenter eller registrerade användare.

PTS har i samband med möten med berörda brottsbekämpande myndigheter kunnat konstatera att mängden uppgifter dessa myndigheter har tillgång till när de gör förfrågningar till internetleverantörer varierar i hög grad.

PTS har vidare fått indikation på att när det handlar om grova brott, där information inhämtas genom t.ex. underrättelseverksamhet är det vanligare att brottsbekämpande myndigheter har tillgång till fler och mer exakta uppgifter. En lagringsskyldighet för internetleverantörerna kommer därmed att innebära att fler abonnenter eller registrerade användare kommer att kunna identifieras vid utredning av grova brott, vilket rimligtvis bör innebära större möjligheter till lagföring.

PTS konstaterar sammanfattningsvis, utifrån vad som framkommit i kontakterna med de brottsbekämpande myndigheterna, att sådana uppgifter som gör det möjligt att identifiera att en viss abonnent eller användare har använt sig av en adressöversatt ip-adress i många fall varit av påtaglig vikt för en framgångsrik brottsbekämpning. I flera fall har det inte varit möjligt att få fram information om den berörda användaren genom en annan, mindre ingripande

[11] Se prop. 2018/19:86 sid. 35.

åtgärd. Enligt PTS är det därför nödvändigt och proportionerligt att lagra de uppgifter som redovisas ovan, se avsnitt 2.5.

4 Uppgifter om vilka som berörs av regleringen

4.1 Berörd bransch och kategori av företag

Av 2 kap. 1 § LEK jämförd med 6 kap. 16 a § LEK följer att den som är anmälningspliktig enligt LEK också är skyldig att lagra uppgifter om abonnemang eller andra uppgifter som angår ett särskilt elektroniskt meddelande (trafikuppgifter) för brottsbekämpande ändamål. Anmälningsplikt enligt 2 kap. 1 § LEK gäller för den som tillhandahåller allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster.

Marknaden för elektronisk kommunikation består av aktörer som bedriver en mängd olikartade verksamheter. Det finns nätägare som endast tillhandahåller passiv infrastruktur, dvs. fibern är inte tänd (en s.k. svartfiberleverantör). Därtill finns nätägare i grossistledet som tillhandahåller aktiv infrastruktur till operatörer. Därutöver finns en stor variation av operatörer när det gäller utbudet av olika typer av tjänster. En del är operatörer som tillhandahåller telefoni i form av fasta och mobila telefoni- och internettjänster. De aktuella föreskrifterna berör i praktiken främst mobiloperatörer som tillhandahåller internetaccess och ett fåtal tillhandahållare av fast internetaccess som använder sig av en NAT-lösning.

Utöver de direkt berörda av själva skyldigheten att lagra uppgifter dvs. internetleverantörerna berörs också Polismyndigheten och övriga brottsbekämpande myndigheter. Som framgår ovan kommer detta att i förlängningen rimligtvis innebära att förutsättningarna att utreda brottslighet förbättras. Samtidigt ökar kraven på de brottsbekämpande myndigheterna att få fram fullgoda underlag.

4.2 Antalet företag som berörs och storleken på företagen

Marknadsandelar på mobilabonnemang inkluderar mobilabonnemang med samtal och data, mobilabonnemang med endast samtal och mobilt bredband med endast data. De fyra största aktörerna, Telia Company, Tele2, Telenor och Hi3G (Tre), hade sammanlagt 96% av abonnemangen som totalt uppgick till 10,6 miljoner abonnemang (samtal och data).

När det gäller fast bredband kan konstateras att det fanns 3,9 miljoner abonnemang. Marknadsandelarna för de fem största leverantörerna var följande: Telia Company (33,2%), ComHem (21,3%), Telenor (17,4%), Bahnhof (6,9%) och Bredband 2 (6,0%) samt övriga (15,2%). Ovanstående uppgifter är hämtade från PTS promemoria ”Svensk telekommarknad första halvåret 2018”, Dnr 18-790.

Huvuddelen av de aktiva anslutningarna av internettjänster återfinns således hos ett litet antal tjänstetillhandahållare. När det gäller den lagringsskyldighet som förtydligas i de aktuella föreskrifterna bör det noteras att dessa endast berör de internetleverantörer som använder sig av NAT-teknik. Såvitt PTS kunnat utreda är detta en teknik som i dagsläget främst används av mobiloperatörer som tillhandahåller internetaccess och i några fall leverantörer av internettjänster via fast bredband.

5 Uppgifter om vilka kostnadsmässiga och andra konsekvenser föreskrifterna medför

5.1 Inledning

I propositionen Datalagring vid brottsbekämpning – anpassningar till EU-rätten anges att för de lagringsskyldiga inom sektorn för elektronisk kommunikation kommer en förändrad lagringsskyldighet innebära att datasystemen behöver anpassas till de nya förutsättningarna. Detta är en kostnadsdrivande faktor för företagen. För de internetleverantörer som använder NAT-teknik innebär lagringsskyldigheten att de kommer att behöva anpassa sina system och lagra fler uppgifter än förut, vilket innebär kostnadsökningar. Dels krävs en engångsinvestering i form av ombyggnad av systemen för en del operatörer, dels krävs större kapacitet vad gäller lagringsutrymme vid en mer omfattande lagring. Hur stora kostnadsökningar det kan bli fråga om har operatörerna enligt utredningen inte kunnat kvantifiera. Å ena sidan har några operatörer uppgett för utredningen att en sådan förändring skulle medföra att kostnaderna skulle skjuta i höjden och hamna på helt orimliga nivåer. Å andra sidan har någon operatör uppgett att systemet i princip redan finns på plats, eftersom NAT-tekniken infördes medan datalagringsdirektivet fortfarande var gällande.[12]

PTS kan bekräfta ovanstående beskrivning utifrån vad som framkommit vid PTS möten med operatörerna.

Det är alltså svårt att kvantifiera hur stora kostnaderna kan komma att bli, men PTS delar regeringens bedömning att kostnaderna bedöms öka för de operatörer som använder sig av NAT-teknik.

5.2 Administrativa kostnader för företag

Flera operatörer har vid mötena med PTS framfört att PTS föreskrifter och allmänna råd (PTSFS 2012:4) om skyddsåtgärder i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål kommer att medföra ökade administrativa kostnader vid lagring av uppgifter som är nödvändiga för att identifiera abonnent och registrerad användare. PTS vill i

[12] Se prop. 2018/19:86 sid. 109-110

detta sammanhang klargöra att dessa kostnader huvudsakligen uppstår som en följd av att administrativa åtgärder vidtas för att upprätthålla skydd av uppgifter som faller inom ramen för lagringsskyldigheten generellt och att kostnaderna således inte är direkt hänförliga till användningen av NAT-tekniken.

Några internetleverantörer har uppgett att sökning av NAT-relaterade uppgifter i databaser är mer avancerat än den sökning som görs när NAT-teknik inte används vilket därmed kräver kvalificerad personal. Det kan dessutom antas att detta ställer större krav på utbildningsinsatser och även utförligare dokumentation av t.ex. söksystem. Leverantörerna har inte kunnat ange några närmare kostnadsuppskattningar för detta.

När lagringen sker hos en underleverantör på uppdrag av den lagringsskyldige så torde detta innebära att de egna kostnaderna för lagringsskyldigheten begränsas men att det å andra sidan uppkommer vissa administrativa kostnader som hänför sig till ingående av avtal och kontroll av att uppdragstagaren uppfyller de säkerhetskrav som gäller enligt avtal, lag och PTS föreskrifter.

Antalet förfrågningar om utlämnande av uppgifter om vem som vid ett visst tillfälle haft ett visst IP-nummer kan antas öka på sikt för internetleverantörerna när de brottsutredande myndigheterna får bättre möjligheter att bedriva brottsutredningar i och med att uppgifter hänförliga till NAT-tekniken sparas och kan lämnas ut. Internetleverantörerna får dock ersättning baserad på PTS föreskrifter (PTSFS 2013:5) om ersättning vid utlämnande av lagrade uppgifter för brottsbekämpande ändamål, fortsättningsvis benämnda ersättningsföreskrifterna. Detta innebär att leverantörerna får en generell ersättning baserad på uppskattad arbetsinsats i samband med utlämnande av uppgifter. Av konsekvensutredning som utfördes i samband med framtagandet av ersättningsföreskrifterna[13] framgår hur ersättningen för denna arbetsinsats har beräknats. Av ersättningsföreskrifterna framgår att ersättning utgår från två olika kategorier av utlämnanden. Kategori 1 avser utlämnanden av lagrade uppgifter som är hänförliga till ett visst geografiskt område och kategori 2 avser övriga utlämnanden av lagrade uppgifter. Den förstnämnda typen av utlämnande bedöms kräva mer utredningsinsatser för den berörda operatören och därmed utgår en högre ersättning, vilken uppgår till 525 kronor per utlämnande under kontorstid (efter kontorstid är ersättningen 790 kronor). För utlämnande enligt kategori 2, vilka typiskt avser uppgifter om abonnemang, utrustning eller samtals-/sessionslistor, utgår en ersättning om 150 kronor under kontorstid och 170 kronor utanför kontorstid. Inbakat i dessa ersättningsnivåer ligger också kostnaderna för sökverktyg och mjukvara samt personalkostnader för drift och underhåll av de tekniska systemen.

En förfrågan avseende NAT-relaterade uppgifter torde i normalfallet avse ett utlämnande av uppgifter ur kategori 2 och det kan antas att vissa ytterligare moment tillkommer för att få fram efterfrågade uppgifter jämfört med tidigare.

[13] Se PTS dnr. 12-4585

Vidare kan det vara nödvändigt att genomföra vissa tekniska förändringar och utbyte eller uppgradering av den programvara som används. PTS bedömer dock att dessa eventuella ytterligare kostnader får beaktas inom ramen för en kommande översyn av ersättningsföreskrifterna.

Ersättningsföreskrifterna ger dessutom utrymme för berörd internetleverantör att i det enskilda fallet begära ersättning som motsvarar de faktiska kostnaderna för ett utlämnande i de fall kostnaderna bedöms avvika i väsentlig grad från de ersättningar som utgår enligt föreskrifterna.

5.3 Kostnader för tekniska system m.m.

Som ovan nämnts kommer en förändrad lagringsskyldighet för de lagringsskyldiga inom sektorn för elektronisk kommunikation, innebära att datasystemen behöver anpassas till de nya förutsättningarna.

Beroende på internetleverantörens utrustning, kan ett portnummer tilldelas i samband med att en (TCP/UDP-) session upprättas, vilket innebär att en loggrad skickas för lagring varje gång en sådan session startar. Med tanke på hur ofta sessioner startar kommer då en stor mängd information behöva lagras. Med 240 000 sessioner per dygn och enhet vilket är en siffra som nämnts i samband med möten, blir lagringsvolymen grovt räknat 15 megabyte per dygn och användare och då har inte eventuell redundans eller kompression medräknats. Under en 10-månadersperiod blir det under 5 gigabyte per användare. Ett räkneexempel med 1.5, 3 och 6 miljoner mobilanvändare skulle ge 7.5, 15 och 30 petabyte.

En annan uppgift från en internetleverantör med erfarenhet från en befintlig lösning för NAT-loggning redovisar ca 5 gigabyte loggad data per miljon användare och dygn. Under 10 månader blir det ca 1.5 terabyte per miljon användare. De direkta kostnaderna för maskinvara som klarar av att lagra en sådan mängd uppgifter är i sig inte stora. Det som orsakar kostnader är främst organisatoriska åtgärder och åtgärder kopplade till hanteringen av uppgifterna.

Skillnaden i lagringsvolym på en faktor 1 000 mellan exemplen ovan och uppgiften från internetleverantören förklaras sannolikt med skillnader i användarmönster (t.ex. mobil eller fast internetanslutning), smartare lagring (t.ex. binärt/komprimerat) och att internetleverantörens system tilldelar och loggar portnummer i block.

Om internetleverantörens utrustning konfigureras att tilldela portnummer i block i förväg, får varje användare med en given privat ip-adress ett block portnummer med t.ex. 500 portar att disponera. Blockstorleken anpassas vid behov efter användarnas trafikmönster så att nya block inte behöver tilldelas så ofta.

Tilldelning av portar i block minskar drastiskt behovet av loggning (i vissa fall en faktor 1 000), vilket i sin tur sparar stora mängder lagringsvolym och minskar belastningen på utrustningen i övrigt. Tilldelning i block är förbehållet

de internetleverantörer vars utrustning stöder det och som har tillräckligt få användare per publik ip-adress för att blocken ska vara stora nog att inte ta slut för ofta.

Internetleverantörerna uppger att kostnaden för lagring främst avgörs av hur mycket som redan finns på plats, i form av utrustning, rutiner och personal med rätt kompetens.

En annan faktor som kan påverka kostnaderna är om en viss internetleverantör har verksamhet i flera länder. Exempelvis kan en leverantör som även bedriver verksamhet i länder där krav på lagring av NAT-uppgifter finns sedan tidigare utöka sin tekniska lösning att omfatta även Sverige, till en begränsad kostnad och tidsåtgång jämfört med att skapa ett nytt system.

Som framgår ovan kan användningen av blocktilldelning av portar också innebära kostnadsbesparingar som delvis kan variera beroende på den berörda internetleverantörens förutsättningar i form av antal tillgängliga IPv4-adresser och användarnas trafikmönster.

Sammanfattningsvis bedöms kostnaderna för tekniska system öka för de flesta internetleverantörer som använder sig av NAT-tekniken. Den exakta omfattningen av kostnadsökningen är svår att uppskatta eftersom de tekniska och administrativa lösningarna ser olika ut för de olika internetleverantörerna. De kostnadsökningar som uppstår beror inte i första hand på behovet av ökat lagringsutrymme i form av hårddiskar och annan hårdvara utan kan hänföras till behovet av mer avancerade system för hantering av och sökning i de lagrade uppgifterna och kostnader för anställning och utbildning av personal.

5.4 Jämförelse av konsekvenser för alternativa lösningar

PTS ser inte att det finns något större utrymme för att vidta alternativa åtgärder. Som framgår ovan skulle alternativet att inte meddela några föreskrifter riskera att innebära att vissa internetleverantörer inte lagrar de uppgifter som lagringsskyldigheten innefattar medan andra internetleverantörer kan komma att lagra uppgifter utan legalt stöd vilket innebär en ökad risk för omotiverade integritetsintrång. I en sådan situation skulle PTS genom tillsyn behöva klargöra rättsläget och vissa av de investeringar som skett innan rättsläget klarnat riskerar att bli onödiga. Eftersom lagringsskyldighetens omfattning torde bli densamma efter tillsynsåtgärder som den som framkommer i föreskrifterna torde de nödvändiga investeringarna i slutändan vara desamma. Risken finns dock att vissa investeringar, som skett under mellanperioden innan dess rättsläget klarlagts, kan komma att visa sig vara onödiga.

5.5 Påverkan på konkurrensförhållanden för företagen

De företag som berörs av regleringen verkar på en konkurrensutsatt marknad. Konsumenternas möjligheter att välja mellan olika tjänstetillhandahållare

varierar, dels mellan olika typer av kommunikationstjänster och dels mellan olika platser i landet.

De som huvudsakligen berörs av föreskrifterna initialt är större mobiloperatörer med rikstäckande verksamhet och många abonnenter. I något fall har den berörda operatören redan system på plats som möjliggör NAT-teknik och lagring av de i föreskriften aktuella uppgifterna. I övrigt berörs de större mobiloperatörerna i samma utsträckning och påverkan på befintlig konkurrens torde vara relativt låg.

Som nämnts ovan, beror de kostnadsökningar som uppstår, inte i första hand på ett behov av ökat lagringsutrymme i form av hårddiskar och annan hårdvara utan kan hänföras till behovet av mer avancerade system för hantering av och sökning i de lagrade uppgifterna och kostnader för anställning och utbildning av personal. Dessa kostnader ersätts, som också redovisats för ovan, enligt ersättningsföreskrifterna. När det gäller konkurrenspåverkan i detta sammanhang har PTS tidigare noterat att ersättningsföreskrifterna innebär en tydlighet vad avser vilken ersättning de lagringsskyldiga kan förvänta sig vid utlämning. Det innebär också att den administrativa börda som en specificering och ett styrkande av uppkomna kostnader annars skulle innebära underlättas betydligt. Å andra sidan innebär den schabloniserade kostnaden att den faktiska kostnaden inte i alla fall ersätts fullt ut. De förändringar som föreslås kan antas påverka de företag som verkar på marknaden i varierande utsträckning, beroende på bland annat hur många utlämningsärenden som hanteras och hur utvecklade rutiner som finns kring utlämnandefrågor.

Det finns anledning att tro att mindre internetleverantörer som är lagringsskyldiga har mindre välutvecklade rutiner inom området och att ett utlämnande därför kan kräva en större arbetsinsats vilket i sin tur kan innebära att dessa lagringsskyldiga leverantörers administrativa arbete inte kommer att ersättas helt vid en användning av den schabloniserade ersättningen enligt ersättningsföreskrifterna. Å andra sidan har de mindre leverantörerna också mindre kundstockar vilket torde innebära att de får färre förfrågningar än de leverantörer som har större kundstockar.

I ersättningsföreskrifterna finns också som ovan nämnts en möjlighet att när kostnaderna för ett utlämnade avsevärt avviker från den schabloniserade ersättningen istället begära en ersättning som motsvarar kostnaderna i det enskilda fallet.

När det gäller de mindre företag som tillhandahåller internetaccess i det fasta nätet bedömer PTS således att de kommer att ha huvudsakligen liknande förutsättningar som de större företagen att kunna anpassa sig till de aktuella föreskrifterna. Möjlighet finns dessutom att upphandla och ge någon annan i uppdrag att genomföra lagringen av uppgifterna. De aktuella föreskrifterna bedöms således inte få någon avgörande konkurrenspåverkan inom gruppen tillhandahållare av elektroniska kommunikationstjänster.

5.6 Behovet av särskilda hänsyn till små företag

De brottsbekämpande myndigheternas behov av uppgifter och därmed lagringsskyldighetens omfattning är oberoende av företagens storlek. PTS bedömer mot bakgrund av vad som ovan beskrivits och i likhet med regeringen[14]att både små och stora företag kommer att ha huvudsakligen liknande förutsättningar att anpassa sig till de aktuella föreskrifterna. Det saknas därför anledning att ta särskilda hänsyn till små företag i de nu aktuella föreskrifterna.

Dessutom finns enligt bestämmelsen i 6 kap. 16 b § LEK, i enskilda fall en möjlighet för PTS att besluta om undantag från skyldigheten att lagra uppgifter om det finns synnerliga skäl för det. Bestämmelsen är avsedd att ha en restriktiv tillämpning. PTS ska höra Åklagarmyndigheten, Polismyndigheten och Säkerhetspolisen inför varje beslut om ett eventuellt undantag. PTS har hittills inte beslutat om några undantag, men bestämmelsen skulle kunna aktualiseras bl. a. när det gäller mindre företag.

6 En bedömning av om regleringen överensstämmer med de skyldigheter som följer av Sveriges anslutning till Europeiska unionen

De anpassningar av regelverket gällande lagring och tillgång till uppgifter om elektronisk kommunikation i brottsbekämpande syfte som riksdag och regering genomfört i LEK och FEK, har haft till syfte att göra reglerna förenliga med EU-rätten på området. Riksdag och regering har bedömt att regelverket är förenligt med EU-rätten. De nu aktuella föreskrifterna tydliggör endast, på en närmare nivå och inom ramen för den lagringsskyldighet som riksdagen beslutat, vilka andra uppgifter som är nödvändiga att lagra för att identifiera abonnent och registrerad användare. PTS bedömer mot bakgrund av detta att regleringen överensstämmer med de skyldigheter som följer av Sveriges anslutning till Europeiska unionen.

7 Tidpunkten för ikraftträdande och behovet av speciella informationsinsatser

De förändrade reglerna i 40 § första stycket 1 FEK som tar sikte på att omhänderta det förhållandet att vissa internetleverantörer använder NAT-teknik träder i kraft den 1 april 2020. Det är därför angeläget att föreskrifterna som förtydligar bestämmelsen i förordningen träder i kraft samtidigt.

[14] Se prop. 2018/19:86 sid. 111

PTS har i samband med framtagandet av föreskrifterna fört en dialog med ett flertal av de aktörer vars verksamhet omfattas av bestämmelserna rörande NAT-teknik. PTS avser att lämna ytterligare information om de aktuella föreskrifterna på myndighetens webbplats samt i samband med den information som lämnas till nyanmälda aktörer på marknaden.

8 Övrigt

Underrättelse för anmälan till Europeiska kommissionen

Av 6 § förordningen (1994:2029) om tekniska regler framgår att en myndighet som avser att fatta beslut om en teknisk regel i god tid ska underrätta Kommerskollegium om det förslag som den har utarbetat. Bestämmelserna i förordningen implementerar Sveriges internationella förpliktelser enligt bl.a. Europaparlamentet och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (anmälningsdirektivet).

Enligt PTS bedömning är nu föreslagna föreskrifter inte att se som sådana tekniska föreskrifter som ska anmälas till kommissionen enligt ovan nämnda förordning.

Kontaktpersoner

Peder Cristvall, 08-678 55 29 (sakfrågor)
Sofia Wirlée, (rättsliga frågor)