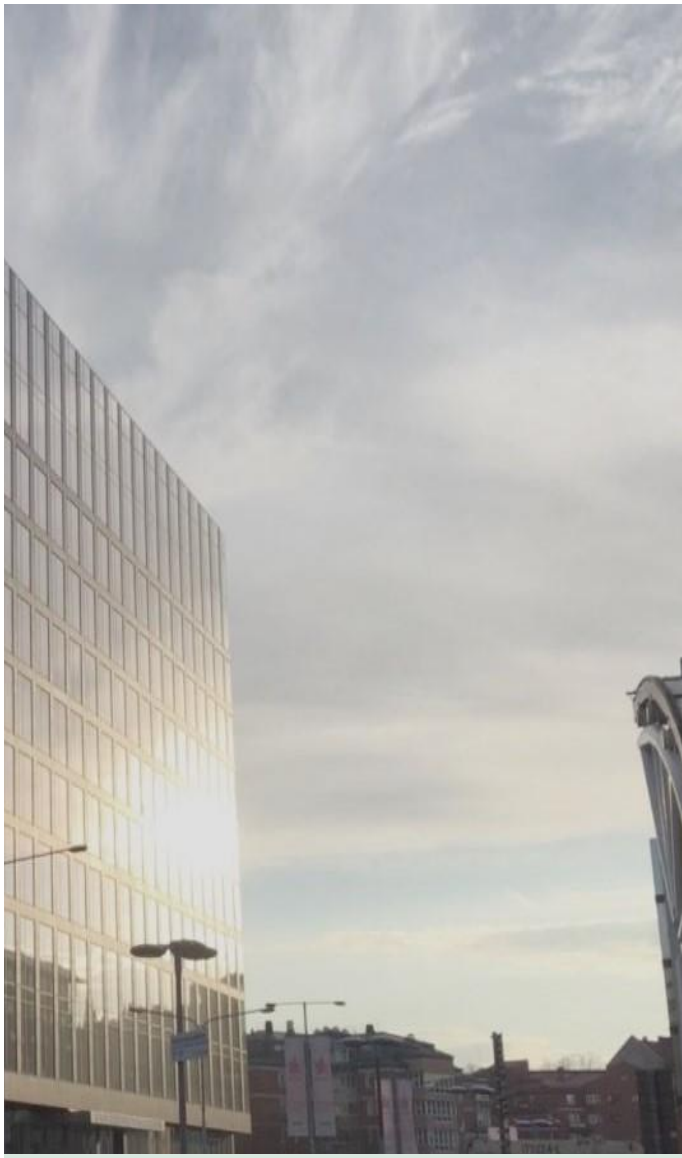
Konsekvensanalys av nya säkerhetskrav vid införandet av 5G



16 DECEMBER

Gröna Städer

Innehållsförteckning

GRÖNA STÄDER

Sammanfattning

Denna rapport är en konskekvensanalys av tillämpningen av säkerhetslagen (2018:585) och nya förändringar i lagen om elektronisk kommunikation. Föreningen Gröna Städer är ensamt ansvarig för rapportens innehåll. Rapporten ifrågasätter inte de säkerhetspolitiska övervägningarna, men anser att konsekvenserna måste vara en del av de fortsatta diskussionerna. Syftet med rapporten är att främja en lösning som både som tillgodoser de säkerhetspolitiska ambitionerna och samtidigt stärker den svenska digitala utvecklingen.

Kommande generations nätverk för mobil telekommunikation kommer att innebära ett paradigmskifte för hela samhället. Tekniken kommer att möjliggöra lösningar som till exempel bidrar till ökad produktivitet, bättre energianvändning, ökad livsmedelsproduktion och effektiva transporter.

Sverige är ett land som historiskt legat i framkant när inom IT och telekommunikation. Idag är Sverige internationellt erkänt som en innovativ och tekniktillvänd nation. Men när det kommer till införandet av femte generationens (5G) mobilnät är bilden inte lika ljus. EU ligger efter jämförbara regioner som Ostasien och Nordamerika och Sverige ligger i sin tur efter flera länder i EU. När Post- och telestyrelsen (PTS) den 20 oktober i år meddelade att två tillverkare av mobil telekommunikatonsutrustning av säkerhetsskäl utestängs från den kommande auktionen av 5G innebär det inte bara att implementeteringen av 5G blir dyrare än vad den hade blivit annars, utan det innebär också ytterligare förseningar. Beslutets konsekvenser kan innebära att forskning- och utveckling kommer att flyttas från Sverige, något som i sin tur skulle påverka vår ställning som ledande innovationsland. Ur ett bredare perspektiv kommer det att påverka Sveriges konkurrenskraft och i förlängningen vår ekonomiska tillväxt, utvecklingen på arbetsmarknaden och uppfyllandet av de klimatpolitiska målen.

Som exempel kan förseningarna få omfattande konsekvenser för den svenska fordons- och transportindustrin. Det innebär att forskningsprojekt förläggs i andra länder där nätet är utbyggt. I förlängningen kommer avsaknaden av 5G att påverka utvecklingen och införandet av autonoma och elektrifierade transporter, något som i sin tur kommer att få långtgående konsekvenser för andra brasncher. Ett sådant exempel är den svenska livsmedelsbranschen. Branschen är en heterogen bransch med olika grad av digitalisering, och den nya teknologin kommer att möjliggöra stora produktivitetsvinster och inte minst lägre användning av kemikalier (så kallad precisionsodling). Genom en smart användning av sensorer kommer 5G att kunna bidra med automatiserad sådd, gödning och skörd för jordbrukare. Med 5G kommer det även att bli möjligt att upprätta en produktion i områden som inte nås av bredband. Även mer effektiva transportlösningar skulle gynna branschen.

1 Inledning

Sedan det sena 1800-talet är Sverige en ledande nation inom telekom. År 1885 hade till exempel Stockholm fler telefonförbindelser i absoluta tal än någon annan stad i hela Europa. Genom åren har Sverige varit med och drivit telekomsektorn framåt med exempelvis telefonväxlar, internetföretag och dataspel. Idag rankas Sverige som ett av världens ledande innovationsländer och är internationellt erkänt som en tekniktillvänd nation.

En viktig anledning till Sveriges utveckling under 2000-talet har varit utbyggnationen av den digitala infrastrukturen. Tillgång till bredband samt snabba och robusta telekommunikationer har möjliggjort utvecklingen av nya innovationer inom flera områden. För att behålla sin tätposition som innovationsnation är det viktigt att Sverige som land arbetar brett och nydanande inom många områden. En möjliggörare för många användningsområden är mobil kommunikation.

Med introduktionen av senare generationer av mobil telekommunikation har dock EU och Sverige varit långsammare än jämförbara länder i Nordamerika och Asien. Inom 5G är europeiska företag som Nokia och Ericsson i framkant när det gäller utvecklingen, men EU ligger cirka tre år efter när det kommer till att implementera dessa lösningar.

I april 2019 trädde en ny säkerhetslag i kraft (2018:585). Lagen gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktigande internationellt åtagande om säkerhetsskydd. Den 1 januari 2020 skedde förändringar av Lagen om elektronisk kommunikation.

Det är dessa bestämmelser som ligger till grund för PTS bedömning. Den 20 oktober 2020 lät PTS meddela i ett pressmeddelande att fyra operatörer godkänts att delta i auktionen av frekvenser i 3,5 och 2,3 gigahertz-banden i Sverige. Auktionen skulle påbörjas den 10 november och pågå under 10 dagar. I samma pressmeddelande framkom att PTS arbetat tillsammans med Försvarsmakten och den svenska Säkerhetspolisen (SÄPO). I pressmeddelandet framkommer följande:

> *Förutom en formell prövning av att ansökningarna är kompletta och korrekta har en förhandsprövning genomförts i samråd med Försvarsmakten och Säkerhetspolisen, i enlighet med den nya lagstiftning som trädde i kraft 1 januari 2020. Syftet är att säkerställa att radioanvändningen inte riskerar att skada Sveriges säkerhet.*

Detta innebär att PTS har formulerat särskilda tillståndskrav som bland annat nyinstallation och implementering inte får genomföras med produkter från tillverkarna Huawei och ZTE. Beslutet innebär också att produkter från dessa tillverkare i centrala funktioner (som t.ex. radioaccessnät och transmissionsnät) ska avvecklas och i den utsträckning centrala funktioner är beroende av personal eller funktioner som är placerade i utlandet ska sådana

beroenden avvecklas och, om möjligt, ersättas av funktioner och personal placerade i Sverige. Vidare ska befintlig infrastruktur för centrala funktioner från dessa två tillverkare avvecklas. All avveckling ska vara genomförd den 1 januari 2025.

Den 9 november beslutade Förvaltningsrätten att PTS beslut tills vidare inte får verkställas. Konsekvensen blev att PTS beslutade att skjuta upp den planerade auktionen i avvaktan på beslut från Förvaltningsdomstolen, något som i sin tur leder till ytterligare förseningar. En process pågår nu i Kammarrätten i Stockholm.

I denna rapport har föreningen Gröna Städer kartlagt hur de ökade säkerhetskraven genom lagen om elektronisk kommunikation och säkerhetsskyddslagen påverkar Sverige och specifikt telekomsektorn, transporter, fordonsonsindustri och i viss mån livsmedelsindustrin. Detta har gjorts ur ett såväl ekonomiskt som ett rättsligt perspektiv.

Gröna Städer ifrågasätter inte de säkerhetsrelaterade avvägningarna i den aviserade auktionen. Däremot har det såvitt vi vet till dags datum ännu inte skett någon samhällsekonomisk konsekvensanalys inför beslutet och de regler som tillämpats. Gröna Städer anser att ett sådan analys borde ha genomförts och att det i fortsatta diskussioner är nödvändigt att lyfta blicken. Syftet med rapporten är att på längre sikt bidra till en lösning som hanterar de säkerhetsmässiga kraven och som så litet som möjligt påverkar utbyggnationen av ett rikstäckande nätverk för 5G. Som den här rapporten visar kommer en försenad utbyggnation att få långtgående effekter för Sveriges konkurrenskraft, tillväxt och för vår förmåga att adressera målen i Agenda 2030. Syftet är att bidra till en fördjupad diskussion om hur vi kan bygga ett robust och säkert samhälle och ändå fortsätta att vara ledande som innovationsnation.

2 Metod och avgränsningar

Arbetet påbörjades i oktober 2020 och rapporten publicerades i den 16 december samma år. Arbetet har utgjorts av en rättslig och en ekonomisk analys. Den rättsliga analysen har genomförts av en underkonsult (Certezza) och den ekonomiska analysen av Gröna Städer. Gröna Städer har haft det övergripande ansvaret för arbetet.

Den ekonomiska analysen baseras helt på data som insamlats av andra. Alla summor i konsekvensanalysen är uppskattningar som framkommit i intervjuer med berörda aktörer eller via dokumentstudier. Konsekvensanalysen i de berörda branscherna baseras på intervjuer och skrivna rapporter.

Som nämns i rapportens inledning har Gröna Städer valt ut branscherna transporter och fordon samt livsmedel. Detta urval har gjorts för att ge exempel av vad 5G kan möjliggöra och vilka konsekvenser som ökade säkerhetskraven kan innebära för olika branscher.

3 Ekonomiska konsekvenser

De nya säkerhetskraven kommer att få långtgående konsekvenser för Sverige som innovationsland. 5G är teknik som möjliggör olika tekniska framsteg brett i hela samhället. I följande avsnitt presenteras först konsekvenserna för telekomsektorn, sedan följer ett fördjupande avsnitt av branscherna för fordon och transporter samt för livsmedel. Avsnittet avslutas med en litteraturgenomgång av ett urval av makroekonomiska analyser.

3.1 Konsekvensanalys för telekomsektorn

Enligt Gröna Städers beräkningar kommer direkta kostnader som uppstår på grund av de nya säkerhetsbestämmelserna att uppgå till cirka 15,2 miljarder kronor den närmsta femårsperioden. Det kan jämföras med operatörernas samlade rörelseresultat som för 2019 var 13,4 miljarder kronor (där ingår även andra produkter och tjänster såsom datakommunikation, fast telefoni, bredband mm). Telia stod för mer än hälften av operatörernas vinst det året (cirka 56 procent).

Det är alltså kostnader som operatörerna kommer att behöva täcka och som kommer att behöva finansieras genom ökade intäkter. Ökade intäkter i det här fallet innebär högre avgifter för konsumenterna och vi kommer därmed att få högre priser för mobil telekommunikation.

3.1.1 Ändrad konkurrenssituation för systemleverantörer

Det finns idag tre systemleverantörer av 5G-utrustning på den svenska marknaden. Dessa är Ericsson, Huawei och Nokia. Med bortfallet av Huawei kommer Ericsson och Nokia få en ännu starkare ställning på marknaden och precis som andra marknader med imperfekt konkurrens kommer producenterna att kunna påverka priset. Då Sverige utgör en relativt liten marknad kommer det inte att leda till några märkbara stordriftsfördelar. Vad Gröna Städer förstår är Huawei och Ericsson de två största leverantörerna av 5G-utrustining i Sverige. Det är också dessa två företag som är tekniska marknadsledare. Med ett frånfall av Huwaei kommer Ericsson att kunna sätta sina egna priser i högre utsträckning. Enligt de kontakter som tagits inom ramen för utredningen är det i dagsläget inte möjligt att beräkna hur mycket den ökningen kommer att bli, men alla bedömningar ligger i spannet 10-40 procent. Med denna osäkerhet är det inte möjligt för operatörerna att beräkna sina investeringskostnader och därmed svårt att lägga sig på rätt nivå i PTS kommande auktion.

Kostnader för imperfekt konkurrens
Investeringarna för utbyggnation i Sverige den kommande femårsperioden beräknas uppgå till cirka 30 miljarder kronor. Av detta är ungefär hälften kostnader för inköp av utrustning. 10-40 procent av 15 miljarder kronor innebär en ökning på 1,5-6 miljarder kronor.

3.1.2 Ersättning av befintlig infrastruktur

En ytterligare förväntad kostnadsökning är ersättningen av produkter i befintlig infrastruktur. Detta är en kostnad som om möjligt är ännu svårare att beräkna eftersom Gröna Städer inte känner till andelen utrustning i befintlig infrastruktur som ska ersättas.

Kostnader för ersättning av befintlig utrustning
Efter kontakt med en operatör har Gröna Städer extrapolerat kostnaden baserat på den operatörens kostnader och marknadsandel. Med det beräknas de totala kostnaderna uppgå till 10 miljarder kronor från idag till 1 januari 2025. Med ökade kostnader (se imperfekt konkurrens ovan) riskerar inköp av utrustningen bli ännu dyrare.

3.1.3 Olika kostnadsbild för operatörerna

Den svenska marknaden för mobila telefonabonnemang består av fyra olika operatörer i Telia, Tele 2, Telenor och Tre[1]. Telia är störst följt av Tele 2, Telenor och Tre. De olika operatörerna har olika andel av utrustning från kinesiska tillverkare, och de operatörer som har hög andel kommer att tvingas till relativt högre investeringar än de som har en lägre andel. Säkerhetsbestämmelserna kommer således att påverka kostnadsbilden för operatörerna på olika sätt och därmed påverka konkurrensen på marknaden. De operatörer som har högt innehåll av kinesisk utrustning kommer att tvingas till större investeringar och få en annan kostnadsbild.

3.1.4 Säkerhetsklassade anläggningar

Som fram går av den rättsliga analys som Gröna Städer låtit genomföra kommer definitionen av vad som är av betydelse för Sveriges säkerhet att innebära att operatörernas säkerhetsskyddsanalys måste bli mycket omfattande. Det kommer troligen att innebära att operatörerna måste beakta varje basstation och dessa måste säkerhetsklassas. Vad det innebär i kostnader är svårt att bedöma och det kommer att bero på basstationens läge.

[1] PTS beslut inte gäller för Tele2 eller Telenor utan endast för deras gemensamma nätbolag Net4Mobility.

Kostnader för att säkerhetsskydd av den tekniska utrustningen
Lågt räknat har rapporten räknat med att det finns cirka 40 000 basstationer i Sverige[2] och att kostnaden att bygga om varje basstation kommer att uppgå till minst 35 000 kr per basstation. Det medför merkostnader på 1,4 miljarder kronor. Det ska här sägas att kostnaderna kan bli ännu högre beroende på vilka delar av den tekniska utrustningen som ska säkerhetsklassas.

3.1.5 Säkerhetsprövning av personal

All personal som arbetar i verksamheterna måste säkerhetsprövas och registerkontrolleras. Det i sig innebär omfattande intrång i många människors enskilda integritet – vilket i vissa fall inte begränsar sig till anställda utan även deras partner. Samtidigt blir det svårare med rekrytering dels eftersom PTS måste först fatta beslut om inplacering i säkerhetsklass och därefter ska registerkontroll och säkerhetsprövning göras innan personalen kan börja arbeta i verksamheten. Det kan ibland ta lång tid att få svar från säkerhetspolisen i registerkontrollärenden då det löpande görs många förfrågningar – genom att ytterligare en stor mängd kontroller måste göras kan det också påverka andra verksamheter som är beroende av registerkontroller för sina rekryteringar. Detta medför sammantaget att det förutses bli svårare, dyrare och långsammare för operatörerna att rekrytera personal som ska arbeta i verksamheten.

Kostnader för att säkerhetsskydd av den tekniska utrustningen
Gröna Städer har inte haft tillgång till data för att uppskatta vilka kostnader som säkerhetsprövningen av personal kommer att medföra.

3.2 Konsekvenser för utpekade branscher

5G är en så kallad General Purpose Technology som betyder är det teknologi som möjliggör utvecklingen av flera områden. I följande avsnitt presenteras möjliga konsekvenser av en försening för branscherna fordon och transport samt livsmedel.

3.2.1 Fordon och transporter

Med två tillverkare för tunga fordon (Volvo och Scania) samt två personbilstillverkare (Volvo Cars och Nevs) och därtill många underleverantör är fordonsindustrin en av Sveriges viktigaste branscher. Med ett totalt exportvärde av cirka 235 miljarder kronor är det den

[2] Baseras på PTS rapport från 2015: https://www.pts.se/globalassets/startpage/dokument/icke-legala-dokument/rapporter/2015/radio/statistik-om-tillgangen-till-mobila-kommunikationsnat-pts-er-2015_7.pdf

exportnäring som omsätter mest.[3] Det bedrivs omfattande forskning och utveckling (FoU) inom branschen, där samtliga tillverkare har Sverige som en viktig bas. På senare år har Sverige kommit att bli ledande inom en rad fordonsrelaterade områden, däribland autonoma bilar. Med upprättandet av NorthVolt i Skellefteå och med utbyggnaden av elvägar spås Sverige även ta en tätposition inom elektromobilitet.

För fordonsindustrin betyder implementeringen av 5G många möjligheter. På tillverkningssidan antas 5G att leda till ökad produktivitet och flexibilitet. Det kommer också att innebära möjligheter till förbättrat underhåll, där diagnostik av fordonen kommer att kunna ske i realtid. Realtid för denna tillämpning tillhandahålls redan av 4G. 5G innebär en förbättring, men inte principskillnad. I en intervju i Dagens Industri från 2 oktober i år menar Volvo AB:s VD, Martin Lundstedt, att den mobila telekommunikationen redan idag möjliggör en rad funktioner. Till exempel kan maskiner och fordon kommunicera med varandra och slås av när de inte används. Detta är möjligt tack vare en bra digital uppkoppling och i vissa projekt kan det minska utsläppen med 10–15 procent. Martin Lundstedt menar att det tekniska skiftet till elektromobilitet och autonoma fordon kommer endast att bli möjligt med stöd av 5G.[4]

Volvo Cars och det strategiska innovationsprogrammet Drive Sweden menar att dagens självkörande fordon inte är beroende av utveckling av 5G. Självkörande fordon kommer att behöva utvecklas så att de kan framföras oberoende av externa faktorer. Detta gäller även de framtida helt autonoma fordonen utan förare närvarande ombord eller på distans. Däremot, menar både Volvo Cars och Drive Sweden, kan 5G utgöra stöd genom t.ex. styrning av trafiksignaler och annan infrastruktur som påverkar framkomlighet genom de möjligheter till prioriterad (säkerställd) telekomtrafik som 5-G erbjuder. Det kan också bli så att 5G, enligt Drive Sweden, innebär en lösning för kommunikation mellan fordon. Det svenska startupföretaget Einride har en affärsmodell, där de säljer autonoma elektrifierade transporter (snarare än ”bara” själva fordonet). Med sin affärsmodell behåller de ansvaret för framförandet av fordonet. De menar i en intervju med Gröna Städer att ett utbyggt 5G-nät är vitalt för deras affärsmodell. Största skälet varför de anser att 5G är så viktigt är att nätet är mer pålitligt än existerande lösningar. Einride menar att det inte kommer att vara möjligt att rulla ut stora flottor av elektriska och automatiserade lastfordon utan en miljö med 5G.

Transportbranschen tangerar fordonsindustrin och precis som för andra branscher är det svårt att förutse om vad 5G kommer att innebära. Säkert är att 5G kommer att möjliggöra övervakning av transporternas innehåll, till exempel om tillståndet av en känslig vara som

[3] Bil Swedens hemsida (besökt 13 december 2020): https://www.bilsweden.se/industrin
[4] Dagens Industris hemsida (besökt den 13 december 2020): https://www.di.se/nyheter/volvochefen-fasar-for-langsam-5g-utrullning-kravs-for-nasta-steg-inom-industrin/

transporteras. Vidare kan utvecklingen av drönartransporter komma att påverkas. Särskilt viktigt för att transporter är att den mobila kommunikationen kan bli mer pålitlig och att sensorer i infrastrukturen inte störs ut av andra aktörer på samma sätt som 4G gör idag.

Mot bakgrund av det som framkommit i denna studies datainsamling gör Gröna Städer bedömningen att delar av FoU riskerar att försvinna från Sverige om 5G försenas med 3-5 år. Fordonsindustrin är i snabb utveckling och är en bransch med hård konkurrens. Den senaste tioårsperioden har samarbetet mellan fordonsindustrin och landets lärosäten utvecklats avsevärt. En utflyttning av FoU kommer därmed också att påverka Sveriges lärosäten, främst de högskolor som har en teknisk inriktning. Det kan också bli så att forskningsprojekt som finansieras av EU kommer att förläggas till de länder där 5G är implementerat i högre utsträckning. Förseningen av 5G kan också göra att det blir svårare för svenska företag att rekrytera personal från andra länder.

3.2.2 Livsmedel

De svenska livsmedelsföretagen utgör en av Sveriges viktigaste industrigrenar och är en bransch i tillväxt. Det är geografiskt spridd bransch som skapar jobb och tillväxt i hela landet. Svenska livsmedelsföretag kan delas in ett stort antal delbranscher och det är en mycket heterogen grupp, inte minst inom grad av digitalisering. Det finns stora företag som är långt fram inom digitalisering och mindre företag som knappt alls nyttjar digitaliseringens fördelar.

Livsmedelsindustrin anses spela en viktig roll för de globala utmaningarna som vi står inför. Den svenska livsmedelsstrategin är en plattform för det långsiktiga arbetet för en konkurrenskraftig livsmedelskedja. Strategin ska bland annat bidra till att öka produktionen, innovationskraften och lönsamheten samtidigt som relevanta miljömål nås.

Enligt de förespråkare av 5G som Gröna Städer varit i kontakt med kommer tekniken att möjliggöra stora produktivitetsvinster och inte minst lägre användning av kemikalier (så kallad precisionsodling). Genom en smart användning av sensorer kommer 5G att kunna bidra med automatiserad sådd, gödning och skörd för jordbrukare. Med 5G kommer det även att bli möjligt att upprätta en produktion i områden som inte nås av bredband. Som tidigare nämnts om transporter kommer 5G även att kunna erbjuda en vidare bredd av transportlösningar för produkter som är beroende av effektiva transporter. Det kommer även att innebära möjligheter att bedriva en bättre lagerhushållning, något som förväntas bidra till minskat matsvinn i samhället. Genom insatser av drönare kommer jordbruket att kunna övervaka sina odlingar i högre utsträckning och snabbare reagera vid till exempel skadedjursangrepp.

Enligt en expert inom 5G som Gröna Städer intervjuat kan 5G innebära att företag som tidigare inte varit digitaliserade börja den processen och då realisera en rad applikationer som ger det företaget stora fördelar på en konkurrensutsatt marknad.

Med klimatförändringar och en ökande befolkning kommer det ställas högre krav på svensk livsmedelsproduktion. Användningen av digitalisering är avgörande för om Sverige ska nå de klimatpolitiska målen och målen i livsmedelsstrategin. Med ett försenat införande av 5G kommer andra länder att realisera tekniken innan Sverige. Det kan därtill tilläggas att konkurrensen för branschen bitvis är mycket hård, och en del länder i vårt närområde har idag redan fördelar med mer gynnsamt klimat, stordriftsfördelar och lägre arbetskostnader. Ett snabbt införande av digitalisering och 5G är nödvändigt om industrin ska uppnå satta tillväxt- och klimatmål.

3.3 Litteraturgenomgång av makroekonomiska konsekvensanalyser

Det finns i dagsläget, vad Gröna Städer känner till, ingen samhällsekonomisk analys av vilka konsekvenser som en försening av 5G kommer att innebära för Sverige. Men internationellt finns det en del ex ante rapporter som försöker ge svar på de makroekonomiska konsekvenserna av 5G.

En rapport från nätverket *Global System for Mobile Communication* (GSMA) från juni 2018 visar att 5G kommer att bidra till ökad ekonomisk tillväxt med 2,2 biljoner (10^{12}) US-dollar åren 2020-2034.[5] I en annan rapport, skriven av IHS Markit, från förra året kommer 5G bidra till en ökning av BNP med 3,6 biljoner US-dollar åren 2020-2035.[6]

En rapport som är mer relevant för att analysera den ekonomiska effekten av att stänga ute dominerande tillverkare från utbyggnationen av 5G är Oxford Economics rapport *Restricting competition in 5G network equipment throughout Europe – an economic impact study* från juni i år. Det är en makorekonomisk analys av vad som potentiellt skulle hända i EU28. Enligt den skulle ett uteslutande likt det som PTS föreslår leda till en imperfekt konkurrens (där Nokia och Ericsson skulle ha en gemensam marknadsandel i EU på 90 procent). Det i sin tur kommer att leda till ökade kostnader för inköp av utrustning med 19 procent. Med en försening på tre år kommer det enligt rapporten att leda till en minskad BNP-tillväxt på 8,8 miljarder Euro åren 2020–2035.[7]

[5] Från GSMA:s hemsida den 11 december: 2020 https://www.gsma.com/spectrum/wp-content/uploads/2019/10/mmWave-5G-benefits.pdf
[6] Från Qualcomms hemsida den 11 december 2020: https://www.qualcomm.com/media/documents/files/ihs-5g-economic-impact-study-2019.pdf
[7] Från Oxford Ecnomics hemsida den 14 december 2020: https://d2rpq8wtqka5kg.cloudfront.net/569099/open20200629032700.pdf?Expires=1607980078&Signature=k~rTMdmLJjiS41

En studie av European Round Table for Industry (ERT) publicerad i september i år, visar att Europa ligger långt efter framförallt Asien men även USA när det kommer till utbyggnation av 5G. Studien visar på stora prisskillnader för licenser mellan olika europeiska länder och att det i snitt finns en längre avkastning på investering (ROI) jämfört med de två andra regionerna. Studien visar inte specifikt på säkerhetsbestämmelser utan diskuterar riskerna med att vara senare med implementeringen jämfört med andra regioner. ERT efterlyser mer samarbete inom EU så att samma regler gäller för alla länder. Framförallt behöver utbyggnationen gå snabbare. Enligt rapporten ligger EU:s ekonomiska styrka i flera branscher där fördelarna av 5G kommer att vara tydligast, däribland tekniktung industri som flygplans- och fordonstillverkning.[8] Fjärrstyrning av maskiner för t.ex. gruvindustrin kommer att bli möjlig med 5G[9], något som skulle gynna den svenska gruvindustrin.

4 Om rättsliga konsekvenser

Gröna Städer bad Certezza genom dess chefsjurist Andreas Dahlqvist att göra en analys av de rättsliga konsekvenserna av PTS:s beslut och att beskriva vilka de rättsliga konsekvenserna skulle bli för IT- och telekomsektorn och några övriga sektorer i Sverige. Avsikten var att se vilka generella slutsatser som kan dras om höjda säkerhetskrav. Analysen baseras på att PTS är tillsynsmyndighet såväl avseende lagen om elektronisk kommunikation som säkerhetsskyddslagen, att beslutet inte enbart omfattar 5G-näten utan även 4G, 3G och 2G-näten, att tillsynsmyndigheten gjort en mycket omfattande och generell definition av vad som är av betydelse för Sveriges säkerhet, att det är oklart vad som kan komma att hända om operatörerna inte skulle efterlever villkor och att fyra operatörers nät är av betydelse för Sveriges säkerhet och att dessa inte får vara beroende av personal eller funktioner i andra länder – inte ens andra länder inom EU.

I rapporten konstateras att lagstiftaren inte gjort någon konsekvensanalys av denna typ av beslut (dvs. att ställa den sorts säkerhetskrav som PTS gjort) eller gjort en proportionalitetsbedömning av beslutets innebörd. Dessa allvarliga brister kan i sig leda till en långvarig regulatorisk osäkerhet då frågorna i flera avseenden kan komma att få avgöras i EU-domstolen.

---

lGEm643V9qcBc5dTdCCYO4fARK-G695p6VnNe6DseF1VkOXnjowHMHKhinZgwEWYQKAuuNPOdu8pJFYKs6vkM6wR0ZvdIM-YPA8xvBqI8tioJBVm7ggPP~3pf9P4zUVdaPWlqC1OPW2yviTTI18cw3tu7O40sUh5spzVL8qox-TLTMBdS3nyG~TmBU8GwB0cwgzujWHmKQFajfAo6LQhyqmY5c9tIdQk3O8JXeD6kECcZbcNGTIQrP4QUw6c0whUi2Z6LQnBFij~~qOmT~bHLTCE7W5pqnAqNppViR4UtLtqxPgZbzY486dC7whoi~8rfLyhhV~g__&Key-Pair-Id=APKAJVGCNMR6FQV6VYIA

[8] Från ERT:s hemsida 14 december 2020: https://ert.eu/documents/5g-assessment/

[9] Från ERT:s hemsida 14 december 2020: https://ert.eu/documents/5g-assessment/

4.1 Rättslig analys

Enligt säkerhetsskyddslagen är det verksamhetsutövaren själv som ska definiera vilka delar av verksamheten som omfattas av säkerhetsskydd genom att göra en säkerhetskyddsanalys. PTS beslut innebär således ett avsteg från den regeln eftersom tillsynsmyndigheten gjort avgränsningen – trots att regeringen uttalat att det är inte är lämpligt att tillsynsmyndigheten utifrån sin analys pekar ut vilka verksamheter som omfattas av lagstiftningen.[10] Tillsynsmyndigheten (PTS) har i beslutet gjort en mycket omfattande och generell definition av vad som är av betydelse för Sveriges säkerhet vad avser de aktuella operatörernas elektroniska kommunikationsnät. Det innebär i sig att operatörernas säkerhetskyddsanalys måste bli mycket omfattande då operatörerna troligen måste beakta varje basstation och varje nätkomponent i samtliga delar av deras rikstäckande elektroniska kommunikationsnät i detta dokument.

Som regeringen anger i förarbetena innebär detta att verksamhetsutövaren måste vidta långtgående åtgärder för att skydda hemliga uppgifter och den säkerhetskänsliga verksamheten. Säkerhetsåtgärderna är kostsamma och medför en extra administrativ påfrestning inom organisationen.[11]

Operatörerna i fråga måste göra omfattande fiktiva sekretessprövningar enligt offentlighets- och sekretesslagen för att bedöma vilka uppgifter hos operatören som behöver säkerhetsskyddsklassificeras enligt säkerhetsskyddslagen.[12]

Varje plats där det bedrivs denna typ av verksamhet måste också säkerhetsskyddsklassificeras enligt SÄPO:s föreskrifter om säkerhetsskydd (PMFS 2019:2). Platserna där verksamheterna bedrivs - vilket även omfattar ett stort antal vindsvåningar och tak till flerfamiljsbostäder - måste klassas och förses med inpasseringssystem, stängsel kan behöva installeras på tak, vilket i sig både kan vara kostsamt och riskabelt för byggnader. Dessa typer av krav och åtgärder kan innebära betydande begränsningar i möjligheterna att bygga ut de allmänt tillgängliga elektroniska kommunikationsnäten samtidigt som det innebär ofantliga kostnader. Inte minst i en framtid där fullt utbyggda 5G-nät med efterföljande teknikgenerationer medför att basstationer behöver placeras mycket tätare än idag i tätortsmiljöer.

[10] Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag, prop. 2017/18:89 s. 43.
[11] Prop. 2017/18:89 s. 38 f
[12] Prop. 2017/18:89 s. 52.

Det blir svårare för operatörerna att köpa utrustning och komponenter. Eftersom all utrustning och alla komponenter är av betydelse för Sveriges säkerhet måste operatörerna göra en analys innan de köper in utrustningen. Beroende på vilken klass utrustningen hör till, finns det krav på att särskilt säkerhetsskyddsavtal upprättas med leverantören innan beställningar görs. Detta gäller även underleverantörer till leverantörerna. Samråd ska också genomföras med PTS innan säkerhetsskyddsavtal upprättas. Med tanke på den mängd inköp som en operatör behöver göra för drift-, underhåll och utbyggnad av kommunikationsnäten kan detta bli en oerhörd belastning på operatören men också på operatörernas leverantörer. Det kan förutses att den typen av kunder kan bli nedprioriterade i förhållande till andra kunder där affärerna kan bedrivas snabbare och mer effektivt och som inte ställer lika höga krav på leverantören och dess underleverantörer.

Om ett inköp innebär att operatören behöver lämna uppgifter till en leverantör som bedöms vara säkerhetskyddsklassificerade (oavsett säkerhetsskyddsklass) får operatören endast använda leverantörer från länder som Sverige har ett generellt säkerhetsskyddsavtal (GSA) med. Antalet länder är i dessa fall begränsat.[13] Om en operatör i sådana fall vill köpa utrustning från en leverantör som Sverige inte har GSA med måste operatören vända sig till regeringen så att regeringen påbörjar ett arbete med att upprätta en sådan överenskommelse mellan Sverige och det aktuella landet. Beroende på vilket land det rör sig om kan det ta mellan 2 och 10 år att ta fram ett sådant bilateralt avtal, om det ens är möjligt i vissa fall. Även om operatörerna övervinner dessa hinder begränsas samtidigt mängden möjliga leverantörer vilket ofta leder till sämre konkurrens, högre priser samt sämre produkter i slutändan. I vissa fall kan till och med önskad potentiellt tillgänglig funktionalitet helt utebli eftersom det inte finns tillåtna leverantörer att köpa från.

Den rättsliga analysen i sin helhet återfinns i denna rapports bilaga.

5 Säkerhetskravens möjliga ekonomiska konsekvenser

Utgångsläget är att implementeringen av Sverige ligger efter jämförbara länder. Som nämndes i tidigare kommer det att finnas drygt 160 miljoner 5G-abonnemang i Kina vid årsskiftet 2020/2021. Branschexperter som Gröna Städer varit i kontakt med räknar med att ta att det kan ta upp till fem år innan 5G finns tillgängligt i hela Sverige.

[13] Sverige har idag GSA med Australien, Belgien, Brasilien, Bulgarien, Danmark, Estland, Finland, Frankrike, Island, Italien, Irland, Jugoslavien (Bosnien och Hercegovina, Serbien), Kanada, Kroatien, Lettland, Litauen, Luxemburg, Nederländerna, Norge, Polen, Portugal, Rumänien, Schweiz, Singapore, Slovakien, Slovenien, Spanien, Storbritannien och Nordirland, Sydafrika, Sydkorea, Tjeckien, Tyskland, Ungern, USA och Österrike

6 Slutsatser

PTS beslut kommer, förutsatt att det genomförs, att medföra långtgående konsekvenser. För telekomoperatörerna kommer det att betyda högre kostnader (till följd av att ersätta befintlig utrustning och dyrare inköp av ny utrustning för 5G). Det i sin tur medför att mobil telekommunikation blir dyrare jämfört med idag. Men kanske än viktigare är att införandet av 5G kommer att bli försenat ytterligare och kan leda till att Sverige hamnar på efterkälken jämfört med andra EU-länder (som i sin tur ligger efter Asien och Nordamerika) och det riskerar sätta igång en kedjereaktion. Med försenad 5G kommer det att ske mindre forskning och utveckling av applikationer som kräver 5G-stöd i Sverige. Delar av den FoU som annars skulle ha bedrivits i Sverige kommer att förläggas utomlands. Med mindre investeringar i FoU kommer Sveriges internationella konkurrenskraft att försämras. Resultatet blir att Sveriges tillväxt och sysselsättning påverkas negativt.

Flera aktörer som Gröna Städer har varit i kontakt med menar att den rättsliga tolkningen skapar osäkerhet. Det finns tre aspekter. Den ena aspekten är att det i dagsläget inte är klart vilken utrustning som omfattas, vilket framkommer av rapportens rättsliga analys. Den andra aspekten är om möjligt ännu allvarligare. Utbyggnationen av 5G är känt sedan en längre tid tillbaka. Den rättsliga tolkningen innebär mycket höga kostnader för att ersätta utrustning som köpts in under senare tid. PTS beslut var oförutsett för mobiloperatörerna och om de hade känt till att beslutet skulle komma hade avvaktat med att genomföra nu gjorda investeringar. Risken är här att aktörer inom andra branscher som arbetar med elektroniska komponenter kommer att avvakta sina investeringsbeslut. Beslutet om att med kort framförhållning utestänga dominerande aktörer från 5G riskerar därmed att få konsekvenser även inom andra branscher. Den tredje osäkerhetsaspekten rör Sveriges handelsrelationer, där det finns en oro för att Kina kommer att besvara förbudet med upprättandet av handelshinder.

Gröna Städer inser att konsekvenserna är okända av att *inte* tolka och tillämpa lagen på det sätt vi beskriver i rapporten, men den bevisbördan ligger rimligen på de myndigheter som ansvarar för den analysen. Vi anser att det är av yttersta vikt den slutliga lösningen beaktar och tar hänsyn till de samhällsekonomiska konsekvenserna av beslutet och att det fortsatt utreds om det finns andra lösningar som uppfyller såväl säkerhetspolitiska som samhällsekonomiska målsättningar på bästa möjliga sätt.

Bilaga 1: Utredningens rättsliga analys

Titel:
Rättsliga konsekvenser för it- och telekomsektorn m.fl. avseende säkerhetskrav i Post- och Telestyrelsens beslut om Godkännande av sökande samt tillkommande villkor i auktion av frekvensbanden 3,5 GHz och 2,3 GHz den 20 oktober 2020

Inledning

Denna framställning syftar till att analysera rättsliga konsekvenser för it- och telekomsektorn med flera med anledning av det godkännandebeslut som Post- och telestyrelsen (PTS) fattade den 20 oktober 2020 inför kommande auktion av frekvenser i 3,5 och 2,3 gigahertz-banden.
Rapporten inleds med en sammanfattning och sedan refereras huvuddragen av PTS beslut. Därefter följer analysen av rättsliga konsekvenser, i analysen används begreppet operatörerna för de operatörer som i beslutet godkänts att delta i auktionen. När analysen pekar på andra operatörer än dessa så tydliggörs det i texten. Efter detta avsnitt presenteras också en möjlig alternativ lösning för att uppnå en högre grad av säkerhet i de elektroniska kommunikationsnäten. Avslutningsvis presenteras den rättsliga kontexten, det vill säga de lagrum och förarbetsuttalanden som legat till grund för analysen. I denna del kan läsaren hitta de rättsliga grunderna som stödjer analysens slutsatser, avsnittet innehåller således ett urval av relevanta bestämmelser som kan aktualiseras.

Post- och telestyrelsens beslut[14]

I sitt förberedande beslut inför kommande frekvenstilldelning av frekvenser i frekvensbanden 3,5 GHz och 2,3 GHz beslutade PTS bland annat följande:

> *Hi3G Access AB, Net4Mobility HB, Telia Sverige AB och Teracom AB (operatörerna) godkänns som deltagare i auktionsförfarandet […].*
> *Tillstånd att använda radiosändare i frekvensbandet 3400–3720 MHz [och 2300-2380 MHz] ska förenas med […] villkor om krav som är av betydelse för Sveriges säkerhet, […]:*
> *Kraven gäller centrala funktioner i*
> - *radioaccessnät (antenner och basstationsutrustning)*
> - *transmissionsnät (överföring till kärnnätet antingen via fiber eller radiolänkar)*
> - *kärnnät, (funktioner för tjänsteproduktion, kunddata och fakturering m.m.) och*
> - *drift- och underhållsnät (i detta övervakas och styrs nätets funktion)*
>
> *Utöver vad som anges i punkt 26 ovan ska tillståndshavaren iaktta följande.*

[14] PTS beslut den 10 oktober 2020 om godkännande av sökande samt tillkommande villkor i auktion av frekvensbanden 3,5 GHz och 2,3 GHz, dnr. 18-8496

- *Nyinstallation och ny implementering av centrala funktioner för radioanvändning i frekvensbandet 3400–3720 MHz [och 2300-2380 MHz] får inte genomföras med produkter från leverantörerna Huawei eller ZTE.*
- *I fall befintlig infrastruktur för centrala funktioner kommer att användas för tillhandahållande av tjänster i de aktuella frekvensbanden ska en avveckling av produkter från Huawei och ZTE vara genomförd senast den 1 januari 2025.*

[…]

I den utsträckning centrala funktioner är beroende av personal eller funktioner som är placerade i utlandet ska sådana beroenden avvecklas och, om nödvändigt, ersättas med funktioner eller personal placerade i Sverige. Detta ska vara genomfört senast den 1 januari 2025.

Av skälen framgår att PTS har identifierat följande hot:

1. I och med teknikutvecklingen uppstår sårbarheter löpande som underlättar för främmande makts säkerhetshotande verksamhet.
2. Kina bedriver cyberspionage mot tjänstesektorn inbegripet leverantörer av elektroniska kommunikationstjänster.
3. Underrättelseinhämtning om infrastruktur kan göras som en del i en kartläggning av en stats civila infrastruktur eller för att inhämta eller överföra civil teknologi.
4. Beroenden mellan sektorn elektronisk kommunikation och andra samhällssektorer gör att mål i dessa andra sektorer kan utsättas för antagonistiska handlingar eller kartläggas.
5. Kinas nationella lagstiftning innebär att organisationer, företag och medborgare ska stödja och assistera kinesiskt underrättelsearbete.
6. Kinesiska staten kan påverka och utöva påtryckningar på Huawei och ZTE.
7. USA:s beslut om handelsrestriktioner mot Huawei innebär sannolikt att företagets förmåga att på sikt konstruera och tillverka nödvändiga produkter för framtida 5G-nät påverkas negativt.

Sammantaget kan produkter från Huawei eller ZTE i centrala funktioner *skada Sveriges* säkerhet.

Centrala funktioner definieras som radioaccessnät, transmissionsnät, kärnnät och drifts- och underhållsnät.

Säkerhetsbrister i någon av de centrala funktionerna kan leda till att nätet kan angripas utifrån. Skada på Sveriges säkerhet genom den radioanvändning som tilldelningsförfarande avser kan därmed uppstå.

När centrala funktioner är beroende av funktioner eller personal placerade i utlandet kan situationer där förbindelserna mellan Sverige och utlandet bryts medföra att nätens funktionalitet skadas allvarligt. Detta kan medföra *fara för* Sveriges säkerhet.

Det behövs därför tillståndsvillkor som innebär att centrala funktioners beroenden av funktioner eller personal i utlandet ska avvecklas och ersättas med funktioner eller personal placerade i Sverige, om det är nödvändigt. Även dessa villkor måste vara proportionella och ta hänsyn till vad som är praktiskt genomförbart. Det bedöms tillräckligt att avvecklingen ska vara genomförd senast den 1 januari 2025.

Analys av rättsliga konsekvenser av PTS beslut om godkännande av sökande

Sveriges säkerhet och 5G-näten – avser samtliga delar av operatörernas elektroniska kommunikationsnät

PTS är tillsynsmyndighet över säkerhetsskyddet för enskilda verksamhetsutövare som bedriver verksamhet som avser elektronisk kommunikation. Genom att i beslutet om godkännande av sökande definiera vilka delar av operatörernas nät som är av betydelse för Sveriges säkerhet har PTS samtidigt definierat säkerhetsskyddslagens tillämpningsområde för dessa aktörer.

I beslutet skriver PTS att omfattningen är centrala funktioner ”i” radioaccessnät, transmissionsnät, kärnnät och drift- och underhållsnät. Det skulle kunna tolkas som att det endast är delar av dessa nät som avses – även om det är oklart vilka delar. Av skälen till beslutet framgår emellertid att de uppräknade näten utgör centrala funktioner i ett 5G-nät.[15] Därmed avses inte endast begränsade delar av de uppräknade näten utan de uppräknade näten i sina helheter. PTS synes därför mena att varje enskild mobil basstation och komponent i samtliga delar av de elektroniska kommunikationsnäten är betydelse för Sveriges säkerhet och att säkerhetsskyddslagens bestämmelser ska tillämpas på denna verksamhet (PTS är tillsynsmyndighet såväl avseende lagen om elektronisk kommunikation som säkerhetsskyddslagen).

Villkoren avseende de aktuella frekvensbanden påverkar även andra tidigare tillstånd som de aktuella operatörerna har, liksom sådana delar av de elektroniska kommunikationsnäten som inte omfattas av krav på tillstånd dvs. även trådlös och trådbundna delar av näten eftersom redan befintlig utrustning från de aktuella leverantörerna ska avvecklas i sin helhet senast den 1 januari 2025. Kärnnät och transportnät kan vara både trådlösa och trådbundna. Detta beslut påverkar således även de delar av verksamheten som normalt inte kräver tillstånd. Det innebär också att PTS beslut inte enbart omfattar 5G-näten utan även 4G, 3G och 2G-näten. Dessa är ju dessutom sammankopplade.

[15] PTS beslut den 10 oktober 2020 om godkännande av sökande samt tillkommande villkor i auktion av frekvensbanden 3,5 GHz och 2,3 GHz, dnr. 18-8496, s. 7.

Konsekvenser av att säkerhetsskyddslagen måste tillämpas på de elektroniska kommunikationsnäten som helhet

Enligt säkerhetsskyddslagen är det verksamhetsutövaren själv som ska definiera vilka delar av verksamheten som omfattas av säkerhetsskydd genom att göra en säkerhetskyddsanalys. PTS beslut innebär således ett avsteg från den regeln eftersom tillsynsmyndigheten gjort avgränsningen – trots att regeringen uttalat att det är inte är lämpligt att tillsynsmyndigheten utifrån sin analys pekar ut vilka verksamheter som omfattas av lagstiftningen.[16] Tillsynsmyndigheten (PTS) har i beslutet gjort en mycket omfattande och generell definition av vad som är av betydelse för Sveriges säkerhet vad avser de aktuella operatörernas elektroniska kommunikationsnät. Det innebär i sig att operatörernas säkerhetskyddsanalys måste bli mycket omfattande då operatörerna troligen måste beakta varje basstation och varje nätkomponent i samtliga delar av deras rikstäckande elektroniska kommunikationsnät i detta dokument.

Som regeringen anger i förarbetena innebär detta att verksamhetsutövaren måste vidta långtgående åtgärder för att skydda hemliga uppgifter och den säkerhetskänsliga verksamheten. Säkerhetsåtgärderna är kostsamma och medför en extra administrativ påfrestning inom organisationen.[17]

Operatörerna i fråga måste göra omfattande fiktiva sekretessprövningar enligt offentlighets- och sekretesslagen för att bedöma vilka uppgifter hos operatören som behöver säkerhetsskyddsklassificeras enligt säkerhetsskyddslagen.[18]

Varje plats där det bedrivs denna typ av verksamhet måste också säkerhetsskyddsklassificeras enligt SÄPO:s föreskrifter om säkerhetsskydd (PMFS 2019:2). Platserna där verksamheterna bedrivs - vilket även omfattar ett stort antal vindsvåningar och tak till flerfamiljsbostäder - måste klassas och förses med inpasseringssystem, stängsel kan behöva installeras på tak, vilket i sig både kan vara kostsamt och riskabelt för byggnader. Dessa typer av krav och åtgärder kan innebära betydande begränsningar i möjligheterna att bygga ut de allmänt tillgängliga elektroniska kommunikationsnäten samtidigt som det innebär ofantliga kostnader. Inte minst i en framtid där fullt utbyggda 5G-nät med efterföljande teknikgenerationer medför att basstationer behöver placeras mycket tätare än idag i tätortsmiljöer.

[16] Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag, prop. 2017/18:89 s. 43.
[17] Prop. 2017/18:89 s. 38 f
[18] Prop. 2017/18:89 s. 52.

All personal som arbetar i verksamheterna måste säkerhetsprövas och registerkontrolleras. Det i sig innebär mycket omfattande intrång i många människors enskilda integritet – vilket i vissa fall inte begränsar sig till anställda utan även deras make eller sambo. Samtidigt blir det svårare med rekrytering dels eftersom PTS måste först fatta beslut om inplacering i säkerhetsklass och därefter ska registerkontroll och säkerhetsprövning göras innan personalen kan börja arbeta i verksamheten. Det kan ibland ta lång tid att få svar från säkerhetspolisen i registerkontrollärenden då det löpande görs många förfrågningar – genom att ytterligare en stor mängd kontroller måste göras kan det också påverka andra verksamheter som är beroende av registerkontroller för sina rekryteringar. Detta medför sammantaget att det förutses bli svårare, dyrare och långsammare för operatörerna att rekrytera personal som ska arbeta i verksamheten.

Det blir svårare för operatörerna att köpa utrustning och komponenter. Eftersom all utrustning och alla komponenter är av betydelse för Sveriges säkerhet måste operatörerna göra en analys innan de köper in utrustningen. Beroende på vilken klass utrustningen hör till, finns det krav på att särskilt säkerhetsskyddsavtal upprättas med leverantören innan beställningar görs. Detta gäller även underleverantörer till leverantörerna. Samråd ska också genomföras med PTS innan säkerhetsskyddsavtal upprättas. Med tanke på den mängd inköp som en operatör behöver göra för drift-, underhåll och utbyggnad av kommunikationsnäten kan detta bli en oerhörd belastning på operatören men också på operatörernas leverantörer. Det kan förutses att den typen av kunder kan bli nedprioriterade i förhållande till andra kunder där affärerna kan bedrivas snabbare och mer effektivt och som inte ställer lika höga krav på leverantören och dess underleverantörer.

Om ett inköp innebär att operatören behöver lämna uppgifter till en leverantör som bedöms vara säkerhetskyddsklassificerade (oavsett säkerhetsskyddsklass) får operatören endast använda leverantörer från länder som Sverige har ett generellt säkerhetsskyddsavtal (GSA) med. Antalet länder är i dessa fall begränsat.[19] Om en operatör i sådana fall vill köpa utrustning från en leverantör som Sverige inte har GSA med måste operatören vända sig till regeringen så att regeringen påbörjar ett arbete med att upprätta en sådan överenskommelse mellan Sverige och det aktuella landet. Beroende på vilket land det rör sig om kan det ta mellan 2 och 10 år att ta fram ett sådant bilateralt avtal, om det ens är möjligt i vissa fall. Även om operatörerna övervinner dessa hinder begränsas samtidigt mängden möjliga leverantörer vilket ofta leder till sämre konkurrens, högre priser samt sämre produkter i

[19] Sverige har idag GSA med Australien, Belgien, Brasilien, Bulgarien, Danmark, Estland, Finland, Frankrike, Island, Italien, Irland, Jugoslavien (Bosnien och Hercegovina, Serbien), Kanada, Kroatien, Lettland, Litauen, Luxemburg, Nederländerna, Norge, Polen, Portugal, Rumänien, Schweiz, Singapore, Slovakien, Slovenien, Spanien, Storbritannien och Nordirland, Sydafrika, Sydkorea, Tjeckien, Tyskland, Ungern, USA och Österrike

slutändan. I vissa fall kan till och med önskad potentiellt tillgänglig funktionalitet helt utebli eftersom det inte finns tillåtna leverantörer att köpa från.

Betydande osäkerheter och otydligheter

Villkoren i PTS beslut hindrar inte införskaffande av nödvändiga reservdelar eller utrustning för utbyte. Det är svårt att veta om detta gäller reservdelar och utrustning från de nämnda leverantörerna och/eller om det endast gäller fram till den 1 januari 2025.
Operatörerna har mindre än fyra år på sig att byta ut samtlig utrustning från de uppräknade leverantörerna. Beroende på när tillstånden kan börja användas kan det bli kortare tid än så. Det måste i sammanhanget betraktas som orimligt kort tid. Tidpunkten för utrustningsbytet är den enda proportionalitetsbedömning som PTS har gjort och myndigheten har inte redovisat ur den kommit fram till bedömningen. Komponenter kan ha en betydligt längre faktiskt livslängd än den bokföringstekniska avskrivningstiden, huruvida detta är skälet till tidsgränsen till den 21 januari är oklart eller om tidsgränsen är bestämd av andra skäl. Det kan bli svåra avvägningar att göra för hur operatörerna ska göra med redan beställd men ännu inte levererad utrustning. Så länge beslutet dessutom är föremål för juridisk prövning kan det förutses att operatörernas inköp påverkas negativt och därmed även utbyggnaden av näten.

I skälen till beslutet anger PTS tillkommande villkor om att operatörer som använder utrustning från de uppräknade leverantörerna kontinuerligt ska genomföra analyser av risker och sårbarheter. Det är otydligt om detta är ett krav utöver det krav som ställs på säkerhetsskyddsanalys enligt 2 kap. säkerhetsskyddslagen. Det är också oklart vad som kan komma att hända om operatörerna inte skulle efterleva detta villkor. Det är också oklart om bilagorna till beslutet ska ses som villkor förknippade med beslutet.

Försämrad konkurrens

I och med det aktuella beslutet är det tydligt att fyra operatörers nät är av betydelse för Sveriges säkerhet och att dessa inte får vara beroende av personal eller funktioner i andra länder – inte ens andra länder inom EU. I och med de stora kostnader som är förknippade med detta, den administrativa börda som det innebär och svårigheterna att upphandla utrustning och tillgång till personal kommer dessa kommunikationsleverantörer att få ett sämre utgångsläge jämfört med andra operatörer som inte har dessa krav och villkor förknippade med deras verksamheter. Det innebär också att operatörer som har som affärsidé att tillhandahålla nät som tillämpar den högsta nivån av säkerhet och av affärsmässiga skäl väljer att enbart använda utrustning från en viss särskild tillverkare tappar den unika egenskapen som utmärker deras erbjudande från dess konkurrenter.
Det finns endast ett fåtal tillverkare och leverantörer av utrustning till mobilnät – inklusive 5G-nät. Genom att begränsa möjligheten att förvärva utrustning från leverantörer blir

utbyggnaden av 5G-näten sannolikt mycket dyrare och långsammare till följd av att konkurrensen mellan leverantörer minskar eller försvinner i vissa avseenden men också att dessa leverantörer kommer att tvingas öka produktionstakten av utrustning. Det finns en uppenbar risk att operatörerna kommer att tvingas vänta lång tid på att få tillgång till utrustning då de kvarvarande leverantörernas kötid för leveranser kommer att öka, vilket i sig kommer att försena utbyggnaden av näten.
De aktuella operatörerna har också mycket olika förutsättningar då det gäller att uppfylla kraven eftersom vissa operatörer har betydligt mer utrustning i sina nät från de aktuella tillverkarna. Det innebär att det kommer bli avsevärt dyrare och besvärligare för vissa av operatörerna att uppfylla kraven, något som innebär en konkurrensnackdel gentemot konkurrenterna.

Den inre marknaden på området elektronisk kommunikation och nationell säkerhet
I Fördraget om Europeiska Unionen (FEU) anges i Artikel 4.2 att Unionen ska respektera medlemsstaternas likhet inför fördragen samt deras nationella identitet, som kommer till uttryck i deras politiska och konstitutionella grundstrukturer, inbegripet det lokala och regionala självstyret. Den ska respektera deras väsentliga statliga funktioner, särskilt funktioner vars syfte är att hävda deras territoriella integritet, upprätthålla lag och ordning och skydda den nationella säkerheten. I synnerhet ska den nationella säkerheten också i fortsättningen vara varje medlemsstats eget ansvar.

EU-domstolen har förtydligat att denna bestämmelse endast ska användas för att skydda mot aktiviteter som allvarligt kan destabilisera grundläggande konstitutionella, politiska, ekonomiska eller sociala strukturer i ett land, speciellt vad avser aktiviteter som direkt hotar samhället, befolkningen eller staten.[20] Utöver detta måste åtgärderna om de begränsar enskildas fri och rättigheter också vara proportionella och strikt nödvändiga i ett demokratiskt samhälle. Någon proportionalitetsbedömning för denna typ av inskränkning har inte gjorts, varken av lagstiftaren eller av PTS.

Genom att definiera operatörernas mobilnät i sin helhet som av betydelse för Sveriges säkerhet så innebär det en betydande osäkerhet om vilka delar av näten som Sverige menar fortfarande omfattas av EU-regelverket om elektronisk kommunikation. Frågor om nationell säkerhet ligger, som nämnts, utanför EU-rätten enligt art 4.2 EU-fördraget, därför finns det en stor risk att stora delar av EU-regelverket om elektronisk kommunikation inte kan tillämpas på svenska 5G-nät och i slutändan mobilnäten, samtidigt som det senaste

[20] Stycke, 74, och La Quadrature du Net and Others, C-511/18, C-512/18 och C-520/18, stycke 135.

direktivet[21] har ett tydligt fokus att främja 5G-utvecklingen inom unionen. Det blir därför väldigt oklart vilka regler som ska tillämpas, kanske blir det endast de EU-regler som rör hantering och rapportering av incidenter som inte är kopplade till antagonistiska hot, dvs. olyckor och naturkatastrofer.

Den regulatoriska osäkerheten kan bli mycket långvarig då det inte är otänkbart att dessa frågor i slutändan behöver avgöras i EU-domstolen.

Förslag om sanktioner för brott mot säkerhetsskyddslagen
Under år 2021 kan det komma att införas sanktionsavgifter för brott mot säkerhetsskyddslagen. Givet de stora kostnaderna för att tillämpa säkerhetsskyddslagens regelverk på alla delar av operatörernas nät kan detta komma att bli en tillkommande kostnad för operatörerna som kan få svårt att mäkta med de nya ökade kraven i tid.

Samhällsekonomiska konsekvenser
Radiospektrum är en naturresurs av mycket stort samhällsekonomiskt värde. Detta värde realiseras i samhället framförallt genom den nytta som tjänster baserade på radiospektrum genererar. Genom nya tekniker och användarfall kan nyttan som radionäten genererar öka. Men även de säkerhetsfunktioner för samhället och enskilda som kan implementeras och de effektiviseringar och besparingar som kan göras såväl avseende miljö som andra viktiga värden, kan möjliggöra ökad nytta för samhället och för samhällsekonomin. Då värdefulla frekvenser tilldelas i en auktion genereras icke obetydliga auktionsintäkter till statskassan. Om PTS genomför auktionen med rättsläget avseende de aktuella villkoren olöst kommer det troligen att påverka auktionslikviden negativt på grund av den osäkerhet som råder. Operatörerna kommer ändå att behöva värdera spektrumtillgången såsom att villkoret är rättsligt bindande även om det sedan skulle visa sig inte hålla i en domstolsprövning. Om PTS avvaktar med att hålla auktionen tills de rättsliga frågorna är slutligt avgjorda kommer det att ytterligare bromsa ned utbyggnaden av 5G-näten i Sverige. Den rättsliga processen kan ta flera år, och även kommande frekvenstilldelningar, bland annat omtilldelning av 900 MHz-bandet som idag redan används av mobiloperatörerna och där tillstånden går ut år 2025, riskerar då att påverkas.

Genom de stora osäkerheter såväl avseende de aktuella tillståndsvillkoren samt de regulatoriska kraven inbegripet stora kostnader för operatörerna är det inte otänkbart att statens intäkter från auktionen kommer att bli signifikant lägre samtidigt som det kan förutses att den tekniska utvecklingen, innovationen och tillgången till 5G för enskilda,

[21] Skäl 12, 123 och 135 i Europaparlamentets och rådets direktiv om inrättande av en europeisk kodex för elektronisk kommunikation.

företag och myndigheter kommer att bromsas ned betydligt. Detta kan vidare få negativa konsekvenser för hur Sverige och svenska företag uppfattas som handelspartner i internationella sammanhang. Samtidigt är inte säkert att de positiva effekter som bland annat minskad underrättelseinhämtning om infrastruktur som en del i en kartläggning av Sveriges civila infrastruktur eller för att inhämta eller överföra civil teknologi – som PTS nämner i sitt beslut – kommer att uppstå genom att dessa leverantörer utesluts från att leverera utrustning till de mobila näten.

Det finns en uppenbar risk att åtgärderna inte möter det hot som åtgärderna har för avsikt att möta

Det har inte tydligt angivits vad åtgärderna genom villkoren ska uppnå. Av den hotbild som PTS lyfter fram ges emellertid en fingervisning av vilka hot man tänker sig att konsekvenserna av beslutet ska möta. Det saknas emellertid en analys som visar att det åtgärder som införs genom tillståndsvillkoren leder till en minskning av den risk som PTS har påtalat.

I en rapport som tagits fram gemensamt av Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap, Polismyndigheten och Säkerhetspolisen (samarbetsmyndigheterna), *Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden* presenterar myndigheterna tillsammans – utifrån de lägesuppfattningar som respektive myndighet har – en lägesbild som på ett enkelt och tillgängligt sätt beskriver cybersäkerhet ur ett nationellt perspektiv.[22] I rapporten påtalas framför allt betydelsen av tillgänglighet vad avser eltillförsel och elektroniska kommunikationer som en brist.

Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, PTS och Säkerhetspolisen har gemensam tagit fram en rapport Cybersäkerhet i Sverige – Rekommenderade säkerhetsåtgärder.[23] En av de säkerhetshöjande åtgärder som nämns är att endast tillåta godkänd utrustning i nätverket. Säkerhetsåtgärden handlar emellertid endast om att motverka att obehöriga enheter får åtkomst till organisationens informationssystem – inte att utesluta utrustning från vissa leverantörer. Det är enligt dessa myndigheter organisationen själv som ska godkänna utrustningen för anslutning till informationssystem.

I sammanhanget kan det vara på sin plats att nämna att om hotet man vill möta är att undvika underrättelseinhämtning så är det självfallet så att den aktör som står för det hotet

[22] Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden, 2020, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cyberhot/.
[23] Cybersäkerhet i Sverige – Rekommenderade säkerhetsåtgärder, 2020, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cyberhot/.

inte har något intresse att de elektroniska kommunikationerna ska upphöra så att de inte längre är tillgängliga eftersom då upphör också tillgången till färska underrättelser. Underrättelsehotet möter man således huvudsakligen med informationssäkerhetsåtgärder och tillgänglighetshotet möter man med robusthetshöjande åtgärder. Det har inte i PTS beslut gjorts någon analys som visar att de aktuella ländernas möjligheter till inhämtning av information skulle minska om de utpekade leverantörernas utrustning utesluts från de elektroniska kommunikationsnäten. Rapporten om Rekommenderade säkerhetsåtgärder pekar istället på verktyg som en verksamhetsutövare kan använda för att minska risken för att obehöriga får åtkomst till information. Bland annat genom att säkerställa en förmåga att upptäcka säkerhetshändelser, till exempel loggar och nätflödesanalysverktyg.

Sammanfattningsvis
Sammantaget riskerar de åtgärder PTS nu vidtar att leda till omfattande fördyringar, ökad administration, minskad och inbromsad utbyggnad, försämrad innovation och försämrad konkurrenskraft inom hela samhället för ett problem som det är högst osäkert att åtgärderna löser. Underrättelsehotet från andra stater med metoder som använder allmänt tillgängliga elektroniska kommunikationsnät kommer att fortsätta och kanske till och med bli mer framgångsrik eftersom vi invaggar oss själva i en falsk trygghet om att våra nät i framtiden kommer att vara så mycket säkrare från det hot som PTS har identifierat i beslutet.

Vad kan man göra istället då?

EU:s cybersäkerhetsakt tillhandahåller ett ramverk för cybersäkerhetscertifiering. Det är inte tvingande eftersom processen är kostsam. Samtidigt skulle det kunna innebära att en del av denna kostnad fördelas även på leverantörerna. Därför hade det kanske varit bättre att ställa krav på att använda cybersäkerhetscertifierade produkter i 5G-näten. Certifiering är dock ingen garanti för att antagonistiska aktörer kan komma att använda eller dra nytta av felaktigheter eller sårbarheter i utrustning som finns i näten. Men det skapar i varje fall en genomlysning och en möjlighet till granskning samt en möjlighet att sanktionera leverantörer som inte lever upp till kraven.

De verksamheter som är beroende av starkt skydd för konfidentialitet, tillgänglighet och riktighet kan ändå inte strunta i att vidta egna åtgärder för att skydda sina informationstillgångar och verksamheter i enlighet med de risk- och sårbarhetsanalyser som de ändå måste göra.

Utöver detta kan robusthetshöjande åtgärder användas. Delar av det skulle kunna bestå i näten endast till viss del får vara uppbyggda av utpekade leverantörers utrustning och komponenter.

Rättslig kontext

Konstitutionell EU-rätt

EU-rätten är en självständig rättsordning. Samtidigt utgör EU-rätten en del av varje medlemsstats rättsordning och medlemsstaterna är skyldiga att tillämpa och ge effekt åt dess regler och principer.

Av artikel 3 fördraget om Europeiska unionen (FEU) framgår EU:s mål och i artikeln upprättas den fria rörligheten för personer inom EU och den inre marknaden som ska bygga på en välavvägd ekonomisk tillväxt och på prisstabilitet, på en social marknadsekonomi med hög konkurrenskraft där full sysselsättning och sociala framsteg eftersträvas.

Av artikel 4.2 i FEU framgår att unionen ska respektera medlemsstaternas likhet inför fördragen samt deras nationella identitet, som kommer till uttryck i deras politiska och konstitutionella grundstrukturer, inbegripet det lokala och regionala självstyret. Den ska respektera deras väsentliga statliga funktioner, särskilt funktioner vars syfte är att hävda deras territoriella integritet, upprätthålla lag och ordning och skydda den nationella säkerheten. I synnerhet ska den nationella säkerheten också i fortsättningen vara varje medlemsstats eget ansvar.

Av artikel 49 fördraget om Europeiska unionens funktionssätt (FEUF) framgår att inskränkningar för medborgare i en medlemsstat att fritt etablera sig på en annan medlemsstats territorium ska förbjudas. Detta förbud ska även omfatta inskränkningar för medborgare i en medlemsstat som är etablerad i någon medlemsstat att upprätta kontor, filialer eller dotterbolag. Etableringsfriheten ska innefatta rätt att starta och utöva verksamhet som egenföretagare samt rätt att bilda och driva företag [..] på de villkor som etableringslandets lagstiftning föreskriver för egna medborgare, om inte annat följer av bestämmelserna i kapitlet om kapital.

Av artikel 52.1 FEUF framgår bland annat att bestämmelserna om etableringsfrihet inte ska hindra tillämpning av bestämmelser i lagar och andra författningar som föreskriver särskild behandling av utländska medborgare och som grundas på hänsyn till allmän ordning, säkerhet eller hälsa.

Av artikel 56 FEUF framgår bland annat att inskränkningar i friheten att tillhandahålla tjänster inom unionen ska förbjudas beträffande medborgare i medlemsstater som har etablerat sig i en annan medlemsstat än mottagaren av tjänsten.

Europeiska unionens stadga om de grundläggande rättigheterna (stadgan)

Av artikel 16 i stadgan framgår att näringsfriheten ska erkännas i enlighet med unionsrätten samt nationell lagstiftning och praxis.

Enligt artikel 52.1 i stadgan ska varje begränsning i utövandet av de rättigheter och friheter som erkänns i stadgan vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

Direktivet om en europeisk kodex för elektronisk kommunikation (koden)

Den 11 december 2018 beslutades om Europaparlamentets och rådets direktiv om inrättande av en europeisk kodex för elektronisk kommunikation. Ett tydligt fokus på direktivets tillämplighet har bland annat varit den femte generationens trådlösa kommunikationsmiljö, vilket till exempel framgår av skäl 12, 123 och 135.
Direktivet har ännu inte implementerats i svensk nationell lagstiftning. Ärendet bereds för närvarande inom Regeringskansliet.

I skäl 5 till koden anges att direktivet upprättar ett rättsligt ramverk för att säkerställa frihet att tillhandahålla elektroniska kommunikationsnät och kommunikationstjänster, med förbehåll för endast de villkor som fastställs i koden och eventuella begränsningar i enlighet med artikel 52.1 i EUF-fördraget (se ovan), särskilt åtgärder med hänsyn till allmän ordning, allmän säkerhet och folkhälsa, samt i enlighet med artikel 52.1 i stadgan (se ovan).

Av skäl 6 framgår att koden inte påverkar varje medlemsstats möjlighet att vidta nödvändiga åtgärder för att skydda sina väsentliga säkerhetsintressen, skydda allmän ordning och säkerhet samt tillåta att brott utreds, avslöjas och lagförs, med beaktande av att varje begränsning i utövandet av de rättigheter och friheter som erkänns i stadgan […] måste vara lagstadgade, respektera själva kärnan i dessa rättigheter och friheter och vara underställda proportionalitetsprincipen, i enlighet med artikel 52.1 i stadgan.
Av skäl 117 framgår att när medlemsstater undantagsvis beslutar att begränsa friheten att tillhandahålla elektroniska kommunikationsnät och kommunikationstjänster på grunder som avser allmän ordning, allmän säkerhet eller folkhälsa bör medlemsstaterna förklara skälen till denna begränsning.

Skäl 135 i koden anger bland annat att I syfte att säkerställa ökad samordning av tillgången till radiospektrum fram till 2020 och bygga upp mycket snabba fasta och trådlösa nät i 5G-

sammanhang, har RSPG identifierat frekvensbanden 3,4–3,8 GHz och 24,25–27,5 GHz som prioriterade band som är lämpade för att uppfylla målen för handlingsplanen för 5G fram till 2020. Det är därför nödvändigt att säkerställa att frekvensbanden 3,4–3,8 GHz och 24,25–27,5 GHz eller delar av dem senast den 31 december 2020 är tillgängliga för markbundna system som kan tillhandahålla trådlösa bredbandstjänster enligt harmoniserade villkor som fastställts genom tekniska genomförandeåtgärder antagna i enlighet med artikel 4 i beslut nr 676/2002/EG, som ett komplement till Europaparlamentets och rådets beslut (EU) 2017/899 (33), eftersom de banden har särskilda egenskaper när det gäller täckning och datakapacitet, som gör det möjligt att kombinera dem på lämpligt sätt för att uppfylla kraven för 5G

Målet med koden är bland annat att genomföra en inre marknad för elektroniska kommunikationsnät och kommunikationstjänster som leder till anläggning och nyttjande av nät med mycket hög kapacitet, hållbar konkurrens och interoperabilitet för elektroniska kommunikationstjänster, tillgänglighet, säkerhet för nät och tjänster samt nytta för slutanvändare samt genom effektiv konkurrens och valmöjligheter säkerställa att allmänt tillgängliga tjänster av god kvalitet och till ett överkomligt pris tillhandahålls i hela unionen (artikel 1.2 a och b).

Artikel 3 c) anger att koden inte påverkar åtgärder som medlemsstater vidtagit för ändamål som rör allmän ordning och säkerhet samt försvar.

Svensk konstitutionell rätt

Vid beredningen av regeringsärenden ska behövliga upplysningar och yttranden inhämtas från berörda myndigheter. Upplysningar och yttranden ska också i den omfattning som behövs inhämtas från kommuner. Även sammanslutningar och enskilda ska i den omfattning som behövs ges möjlighet att yttra sig (7 kap 2 § regeringsformen).

Lagen om elektronisk kommunikation

Av 3 kap. 6 § 7 p lagen (2003:389) om elektronisk kommunikation (LEK) framgår bland annat att tillstånd att använda radiosändare ska beviljas om det kan antas att radioanvändningen inte kommer att orsaka skada för Sveriges säkerhet.

Tillstånd att använda radiosändare får förenas med villkor bland annat om krav som är av betydelse för Sveriges säkerhet, (3 kap. 11 § 10 p LEK).

Villkor som innebär en begränsning av vilka elektroniska kommunikationstjänster eller vilka tekniker som får användas, får, enligt 3 kap. 11 § 2 st. LEK, meddelas endast om det krävs för att

1. undvika skadlig störning,
2. säkerställa ett effektivt frekvensutnyttjande,
3. skydda människors liv eller hälsa,
4. tillgodose det allmännas intresse av att vissa elektroniska kommunikationstjänster finns tillgängliga i vissa delar av landet, eller
5. tillgodose det allmännas intresse av att främja tillhandahållandet av radio- och tv-tjänster för vilka tillstånd meddelats enligt annan lag.

Förarbetena till de aktuella bestämmelserna

Förslaget till 3 kap. 6 § 7 p LEK lämnades först i betänkandet *Frekvenser i samhällets tjänst (SOU 2018:92)*. I förslaget användes ”*vållar fara*” för Sveriges säkerhet i anslutning till terminologin i 15 kap. 2 § offentlighets och sekretesslagen (2009:400) (OSL). I lagrådsremissen valdes istället uttrycket ”*orsaka skada*” för Sveriges säkerhet framför allt för att anpassa regleringen till säkerhetsskyddslagens terminologi.[24]
Förslaget till 3 kap. 11 § 10 p LEK i SOU 2018:92 är identiskt med det beslut som riksdagen sedermera beslutade.

Direktiven till utredningen och betänkandets arbete fokuserade uteslutande på radiofrekvensanvändning. Sändning av radiovågor är definitionen av radiosändare enligt 1 kap. 7 § LEK.[25] Radiosändare är alltså endast den utrustning som alstrar radiovågor. Inte något annat. Av denna anledning utreddes inte heller några konsekvenser av att annan utrustning i de allmänt tillgängliga elektroniska kommunikationsnäten skulle kunna omfattas av tillståndsvillkor. Tanken med de aktuella bestämmelserna var framför allt att skapa ett heltäckande regelverk och att möjliggöra särskilda åtgärder i anslutning till beslut om höjd beredskap.[26]

Promemorian *Kompletterande förslag till betänkandet Frekvenser i samhällets tjänst (SOU 2018:92)* gav inga förslag till andra skrivningar i ovan nämnda lagrum än det som SOU 2018:92 lämnade. I utgångspunkterna för promemorian nämns säkerhetsproblem med den utrustning som används som exempel på när radioanvändning kan medföra säkerhetshot mot Sverige. Detta exempel nämns även i den allmänna motiveringen till den kompletterande bestämmelsen om att PTS ska samråda med Säkerhetspolisen och Försvarsmakten i ärenden som rör tillstånd. I konsekvensanalysen berörs inte frågan om utrustning över huvud taget.

[24] Lagrådsremissen Skydd av Sveriges säkerhet vid radioanvändning sid. 29 samt prop. 2019/20:15 Skydd av Sveriges säkerhet vid radioanvändning s. 30, bet. 2019/20:TU4, rskr. 2019/20:74.
[25] Frekvenser i samhällets tjänst, SOU 2018:92, s. 59 ff. och bilaga 1.
[26] SOU 2018:92 s. 246 f.

Begreppet Sveriges säkerhet i LEK har enligt regeringen samma innebörd som i säkerhetsskyddslagen.[27]

I propositionen utvecklade regeringen tankegångarna något och förklarade att radioanvändning kan vara säkerhetshotande på grund av den tekniska utrustning som används. Det bör därför vara möjligt att i tillståndsvillkor ställa säkerhetskrav på den tekniska utrustning, den organisation eller de avtal som är relaterade till radiosändningen. Det bör också vara möjligt att t.ex. utesluta komponenter, leverantörer eller servicepersonal som inte håller en tillräckligt hög säkerhetsnivå.[28] I författningskommentaren uttrycks detta emellertid i positiv bemärkelse som att det handlar om att ställa villkor för att säkerställa att komponenter, leverantörer eller servicepersonal som används för eller har koppling till radioanvändningen håller en tillräckligt hög säkerhetsnivå.[29] Alltså inte att utesluta komponenter, leverantörer eller servicepersonal.

Säkerhetsskyddslagen

Säkerhetsskyddslagen gäller för utövare av säkerhetskänslig verksamhet vilket bland annat är den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet, 1 kap. 1 § säkerhetsskyddslagen (2018:585).

Sveriges säkerhet

Begreppet Sveriges säkerhet är inte definierat i lag. Regeringen förklarade i förarbetena att ange alla skyddsvärda verksamheter i författning är inte lämpligt eftersom det skulle riskera att ge främmande makt eller andra antagonistiska aktörer information om vilka de mest skyddsvärda verksamheterna i samhället är och att Sveriges säkerhet är ett etablerat uttryck som förekommer i annan lagstiftning och att det är detta uttryck som bör användas för att avgränsa tillämpningsområdet för säkerhetsskyddslagen, utan att uttrycket behöver definieras närmare.[30]

Regeringen uttalade i förarbetena till förra säkerhetsskyddslagen att uttrycket skydda totalförsvaret eller rikets säkerhet i övrigt omfattar såväl den yttre säkerheten till skydd för Sveriges försvarsförmåga, politiska oberoende och territoriella suveränitet som den inre säkerheten till skydd för Sveriges demokratiska statsskick.[31] Regeringen uttalade sig på nytt om uttryckets innebörd i samband med propositionen Förstärkt skydd mot främmande makts underrättelseverksamhet och angav då att uttrycket kan sammanfattas som skyddet

[27] Lagrådsremissen Skydd av Sveriges säkerhet vid radioanvändning s. 28 och 44, samt prop. 2019/20:15 Skydd av Sveriges säkerhet vid radioanvändning s. 29 och 45, bet. 2019/20:TU4, rskr. 2019/20:74.
[28] Skydd av Sveriges säkerhet vid radioanvändning, prop. 2019/20: 15 s. 31.
[29] Prop. 2019/20: 15 s. 45.
[30] Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag, prop. 2017/18:89 s. 42.
[31] Säkerhetsskydd, prop. 1995/96:129 s. 22 f.

för Sveriges oberoende – i betydelsen självständighet och suveränitet – och bestånd. Det innefattar en rätt till okränkta landsgränser, ett bevarande av det svenska självstyret och det demokratiska statsskicket samt av nationens grundläggande funktionalitet. Rikets säkerhet tar således inte enbart sikte på skyddet av det fysiska territoriet. Det avser också hävdandet av Sveriges suveränitet, vilket innebär att Sverige ska kunna bruka sin exklusiva frihet under det folkrättsliga regelverket, för att på det egna territoriet självständigt utöva statens funktioner, såväl vad avser statens inre som yttre förbindelser.[32]

I samband med införandet av nu gällande lagstiftning angav regeringen att tillämpningsområdet för säkerhetsskyddslagen även fortsättningsvis endast bör gälla sådana verksamheter som har ett kvalificerat skyddsbehov.[33]
Skälen för detta är att en verksamhetsutövare måste vidta relativt långtgående åtgärder för att skydda hemliga uppgifter eller annan säkerhetskänslig verksamhet.

Säkerhetsskyddsåtgärderna kan vara kostsamma och medföra en extra administrativ påfrestning inom en organisation. Ett annat skäl är att säkerhetsskyddsåtgärderna kan innebära intrång i enskildas integritet. Personal som ska ha tillgång till säkerhetsskyddsklassificerad information behöver t.ex. genomgå säkerhetsprövning och tillträde till vissa områden och byggnader kan vara begränsat till endast en del av de anställda. Därför bör lagstiftningen även fortsättningsvis endast omfatta de verksamheter som av särskilda skäl har behov av säkerhetsskyddande åtgärder.

Behovet av skydd för verksamheter som inte anses ha ett så kvalificerat skyddsbehov men som ändå kan anses samhällsviktiga får i första hand tillgodoses genom annan kris- och skyddslagstiftning, t.ex. sådan vars primära syfte är att upprätthålla kontinuitet i samhällsviktig verksamhet. I propositionen Stärkt krisberedskap – för säkerhets skull definieras samhällsviktig verksamhet som en verksamhet som uppfyller båda eller det ena av följande villkor.

- Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället.
- Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.[34]

Den ovan nämnda definitionen omfattar ett mycket stort antal verksamheter. Verksamheter som bör omfattas säkerhetsskyddslagen omfattas i regel också av dessa kriterier, men för att

[32] Förstärkt skydd mot främmande makts underrättelseverksamhet, prop. 2013/14:51 s. 20
[33] Prop. 2017/18:89 s. 38 f.
[34] Stärkt krisberedskap - för säkerhets skull, prop. 2007/08:92 s. 33.

omfattas av säkerhetsskyddslagen ska verksamheten därutöver karaktäriseras av att den har betydelse för Sveriges säkerhet ur ett nationellt perspektiv.[35]

Grundläggande för säkerhetsskyddslagstiftningen är att ansvaret för identifiering och bedömning av behovet av säkerhetsskydd är knutet till verksamhetsutövaren. Regeringen förklarade att det inte är lämpligt att ge tillsynsmyndigheter ansvar och mandat att utifrån sin analys peka ut vilka verksamheter som omfattas av lagstiftningen.[36]

Säkerhetsskydd

Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetskyddsklassificerade uppgifter.

Med säkerhetskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämpliggifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig

Krav på den som bedriver säkerhetskänslig verksamhet

Den som bedriver säkerhetskänslig verksamhet ska utreda behovet av säkerhetsskydd. Säkerhetsskyddsanalysen ska dokumenteras, 2 kap. 1 § säkerhetsskyddslagen. Verksamhetsutövaren ska planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.

Verksamhetsutövaren ska även kontrollera säkerhetsskyddet i den egna verksamheten, anmäla och rapportera sådant som är av vikt för säkerhetsskyddet och i övrigt vidta de åtgärder som krävs enligt säkerhetsskyddslagen.

Innan ett informationssystem som förutses komma att behandla säkerhetsskyddsklassificerade uppgifter av klass 3 (konfidentiell) eller högre tas i drift ska verksamhetsutövaren samråda med Säkerhetspolisen. Samma sak gäller för verksamheter där obehörig åtkomst kan medföra en skada för Sveriges säkerhet som inte är obetydlig (klass 3), 3 kap. 2 § säkerhetsskyddsförordningen).

---

[35] Prop. 2017/18:89 s. 40.
[36] Prop. 2017/18:89 s. 43.

Ett informationssystem som ska användas i säkerhetskänslig verksamhet får inte tas i drift förrän det godkänts ur säkerhetsskyddssynpunkt av verksamhetsutövaren. Godkännandet ska dokumenteras.

Säkerhetsskyddsåtgärderna består av tre delar: Informationssäkerhet, Fysisk säkerhet och personalsäkerhet

Informationssäkerhet

Informationssäkerhet ska förebygga att säkerhetskyddsklassificerade uppgifter röjs, ändras görs otillgängliga eller förstörs samt förebygga skadlig inverkan på informationssystem som gäller säkerhetskänslig verksamhet, (2 kap. 2 § säkerhetsskyddslagen).
Säkerhetskyddsklassificerade uppgifter ska delas in i säkerhetskyddsklasser från 1-4 där 1 är högsta och 4 är lägsta klassen, (2 kap. 5 § säkerhetsskyddslagen).
Innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift ska verksamhetsutövaren ta fram och dokumentera en särskild säkerhetskyddsbedömning, (3 kap. 1 § säkerhetsskyddsförordningen).

Fysisk säkerhet

Den fysiska säkerheten ska förebygga att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där det finns säkerhetsskyddsklassificerade uppgifter eller bedrivs säkerhetskänslig verksamhet, (2 kap. 3 § säkerhetsskyddslagen).
Områden, byggnader och andra anläggningar eller objekt där säkerhetsskyddsklassificerade uppgifter förvaras eller annars behandlas, eller där säkerhetskänslig verksamhet i övrigt bedrivs, ska vara försedda med funktioner för att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan utifrån ett identifierat säkerhetsskyddsbehov, (4 kap 1 § säkerhetsskyddsförordningen).

Verksamhetsutövaren ska ha ett passersystem för identifiering eller behörighetskontroll till utrymmen där det kan ges tillgång till säkerhetskänslig verksamhet, (5 kap. 6 § Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2)). Verksamhetsutövaren ska också, i den utsträckning skyddsdimensioneringen kräver, använda personell bevakning eller teknisk övervakning för att tidigt upptäcka obehörigt tillträde eller skadlig inverkan, (5 kap. 2 § Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2)).

Personalsäkerhet

Personalsäkerheten ska förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som är säkerhetskänslig samt säkerställa att de som deltar i verksamheten har tillräcklig kunskap om säkerhetsskydd, (2 kap. 4 § säkerhetsskyddslagen).

Alla som ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas. Syftet är att kartlägga om en person kan antas vara lojal mot de intressen som skyddas av säkerhetsskyddslagen och i övrigt pålitlig från säkerhetssynpunkt, (3 kap. 1–2 §§ säkerhetsskyddslagen). Säkerhetsprövningen ska göras innan personen får delta i den säkerhetskänsliga verksamheten, (3 kap 3 § säkerhetsskyddslagen). Det är den som beslutar om anställning eller deltagande i den säkerhetskänsliga verksamheten som ska göra bedömningen, om det finns anledning till det ska en tidigare gjord bedömning omprövas.
Säkerhetsprövningen består av en registerkontroll och särskild personutredning. Anställningar eller deltagande i säkerhetskänslig verksamhet ska placeras i säkerhetsklass beroende på vilken omfattning och hur säkerhetskänsliga uppgifter eller hur säkerhetskänslig verksamheten är som personen ska delta i. Säkerhetsklasserna är indelade i tre nivåer. Där 1 är den högsta klassen.

För säkerhetsklass 1 och 2 får belastningsregistret, misstankeregistret samt uppgifter som behandlas med stöd av brottsdatalagen eller lagen om Säkerhetspolisens behandling av personuppgifter hämtas. Motsvarande uppgifter får även hämtas om den kontrollerades make eller sambo. För säkerhetsklass 3 får uppgifter om make eller sambo inhämtas. Om det finns synnerliga skäl får även andra uppgifter inhämtas, (3 kap. 14 § säkerhetsskyddslagen).

För anställning eller deltagande i verksamhet som placerats i säkerhetsklass 1 eller 2 ska en särskild personutredning göras. Utredningen ska omfatta en undersökning av den kontrollerades ekonomiska förhållanden och i övrigt ha den omfattning som behövs, (3 kap. 17 § säkerhetsskyddslagen).

Det är PTS som ska besluta om säkerhetsklass för anställning eller annat deltagande i verksamhet hos enskilda verksamhetsutövare, (5 kap. 11 § säkerhetsskyddsförordningen). Det är också PTS som i varje enskilt fall ska ansöka om registerkontroll hos Säkerhetspolisen. Det är endast om det finns särskilda skäl som en enskild verksamhetsutövare får ansöka om registerkontroll hos Säkerhetspolisen, (5 kap. 15 – 16 §§ säkerhetsskyddsförordningen).

Verksamhetsutövaren ska se till att alla som anställs eller på annat sätt är delaktig i säkerhetskänslig verksamhet får utbildning i säkerhetsskydd. Behovet av utbildning ska följas upp under hela tiden som deltagandet pågår, (5 kap 1 § säkerhetsskyddslagen).
När en anställning har upphört eller något annat deltagande som föranlett placering i säkerhetsklass upphör ska verksamhetsutövaren skyndsamt anmäla till Säkerhetspolisen att registerkontrollen ska avslutas, (5 kap. 22 § säkerhetsskyddsförordningen).

Om det förekommer uppgifter av klass 1-3 eller motsvarande klassificering för säkerhetskänslig verksamhet ska enskilda verksamhetsutövare ska ingå ett särskilt säkerhetskyddsavtal innan köp av varor, tjänster eller byggentreprenader. I avtalet ska anges hur kraven på säkerhetsskydd ska tillgodoses av leverantören. Verksamhetsutövaren ska kontrollera att leverantören följer säkerhetsskyddsavtalet, 2 kap 6 § säkerhetsskyddslagen.
En enskild verksamhetsutövare som avser att ingå ett säkerhetskyddsavtal ska utan dröjsmål anmäla det till PTS. Efter att säkerhetsskyddsavtalet har ingått ska det anmälas till Säkerhetspolisen. Anmälan till Säkerhetspolisen ska också göras när ett säkerhetsskyddsavtal upphör att gälla, (2 kap. 5 och 7 §§ säkerhetsskyddsförordningen).
Om uppgifterna rör klass 4 eller motsvarande klassificering för verksamhet ska säkerhetsskyddet regleras på något annat sätt än genom ett säkerhetsskyddsavtal, 7 kap 1 § Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2).
Efter den 1 januari 2022 får säkerhetsskyddsklassificerade uppgifter inte lämnas till en leverantör som kommer från ett land som Sverige inte har ingått ett internationellt säkerhetsskyddsåtagande (Generellt säkerhetsskyddsavtal, GSA) och leverantören inte godkänts enligt det landets lagstiftning, 3 kap 9 § säkerhetsskyddsförordningen samt p. 6 i övergångsbestämmelserna nämnda förordning.[37] Detta gäller oavsett vilken klass uppgifterna är placerade i men det gäller enbart säkerhetsskyddsklassificerade uppgifter det är inte kopplat till verksamheter.

Rapporteringsskyldighet

En verksamhetsutövare ska skyndsamt anmäla till Säkerhetspolisen om en säkerhetsskyddsklassificerad uppgift kan ha röjts, om det inträffat en it-incident i ett it-system som har betydelse för säkerhetskänslig verksamhet och incidenten allvarligt kan påverka säkerheten i systemet eller om verksamhetsutövaren får kännedom eller misstanke om någon annan för denne allvarlig säkerhetshotande verksamhet, (2 kap. 10 § säkerhetskyddsförordningen). Även underleverantörer omfattas av denna rapporteringsskyldighet, (2 kap. 11 § säkerhetskyddsförordningen).

Överlåtelse av säkerhetskänslig verksamhet (träder i kraft den 1 januari 2021)[38]

Den som tänker överlåta hela eller delar av säkerhetskänslig verksamhet eller egendom som har betydelse för Sveriges säkerhet ska innan ett förfarande inleds göra en särskild säkerhetsskyddsbedömning och med utgångspunkt från denna bedömning göra en prövning

[37] Sverige har idag GSA med Australien, Belgien, Brasilien, Bulgarien, Danmark, Estland, ESA, EU, Finland, Frankrike, Island, Italien, Irland, Jugoslavien (Bosnien och Hercegovina, Serbien), Kanada, Kroatien, Lettland, Litauen, Luxemburg, NATO, Nederländerna, Norge, Polen, Portugal, Rumänien, Schweiz, Singapore, Slovakien, Slovenien, Spanien, Storbritannien och Nordirland, Sydafrika, Sydkorea, Tjeckien, Tyskland, Ungern, USA och Österrike.
[38] Åtgärder till skydd för Sveriges säkerhet vid överlåtelser av säkerhetskänslig verksamhet, prop. 2020/21:13, bet. 2020/21:JuU10, rskr. 2020/21:79.

om överlåtelsen är lämplig från säkerhetsskyddssynpunkt. Bedömningen och prövningen ska dokumenteras, (2 kap. 8 § säkerhetsskyddslagen).
Om prövningen resulterar i att överlåtelsen är olämplig får den inte genomföras om den leder till att överlåtelsen inte är olämplig ska samråda med den särskilt utsedda samrådsmyndigheten. Samrådsskyldigheten gäller även vid överlåtelse av aktier. Samrådsmyndigheten får förelägga verksamhetsutövaren att vidta åtgärder för att fullgöra sina skyldigheter enligt säkerhetsskyddslagen och om föreläggande inte följs får samrådsmyndigheten förbjuda överlåtelsen, (2 kap. 9 och 11 §§ säkerhetsskyddslagen). Överlåtelser i strid mot ett förbud är ogiltiga. Överlåtelser som genomförs utan samråd och förutsättningarna för förbud är uppfyllda kan innebära att samrådsmyndigheten förklarar överlåtelsen ogiltig genom förbud, 2 kap. 12 § säkerhetsskyddslagen).

Kommande ändringar i säkerhetsskyddslagen

Regeringen har aviserat ytterligare förändringar i säkerhetsskyddslagen under 2021. Bland annat finns förslag om att komplettera säkerhetsskyddslagen med ett sanktionsavgiftsystem enligt vilket en verksamhetsutövare kan komma att bli skyldig att betala en sanktionsavgift om denne bryter mot bestämmelserna i säkerhetsskyddslagen. Sanktionsavgiften föreslås uppgå till mellan 5 000 kr och 10 miljoner kronor.

EU:s cybersäkerhetsakt

Den 17 april 2019 antogs Europaparlamentets och rådets förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

Det huvudsakliga syftet med cybersäkerhetsakten är att säkerställa en väl fungerande inre marknad och samtidigt sträva efter att uppnå en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen. Det europeiska ramverket för cybersäkerhetscertifiering är bland annat avsett att ge följande fördelar för företag och enskilda:

- cybersäkerhetsakten ska stödja och underlätta utvecklingen av en europeisk cybersäkerhetspolitik genom att harmonisera villkoren och de materiella kraven för cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster i EU,
- europeiska ordningar för cybersäkerhetscertifiering ska hänvisa till gemensamma standarder eller kriterier för utvärderings- och testmetoder, vilket bidrar till användningen av gemensamma säkerhetslösningar i EU och undanröjer hinder för den inre marknaden,
- cybersäkerhetsakten ska stödja och komplettera genomförandet av NIS-direktivet genom att förse de företag som omfattas av direktivet med ett verktyg för att visa att nät- och informationssäkerhetskraven uppfylls i hela unionen,

- de europeiska ordningarna för cybersäkerhetscertifiering ska ha företräde framför de nationella systemen och ersätter befintliga parallella nationella ordningar avseende samma IKT-produkter eller IKT-tjänster på en angiven tillförlitlighetsnivå,
- företag ska bara behöva certifiera produkten en gång, och certifikat som utfärdas enligt de europeiska ordningarna ska gälla i alla medlemsstater,
- företag ska få en kontaktpunkt för cybersäkerhetscertifiering inom EU, och
- en produkt eller tjänst ska – beroende på cybersäkerhetsbehov – certifieras enligt en högre eller lägre nivå av säkerhet.

I artiklarna 46–65 i EU:s cybersäkerhetsakt finns bestämmelser om ett övergripande europeiskt ramverk för cybersäkerhetscertifiering. Genom cybersäkerhetsakten skapas en ram för inrättandet av certifieringsordningar för IKT-produkter, IKT-tjänster och IKT-processer (europeiska ordningar för cybersäkerhetscertifiering).
EU:s cybersäkerhetsakt inför en möjlighet för tillverkare och leverantörer att upprätta en s.k. EU-försäkran om överensstämmelse eller ansöka om ett europeiskt cybersäkerhetscertifikat som intygar att en särskild IKT-produkt, IKT-tjänst eller IKT-process uppfyller kraven i en europeisk ordning för cybersäkerhetscertifiering.

En EU-försäkran om överenstämmelse eller ett europeiskt cybersäkerhetscertifikat ska intyga att produkterna, tjänsterna och processerna uppfyller angivna säkerhetskrav när det gäller att skydda tillgänglighet, autenticitet, integritet och konfidentialitet hos lagrade, överförda eller behandlade data eller de funktioner eller tjänster som tillhandahålls av eller är tillgängliga via dessa produkter, tjänster och processer.

EU-försäkringar om överenstämmelse och europeiska cybersäkerhetscertifikat syftar även till att hjälpa slutanvändarna att göra informerade val och bidra till att harmonisera cybersäkerhetsrutinerna inom unionen.

Cybersäkerhetsakten ska inte påverka medlemsstaternas befogenheter i fråga om verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på straffrättens område, (artikel 2).

Cybersäkerhetscertifiering kan vara en kostsam process, vilket i sin tur kan leda till högre priser för kunder och konsumenter. Behovet av certifiering kan också variera beroende på i vilket sammanhanget produkterna och tjänsterna ska användas och den snabba tekniska utvecklingen. Därför är det – enligt cybersäkerhetsakten –frivilligt att använda en europeisk cybersäkerhetscertifiering, om inte annat föreskrivs i unionsrätten eller medlemsstaternas nationella rätt som antagits i enlighet med unionsrätten. På vissa områden kan det bli nödvändigt att i framtiden införa särskilda krav på cybersäkerhet och göra

cybersäkerhetscertifiering obligatorisk för vissa IKT-produkter, IKT-tjänster och IKT-processer för att förbättra cybersäkerheten i unionen, (skäl 92).