

Ert datum 2019-08-30  
Datum 2019-12-02  
Er referens Dnr I2019/02319/D  
Vår referens MB

Infrastrukturdepartementet

Inlämnas via e-post:

[i.remissvar@regeringskansliet.se](mailto:i.remissvar@regeringskansliet.se)

kopia:

[i.d.remiss@regeringskansliet.se](mailto:i.d.remiss@regeringskansliet.se)

## Remissvar avseende promemorian Genomförande av direktivet om inrättande av en kodex för elektronisk kommunikation

IT&Telekomföretagen har beretts tillfälle att lämna remissvar över rubricerad promemoria och vill med anledning av det framföra följande.

### *13.3 Tillträde till fysisk infrastruktur för att montera trådlösa accesspunkter med kort räckvidd*

Regeringen föreslår i implementeringen av artikel 57 att skyldigheten för offentliga myndigheter begränsas till statliga myndigheter, kommuner och landsting medan. Tillträde till byggnader eller anläggningar som ägs eller kontrolleras av statliga eller kommunala bolag omfattas således inte. Det framgår dock inte tydligt av promemorian av vilka skäl som regeringen har valt att göra denna begränsning. Enligt IT&Telekomföretagens uppfattning kan det också ifrågasättas om en sådan snäv tolkning är i linje med direktivet. I den engelska versionen används begreppet "public authorities", vilket är ett vidare begrepp än det svenska begreppet myndighet.

IT&Telekomföretagen ifrågasätter begränsningen och är oroade över dess konsekvenser. Möjligheten att få tillträde till byggnader och anläggningar skulle, med den föreslagna begränsningen, vara beroende av vilken förvaltningsform som en offentlig aktör valt. Det är t.ex. vanligt att fastigheter förvaltas i kommunala fastighetsbolag, vilket alltså leder till att tillträde till dessa byggnader inte skulle garanteras. I skenet av att direktivet ju syftar till att ge tillträde till offentliga byggnader så framstår den föreslagna begränsningen som svår att förstå. På likande sätt varierar det mellan olika regioner hur lokaltrafik organiserats, vilket påverkar möjligheten till tillträde till buss- och spårvagnshållplatser som är ett annat exempel i direktivet. IT&Telekomföretagen anser därför att begränsningen att skyldigheten inte ska omfatta statliga och kommunala bolag bör tas bort.

### 15.22 Ledningsrätt

Tillstånd för förläggning av fiber är avgörande för utbygganden av NGA och för att uppnå de politiska målen om bredbandsutbyggnad. I direktivet (beaktandesats 104) konstateras att:

”Tillstånd som utfärdats för tillhandahållare av elektroniska kommunikationsnät och kommunikationstjänster och som ger dem tillträde till offentlig eller privat egendom är grundläggande faktorer för etablerande av elektroniska kommunikationsnät eller nya nätelement. Onödigt krångel och förseningar i förfarandet för att tilldela ledningsrätter kan därför utgöra ett betydande hinder för konkurrensutvecklingen. Följaktligen bör förvärvet av ledningsrätter förenklas för auktoriserade företag.”

Att korsa vägar och att framförallt på landsbygd kunna förlägga fiber längs Trafikverkets vägnät är en förutsättning för utbyggnaden av fiber och för att Sverige ska kunna nå regeringens bredbandsmål. Att den statliga väginfrastrukturen bör ses som en resurs för den bredbandsinfrastruktur som nu behöver anläggas i Sveriges landsbygder konstaterade regeringen i det uppdrag Trafikverket fick 2018. Redan i nuvarande lagstiftning saknas dock en fullständig implementering av gällande direktivsregler om ledningsrätt. För att uppfylla artikel 31 och 43 i det nya direktivet krävs ändring av väglagen eller ledningsrättslagen. IT&Telekomföretagen förordar en ändring av den förra, där Trafikverkets bemyndigande tydliggörs och utvecklas till att bättre avspegla de villkor som Trafikverket sätter upp för att ge ledningsägare tillgång till vägområde. Enligt praxis kan inte ledningsrätt upplåtas inom ett område som omfattas av vägrätt. Problemet uppmärksammades i samband med utredningen av ledningsrättslagen (SOU 2004:7) men regeringen valde att inte vidta några åtgärder för att komma tillrätta med problemet.

Redan 2003 konstaterades att väghållningsmyndigheten Trafikverket saknade bemyndigande för att meddela de villkor som föreskrevs i tillståndsbeslut enligt väglagen. Trafikverkets möjlighet att meddela föreskrifter är begränsad till vad som följer av 44 § andra stycket väglagen. I stället för att vända sig till regeringen och begära en utvidgad föreskriftsrätt genom lagändring tog Trafikverket fram det civilrättsliga avtalet ABSF09. Avtalet innehåller villkor som bland annat ger Trafikverket rätt att kräva att ledningsägaren flyttar ledningar samt villkor om en kostnadsfördelning för olika drift – och underhållsåtgärder. För att Trafikverket – i egenskap av väghållningsmyndighet – ska handlägga och fatta förvaltningsrättsliga beslut enligt 44 § väglagen begär myndigheten – i egenskap av vägrättsinne-

havare – att ledningsägare ska ingå avtalet. Konsekvenserna av att Trafikverket hanterar villkor för ledningsrätt genom ett civilrättsligt avtal är att Trafikverket ensidigt kan diktera och ändra villkoren, att Trafikverket ställer villkor utöver vad som är möjligt genom föreskriftsrätten enligt 44 § andra stycket väglagen samt att villkoren inte kan överklagas. Ledningsägare kan inte avstå från att teckna avtalet eftersom det skulle innebära att ledningsägaren inte gavs rätt att tillträda vägområdet, vilket skulle förhindra all nyförläggning längs statliga vägnätet och förhindra underhåll av redan existerande ledningar. Villkoren kan inte överklagas i samband med ett enskilt tillståndsbeslut eftersom de i praxis inte ansetts omfattas av det förvaltningsrättsliga beslutet som Trafikverket fattar enligt väglagen. År 2009 försökte Telia få en prövning av saken genom att överklaga ett antal beslut, som visserligen beviljats, men villkorats av att avtalet ABSF09 skulle accepteras. Telia menade att avtalsvillkoren var så pass oskäligen att besluten inte kunde anses utgöra gynnande beslut. Överklagandena avvisades dock eftersom besluten inte ansågs ha gått Telia emot. Enligt IT&Telekomföretagen går det att argumentera för att denna situation (att villkoren inte kan överklagas) står i strid med artikel 31 i direktivet om rätten att kunna överklaga. Med tanke på de stora investeringar som nätägarna gör för att bygga ut fibernät är denna rättsosäkerhet oacceptabel.

IT&Telekomföretagen ifrågasätter inte att Trafikverket behöver ha möjlighet att ställa krav på bl.a. hur förläggning ska ske, säkerhetsåtgärder och villkor för flytt av ledningar. IT&Telekomföretagen anser dock att sådana krav måste tas fram under ordnade former och inom ramar som Sveriges riksdag beslutar om. Exempel på ramar som rimligen borde beslutas av riksdagen är processen för att ta fram villkoren, hänsyn som måste tas när villkoren utformas (t.ex. att villkor inte får stå i strid mot krav enligt lagen om elektronisk kommunikation) samt grunden för eventuella avgifter. Det måste också finnas möjlighet till rättslig prövning om Trafikverket inte följer reglerna så att marknadens aktörer får förutsägbarhet och rättssäkerhet. Fiber är en samhällskritisk infrastruktur där kunder ställer krav på tillgänglighet och alla fiberägare måste även leva upp till robusthetskrav enligt lagen om elektronisk kommunikation. Längs vägnätet har inte bara accessnät för anslutning av bredbandskunder förlagts utan även stomnät. Avbrott på stomnätsförbindelser kan äventyra stora delar av den digitala infrastrukturen. Hanteringen av fiber i vägområdet måste vara förutsägbar och rättssäker. Detta är en angelägenhet för den fortsatta digitaliseringen av Sverige.

## 17.6 Informationskrav i samband med avtal

IT&Telekomföretagen delar promemorians uppfattning att de nya kraven på information i samband med avtal är omfattande och mycket detaljerade. Det föreligger risk att ytterligare informationskrav i form av avtalsdokument (se direktivets artikel 102 och förslag till ny LEK 7:2 och 7:5) leder till att konsumenter får ännu svårare att navigera i och ta till sig avtalsvillkoren.

Med det sagt ser vi en risk att det nuvarande förslaget avseende den information som ska lämnas innan avtal ingås är för otydligt och riskerar att leda till onödiga tillämpningsproblem. Det bör på nytt övervägas om direktivets krav på avtalsunderlagets innehåll och form ändå inte bör framgå direkt av den nya lagen, om dessa krav ska tillämpas före annan lagstiftning såsom lagen (2005:59) om distansavtal och avtal utanför affärslokaler (LODA). För avtal som ingås på distans föreskriver 2:3 LODA t. ex. att informationen enligt 2:2 kan lämnas på ett sätt som är anpassat till det medel för distanskommunikation som används, vilket i dagsläget betyder att informationen får ges muntligen under telefonsamtalet när avtalet ingås per telefon.<sup>1</sup> Om det sedermera i föreskrifter ställs andra formkrav enligt direktivets art 102, d.v.s. att informationen som huvudregel ska tillhandahållas på varaktigt medium alternativt nedladdningsbart dokument, synes det föreligga risk för tolkningssvårigheter.

Om sammanfattningen inte kan tillhandahållas innan avtalet ingår, ska avtalet enligt förslaget till ny LEK 7:2 träda ikraft först när konsumenten har "bekräftat sitt samtycke" efter att ha mottagit sammanfattningen av avtalet. Om en sådan bekräftelse utesluter avtalsingående genom konkludent handlande måste detta klargöras. Detta eftersom avtalet annars inte anses ha trätt ikraft. Det är även viktigt för att kunna bedöma när ångerfristen börjar löpa.

Nuvarande förslag till mall för sammanfattningen innehåller krav på information om maxhastighet för mobila internetanslutningstjänster. Även om den svenska lagstiftaren kanske har begränsade möjligheter att påverka vad sammanfattningen ska innehålla, är det viktigt att här lyfta det arbete som gjordes på nationell nivå under 2013-14, dels i syfte att förbättra transparensen i avtalen,<sup>2</sup> dels för att ge konsumenter en rimlig förväntan på tjänsterna vid marknadsföring av täckning och hastighet för mobila tjänster.<sup>3</sup> Mot den bakgrunden finns problem med att nu kräva att tillhandahållarna ger information om maxhastigheter för mobila tjänster i sammanfattningen, eftersom det riskerar att leda till orimliga förväntningar på tjänsterna. Det måste i vart fall anses berättigat att ange ett intervall för normal hastighet i anslutning därtill, samt att angivna hastigheter endast är en uppskattning av förväntade hastigheter utan att utgöra

---

<sup>1</sup> Proposition 2013/14:15, "Gemensamt konsumentskydd i EU", s. 83

<sup>2</sup> PTSFS 2013:3

<sup>3</sup> BÖ 2014:02, "Överenskommelse om marknadsföring av täckning för mobila tjänster" (Dnr 2014/315).

någon garanti. Detta eftersom tillhandahållare av mobila tjänster inte kan kontrollera alla de faktorer som kan spela in för såväl täckning som hastighet.

### 17.12 *Paketerbjudanden*

IT&Telekomföretagen anser att det finns behov av förtydliganden av vad som avses med begreppen "paketerbjudanden", "andra tjänster", "säljs [...] tillsammans med" enligt förslaget till ny LEK 7:24, samt "del av paketet" enligt förslag till ny LEK 7:25, eftersom vissa slutanvändarrättigheter enligt den nya lagen ska gälla "alla delar" av paketet. Exempelvis gäller detta skyldigheten att tillhandhålla en sammanfattning enligt förslaget till ny LEK 7:2, och där bristande uppfyllelse kan leda till sanktioner. Lagreglerna måste mot den bakgrunden vara glasklara.

Det förefaller orimligt att köp som inte riskerar att leda till inlåsnings effekter avseende elektroniska kommunikationstjänster ska träffas av bestämmelsen om rätt till uppsägning av alla delar av paketet enligt förslag till ny LEK 7:25. Det krävs förtydliganden som klargör en tillämpning i linje därmed. Avtal om tilläggstjänster som ingås separat exempelvis, som inte typiskt sett påverkat kundens val av huvudtjänsten, bör inte anses utgöra något paket. Inte heller när operatörer säljer tjänster som inte är kopplade till elektroniska kommunikationstjänster, t.ex. en försäkring avseende terminalen. Det vore orimligt om en försäkringsgivares beslut att stänga ner en försäkringslösning, ska leda till att en kund kan säga upp ett helt paket hos tillhandahållaren av elektroniska kommunikationstjänster.

### 18.2 *Kontroll av säkerhetsarbetet*

Enligt förslaget (8 kap. 4 § ) ska PTS få förplikta den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst att på egen bekostnad låta ett oberoende organ utföra en säkerhetsgranskning av hela eller delar av verksamheten och att redovisa resultatet av granskningen för tillsynsmyndigheten.

Av direktivets artikel 42.2b framgår att operatörer ska "underkastar sig en säkerhetsgranskning som utförs av ett kvalificerat oberoende organ eller en behörig myndighet". Av regeringens motivering framgår att "avsikten är alltså inte att säkerhetsgranskningar ska åläggas regelmässigt så att tillsynsmyndigheten använder konsulter som ersättning för förmågor som bör finnas inom myndigheten". Men det framgår inte varför (vissa) säkerhetsgranskningar ska hanteras på annat sätt än annan tillsyn av PTS.

Direktivets bestämmelse om oberoende säkerhetsgranskning motsvarar nuvarande bestämmelsen i ramdirektivet artikel 13b 2. Vid det ställningstagande

som gjordes vid implementeringen av ramdirektivet i svensk lag konstaterade utredaren (SOU 2010:19 s 230) att

*”tillsynsmyndigheten redan har en möjlighet att själva utföra säkerhetsgranskning av aktören, så länge säkerhetsgranskningen utgör en kontroll över att lagens krav om vidtagna säkerhetsåtgärder är uppfyllda.../... Den säkerhetsgranskning som avses i artikel 13b torde endast kunna avse en kontroll att aktören uppnår de krav kring säkerhet som ställs enligt lagen, och specifikt dem som ställs i enlighet med ramdirektivets artikel 13a. Kraven i ramdirektivets artikel 13b i fråga om att företag ska kunna underkasta sig en säkerhetsgranskning uppfylls därför genom de ändringar av LEK som inför direktivets säkerhetskrav. Slutligen anges också i artikel 13b.2 b i ramdirektivet att säkerhetsgranskningen ska bekostas av aktören. Eftersom säkerhetsgranskningen i svensk lagstiftning ska utföras genom sedvanliga tillsynsåtgärder är det mindre lämpligt att kostnaden för tillsyn av ett viss enskilt företag direkt ska bekostas i särskild ordning av det företaget. En stor del av PTS tillsynsverksamhet finansieras redan av avgifter som betalas av de företag som anges i artikel 13b.2 i ramdirektivet. Därmed uppfylls finansieringskravet enligt direktivet i Sverige.”*  
(vår understrykning.)

Mot bakgrund av ovan ställningstagande kom bestämmelsen inte att införas i svensk lag (prop 2010/11:115 s 125 ff).

IT&Telekomföretagen tycker det saknas skäl att nu göra annan bedömning i denna fråga än den som utredaren gjorde i SOU 2010:19. Vi instämmer i slutsatsen att det är mindre lämpligt att operatörer, utöver de avgifter som de redan betalar till PTS, som bl.a. är avsett att täcka myndighetens kostnader har för tillsyn, även skulle få stå för kostnaden för extern revision som myndigheten, inom ramen för sitt tillsynsarbete, förpliktigar operatören att genomgå.

Skulle lagstiftaren ändå anse att en sådan lösning bör införas, anser IT&Telekomföretagen att det behöver formuleras strikta kriterier och begränsningar för under vilka förhållanden som myndigheten kan fatta sådana beslut. Dessutom behöver en modell tas fram för hur kostnaderna ska fördelas. Ett närliggande exempel är inom PTS marknads kontroll där företag endast står kontrollkostnaden i de fall där en vara konstaterats inte uppfylla de tekniska krav som lagen ställer. Det framstår för IT&Telekomföretagen som orimligt att en operatör, vilken vid en revision befinner sig ha ett fullgott säkerhetsarbete, skulle behöva stå kostnaden för en sådan granskning.

### *19.1 Företags skyldighet att lämna uppgifter*

Jämte vissa tillägg och språkliga justeringar i utformningen av uppgiftsskyldigheten [i PM 9 kap 1 § jfr LEK 8 kap 1 §] införs också en bestämmelse att tillhandahållaren ska på begäran tillhandahålla PTS uppgifter och handlingar som

behövs för genomförande av geografiska kartläggningar av bredbandsutbyggnad, 9 kap 1 § p 8.

Med denna nya bestämmelse torde också följa att säkerhetskänslig information i än större utsträckning kommer att begäras ut av tillsynsmyndigheten. När det gäller t.ex. geografiska utplaceringar och utbyggnad av infrastruktur kan sådan information utgöra s.k. säkerhetsskyddsklassificerade uppgifter och kan därigenom komma att omfattas av bestämmelserna i säkerhetsskyddslagen (2018:585), SSKL. För att leva upp till SSKL ska den som bedriver säkerhetskänslig verksamhet förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, m.m. I detta fall gäller det inte skada för enskild verksamhet utan skada på Sveriges säkerhet, SSKL 1 kap 1 §. Av SSKLs regelverk följer också ett krav på att teckna säkerhetsskyddsavtal om uppgifter omfattas av en viss säkerhetsskyddsklass för att säkerställa att mottagaren behandlar säkerhetsskyddsklassificerade uppgifter i enlighet med lagen.

PTS har mycket stora befogenheter att inhämta uppgifter från tillhandahållarna för att utföra sina uppdrag enligt LEK, bl.a. att inhämta statistik för publicering i rapporter och inhämtning av uppgifter för marknadsanalyser och SMP-beslut. Den information som inhämtas omfattas normalt av offentlighetsprincipen. PTS har dock möjlighet att med stöd av främst 30 kap 23 § eller 18 kap 8 § i offentlighets- och sekretesslagen (2009:400), 9 § offentlighets- och sekretessförordningen (2009:641) och punkten 99 i bilagan till offentlighets- och sekretessförordningen besluta att inkomna uppgifter som av PTS bedöms vara affärsmässigt känsliga inte ska lämnas ut till den som begär det. Av bestämmelserna framgår dock att uppgifter avseende affärs- eller driftsförhållanden presumeras vara offentliga, dvs. utgångspunkten är att uppgifterna inte omfattas av sekretess om det inte kan antas att den enskilde lider skada om uppgifterna lämnas ut. De uppgifter som omfattas av sekretess som anges i nämnda förordning/bilagan avser utredningar, tillståndsgivning och tillsyn samt ärenden om statligt stöd för att genomföra åtgärder för driftsäkra och robusta elektroniska kommunikationer. Det går inte att utläsa att den förordningen ger något stöd för sekretess avseende genomförandet av geografiska kartläggningar av bredbandsutbyggnad.

Det saknas en analys i promemorian av hur dessa regelverk ska tillämpas samt hur tillhandahållarna som omfattas av kravet på säkerhetsskydd enligt säkerhetsskyddslagen ska förhålla sig till PTS begäran om utlämnande av uppgifter.

Ytterligare så framgår det av EU-direktivet art 20.1 och 21.1 att varje begäran om information ska stå i proportion till uppgiftens utförande och innehålla en [saklig] motivering. Detta krav har inte införts i promemorian. En sådan förklaring är viktig för att tillhandahållarna ska kunna ta tillvara sin rätt att få reda på i vilket syfte informationen ska tillhandahållas och hur den ska användas. IT&Telekomföretagen anser att förslaget bör kompletteras med en sådan bestämmelse som följer av direktivet.

## 21 Sanktionsavgifter

Regeringen föreslår på PTS uppmaning att sanktionsavgifter ska införas. I LEK finns redan idag möjlighet för PTS att meddela förelägganden eller förbud. Sådana beslut får förenas med vite. Enligt PTS har sanktionssystemet i LEK inte i alla delar varit tillräckligt effektivt och myndigheten har därför föreslagit att ett sanktionsavgiftssystem införs. Stöd för detta finns i artikel 29.1 i EU-direktivet. IT&Telekomföretagen ifrågasätter dock om det finns behov av sanktionsavgifter och om det är ett effektivt sätt att uppnå regelefterlevnad och vill framföra följande.

Förslaget om införande av sanktionsavgifter aktualiserar en rad frågor, varav en första är om det över huvud taget finns behov av ytterligare sanktionsåtgärder? År 2009 ändrades underliggande direktivbestämmelser så att frågan om införande av sanktionsavgifter i LEK aktualiserades. Lagstiftaren bedömde emellertid i lagstiftningsärendet år 2011 att möjligheterna att meddela förelägganden och förbud om rättelse vid vite hade varit effektiva för att uppnå syftet med efterlevnad av lagens bestämmelser.<sup>4</sup> Det saknades därför anledning att överväga några andra åtgärder än dessa. I samma lagstiftningsärende effektiviserades också möjligheten att meddela föreläggande eller förbud, genom att kravet på att tillsynsobjektet fått en underrättelse och inte rättat sig efter vad som står i den innan sanktionerna får tillämpas tog bort.<sup>5</sup> Således kan föreläggande och förbud meddelas redan i samband med att myndigheten underrättar om en påstådd överträdelse av LEK, och då med krav på omedelbar rättelse i allvarliga fall. Sanktionsmöjligheterna får därmed sägas vara både omedelbara, direktverkande och avskräckande och då kanske särskilt åtgärderna att återkalla tillstånd eller besluta om upphörande av verksamhet. Avseende nummerportering kan dessutom skadestånd utgå. IT&Telekomföretagen ifrågasätter om dagens behovsbild, jämfört med bedömningen från 2011, är tillräckligt nyanserad och om PTS verkligen uttömt de sanktionsåtgärder som finns i lagen idag vid handläggningen av sina tillsynsärenden.

Om sanktionsavgifter trots allt ska införas, anser IT&Telekomföretagen att de materiella rättsregler till vilken sanktionsavgiften kopplas måste vara så pass klara och tydliga att det inte kan råda något som helst tvivel för tillhandahållarna om vad kravet innebär och heller inte om det är uppfyllt eller ej. Flera av reglerna som omfattas av 11 kap. 1 § nya LEK är emellertid enligt vår uppfattning varken enkla att tillämpa eller tydliga och förutsägbara, varför det enligt vår uppfattning inte bör införas sanktionsavgifter i nuläget. Som illustration av detta kan t.ex. följande nämnas.

- **Krav att vidta åtgärder för att hantera risker som hotar säkerheten i nät och tjänster:** Kravet att vidta s.k. skyddsåtgärder för att ha robusta och säkra nät och tjänster är inte enkelt att tillämpa, då det inte är fråga om

---

<sup>4</sup> Ds 2010:19 s. 260 f.

<sup>5</sup> Prop. 2010/11:115 s. 140 och 185.



att avgöra om åtgärd vidtagits eller ej utan att bedöma om de åtgärder som vidtagits ”på ett lämpligt sätt hanterar de risker som hotar säkerheten”. Bedömningen beror bl.a. av den riskanalys som genomförts (riskbedömning) och ev. incidenter som inträffat. Även i förarbetena till NIS-lagen konstateras att kraven på vidtagande av skyddsåtgärder och incidenthantering är svåra att bedöma.<sup>6</sup>

- **Krav på att bedriva verksamheten så att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation kan ske:** Kravet på s.k. anpassningsskyldighet inbegriper flera olika delar rörande verkställighet av hemlig avlyssning och övervakning, bl.a. hur tillhandahållare med främst tekniska hjälpmedel ska anpassa sin verksamhet för att möjliggöra verkställighet samt frågor om skyndsamt handläggning. Frågorna är bedömningsfrågor som torde vara relativt komplicerade att avgöra vid en tillsyn, då de i stor utsträckning beror av tillhandahållarnas individuella förutsättningar; de kan definitivt inte besvaras med ett ”ja” eller ”nej”. Att anpassningsskyldighet enligt 6 kap. 19 § LEK, som föreslås flyttas över oförändrad till nya LEK, anses som oklar samt att dess tillämpningsområde är otydligt i förhållande till andra regler om utlämnade av uppgifter till Polisen är känt. Av detta skäl har också regeringen nyligen tillsatt en utredning för att förtydliga bl.a. ovan nämnda verkställighetsfrågor. Att till en sådan materiell regel då koppla sanktionsavgifter vid bristande efterlevnad framstår som både olämpligt och oproportionerligt.

Det är alltså vår uppfattning att förslaget om sanktionsavgifter måste omarbetas för att åstadkomma tydlighet och förutsägbarhet om regeringen väljer att gå vidare med.

Vidare bör beslut om sanktionsavgift inte vara strikt, så att avgift alltid ”ska” utgå vid konstaterad överträdelse, utan istället bör vara fakultativt. PTS ska alltså ha möjlighet att använda en sådan sanktion när det är särskilt befogat. För exempel på sådana fakultativa regler se t.ex. lagen (2004:297) om bank- och finansieringsrörelse 15 kap 7 § i, försäkringsrörelselag (2010:2043) 18 kap 16 § och lag (2007:528) om värdepappersmarknaden 25 kap 8 §. I denna del kan fråga uppstå om lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) som föreskriver sanktionsavgifter bör användas som förlaga? Det finns inga krav i NIS-lagen som liknar skyddsreglerna om slutanvändares rättigheter i 5 kap. LEK eller skyddsreglerna om integritet i 6 kap LEK. Vidare anförts i förarbetena till NIS-lagen att sanktionsavgifterna i den lagen ska bygga på strikt ansvar eftersom det är flera olika tillsynsmyndigheter som ska tillämpa

---

<sup>6</sup> Det anförts att krav om att vidta tekniska och organisatoriska åtgärder och incidenthantering är svåra att bedöma underlåtenhet av, bl.a. eftersom skyldigheten att vidta skyddsåtgärder kopplar till den risk som hotar säkerheten, se prop. 2017/18:205 s. 69.

reglerna på samma sätt.<sup>7</sup> Detta argument är inte relevant för LEK, varför strikt ansvar inte behöver vara nödvändigt i denna lag.

Det saknas i PM:an tydliga ställningstagandet till och bedömningen av om sanktioner överhuvudtaget ska utdömas. I 11 kap. 2 § nya LEK föreslås bara vissa kriterier som ska beaktas vid fastställande av beloppets storlek samt kriterier för vad som kan jämka sanktionen i vissa undantagsfall. Det förefaller anmärkningsvärt att, vid ett strikt ansvar för sanktioner på betydande belopp, den beslutande myndigheten inte enligt lag måste ta hänsyn till och beakta vissa omständigheter som i det enskilda fallet bör leda till att sanktion inte ska meddelas. Som jämförelse anger t.ex. dataskyddsförordningen (GDPR) vissa hänsyn som ska beaktas av tillsynsmyndigheten för bedömning av om sanktion ska påföras eller inte (art 83.2 GDPR).

Vad gäller beloppens storlek saknas alltså närmare bestämmelser om hur överträdelser ska inplaceras på den föreslagna skalan. Till skillnad från andra rättsområden saknas här direktiv till PTS om hur beloppen bör bestämmas. Den föreslagna lagstiftningen ger därmed endast i viss utsträckning en förutsägbarhet. Om man gör en jämförelse med den miljöstraffavgift som regeringen själv hänvisar till, så anges exempelvis i 30 kap. 1 § miljöbalken (1998:808) visserligen att miljöstraffavgiften ska uppgå till minst 1 000 kronor och högst 1 000 000 kronor. Men dessutom anges det att, när avgiftens storlek bestäms, så ska hänsyn tas till överträdelsens allvar och betydelsen av den bestämmelse som överträdelsen avser. Vilket belopp som en viss överträdelse riskerar att medföra förtydligas dessutom genom bestämmelser i förordning (2012:259) om miljöstraffavgifter. Om regeringen väljer att införa ett straffavgiftssystem anser IT&Telekomföretagen att det behövs kompletterande regler, t.ex. i form av en förordning, som tydliggör hur beloppens storlek ska bestämmas.

--

För IT&Telekomföretagen,

My Bergdahl

Näringspolitisk expert och förbundsjurist

---

<sup>7</sup> A. a. s. 69.