Försvarsutskottets utlåtande
2012/13:FöU11

Subsidiaritetsprövning av kommissionens förslag om gemensam nät- och informationssäkerhet i unionen

Sammanfattning

Utskottet prövar i detta utlåtande kommissionens förslag om Europaparlamentets och rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och kommunikationssäkerhet i hela unionen (KOM(2013) 48).

Utskottet anser att förslaget inte i sitt nuvarande skick till alla delar är utformat så att det är förenligt med subsidiaritetsprincipen. Utskottet föreslår därför att riksdagen beslutar att lämna ett motiverat yttrande i ärendet.

Innehållsförteckning

Utskottets förslag till riksdagsbeslut

Gemensam nät- och informationssäkerhet i unionen

Riksdagen beslutar att lämna ett motiverat yttrande till Europaparlamentets, rådet och kommissionens ordförande med den lydelse som anges i bilaga 2.

Stockholm den 21 mars 2013

På försvarsutskottets vägnar

Åsa Lindestam

Följande ledamöter har deltagit i beslutet: Åsa Lindestam (S), Annicka Engblom (M), Peter Jeppsson (S), Anders Hansson (M), Kent Härstedt (S), Allan Widman (FP), Clas-Göran Carlsson (S), Staffan Danielsson (C), Anna-Lena Sörenson (S), Peter Rådberg (MP), Mikael Oscarsson (KD), Mikael Jansson (SD), Torbjörn Björlund (V), Stefan Caplan (M), Eva Sonidsson (S), Abdirizak Waberi (M) och Tobias Sjö (M).

Redogörelse för ärendet

Ärendet och dess beredning

Riksdagen har getts möjlighet att lämna ett motiverat yttrande över kommissionens förslag om Europaparlamentets och rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och kommunikationssäkerhet i hela unionen – KOM(2013) 48. Fristen för att avge ett motiverat yttrande går ut den 10 april 2013. Försvarsutskottet beslutade den 21 februari 2013 att begära information av regeringen om hur den bedömer förslagets förenlighet med subsidiaritetsprincipen. Regeringen redovisade den 6 mars 2013 sin bedömning i faktapromemoria 2012/13:FPM68.

Bakgrund

Direktivförslagets huvudsakliga innehåll

Syftet med förslaget till direktiv är att säkerställa en hög gemensam nivå av nät- och informationssäkerhet (NIS). Detta innebär att man förbättrar säkerheten för internet och de privata nät och informationssystem som behövs för att våra samhällen och ekonomier ska fungera. Detta kommer att uppnås genom att medlemsstaterna åläggs att öka sin beredskap och förbättra sitt samarbete med varandra och genom att operatörer av kritisk infrastruktur, inom områden som energi, transport, och viktiga leverantörer av informationssamhällets tjänster (t.ex. e-handelsplattformar och sociala medier), liksom offentliga förvaltningar åläggs att vidta ändamålsenliga åtgärder för att hantera säkerhetsrisker och rapportera allvarliga incidenter till de behöriga nationella myndigheterna.

Nät- och informationssäkerheten blir allt viktigare för vår ekonomi och vårt samhälle. Den är också en förutsättning när man ska skapa en tillförlitlig miljö för världshandeln med tjänster. Informationssystemen kan dock påverkas av säkerhetsincidenter som beror på t.ex. den mänskliga faktorn, naturfenomen, tekniska fel eller it-attacker. Den här typen av incidenter blir alltmer omfattande, vanlig och komplex. Bristande nät- och informationssäkerhet kan ha negativ inverkan på viktiga tjänster som är beroende av nätens och informationssystemens integritet. Detta kan hindra företag från att fungera, ge upphov till stora finansiella förluster för EU-ekonomin och få negativa konsekvenser för den samhälleliga välfärden.

Sättet att hantera nät- och informationssäkerhet i EU måste därför ändras stegvis. Lagstadgade skyldigheter krävs för att ge alla samma konkurrensförutsättningar och fylla luckor i lagstiftningen. För att åtgärda dessa problem och höja nivån på nät- och informationssäkerheten i Europeiska unionen har det föreslagna direktivet följande syften:

För det första ålägger direktivet alla medlemsstater att se till att de har en miniminivå av nationell kapacitet genom att inrätta nationella myndigheter för nät- och informationssäkerhet, inrätta incidenthanteringsorganisationer (Cert) och anta nationella strategier för nät- och informationssäkerhet och nationella samarbetsplaner för nät- och informationssäkerhet.

För det andra bör de behöriga nationella myndigheterna samarbeta inom ett nätverk som tillåter säker och effektiv samordning, inbegripet ett samordnat informationsutbyte samt upptäckt och insatser på EU-nivå. Genom detta nätverk bör medlemsstaterna utbyta information och samarbeta för att bekämpa nät- och informationssäkerhetshot och nät- och informationssäkerhetsincidenter på grundval av den europeiska planen för samarbete inom detta område.

För det tredje syftar förslaget till att utifrån ramdirektivets modell för elektronisk kommunikation säkerställa att en riskhanteringskultur utvecklas och att information utbyts mellan privat och offentlig sektor. Företag inom de specifika kritiska sektorer som anges ovan och offentliga förvaltningar kommer att åläggas att bedöma de risker som de står inför och vidta ändamålsenliga åtgärder som står i proportion till hoten för att garantera nät- och informationssäkerheten. De kommer att vara skyldiga att underrätta de behöriga myndigheterna om alla incidenter som utgör ett hot mot deras nät och informationssystem och som på ett allvarligt sätt påverkar kontinuiteten för kritiska tjänster och tillhandahållandet av varor.

En överklagandemöjlighet ska införas i frågan om beslut som fattas med anledning av de skyldigheter som framgår av direktivet. Medlemsstaterna är enligt förslaget även skyldiga att införa sanktionsmöjligheter som kan användas vid bristande efterlevnad av de nationella bestämmelser som införts för att genomföra direktivet.

Utskottets prövning

Inledning

Subsidiaritetsprincipen regleras i artikel 5 i fördraget om Europeiska unionen. Enligt denna ska unionen, på de områden där den inte har exklusiv befogenhet, vidta en åtgärd endast om och i den mån som målen för den planerade åtgärden inte i tillräcklig utsträckning kan uppnås av medlemsstaterna och därför, på grund av den planerade åtgärdens omfattning eller verkningar, bättre kan uppnås på unionsnivå.

Enligt Lissabonfördragets protokoll om tillämpningen av subsidiaritets- och proportionalitetsprinciperna ska Europeiska kommissionen, Europaparlamentet och Europeiska rådet översända sina utkast till lagstiftningsakter till de nationella parlamenten för att dessa ska kunna ta ställning till om förslaget är förenligt med subsidiaritetsprincipen. Riksdagen ska i enlighet med 10 kap. 6 § riksdagsordningen pröva om lagstiftningsakten strider mot den nyssnämnda principen.

Om det nationella parlamentet anser att förslaget inte är förenligt med den aktuella principen har det rätt att lämna ett s.k. motiverat yttrande till Europaparlamentets, rådets och kommissionens ordförande. Ett sådant yttrande ska lämnas inom åtta veckor från den dag då ett förslag finns på EU:s samtliga officiella språk.

Subsidiaritetsprincipens tillämpning i detta ärende

Kommissionens bedömning

EU-kommissionen menar att europeiska åtgärder inom nät- och informationssäkerheten kan motiveras enligt subsidiaritetsprincipen enligt följande.

Kommissionen anser att frånvaro av åtgärder på EU-nivå, på grund av nät- och informationssäkerhetens gränsöverskridande natur, skulle leda till en situation där varje medlemsstat agerar på egen hand och inte tar hänsyn till att näten och informationssystemen i EU är helt beroende av varandra. En lämplig nivå av samordning mellan medlemsstaterna skulle säkerställa att nät- och informationssäkerhetsriskerna hanteras på rätt sätt i det gränsöverskridande sammanhang där de uppstår. Olika lagstiftning om nät- och informationssäkerhet utgör ett hinder för företag som vill bedriva verksamhet i flera länder och står i vägen för globala stordriftsfördelar. Kommissionen anser vidare att skyldigheterna på EU-nivå krävs också för att säkra samma konkurrensvillkor.

Kommissionen anser att åtgärder på EU-nivå skulle öka effektiviteten i befintliga nationella strategier och underlätta utvecklingen av sådana.

Kommissionen menar att de nät- och informationssäkerhetsåtgärder som vidtas av regeringar måste vara enhetliga och samordnas för att begränsa och minimera konsekvenserna av nät- och informationssäkerhetsincidenter. Inom nätverket kommer de behöriga myndigheterna och kommissionen att samarbeta, genom ett utbyte av bästa praxis och med kontinuerligt deltagande av Enisa, för att främja ett enhetligt genomförande av direktivet i hela EU.

Kommissionen anser att ett tillvägagångssätt baserat på frivillighet hittills endast har mynnat ut i samarbete inom den minoritet av medlemsstaterna som har en hög skyddskapacitet. För att man ska kunna involvera samtliga medlemsstater måste det säkerställas att alla har en kapacitet som uppnår den nödvändiga miniminivån.

Regeringens bedömning

Regeringen anser att det som kommissionen anför kan utgöra skäl för reglering men det finns inget som motiverar varför detta måste genomföras på EU-nivå. Det finns gott om exempel på företag inom berörda sektorer som är verksamma i flera EU-länder trots skillnader i lagstiftning etc.

Regeringen menar att kommissionens motiv har låg relevans för huruvida lagstiftningsåtgärder måste ske på EU-nivå. Det är inte låg kapacitetsnivå som är huvudorsaken till bristande informationsutbyte mellan medlemsstaterna. Det är snarare en fråga om förtroende baserat på andra parametrar som är en nyckelfaktor vilket inte bör lagstiftas om. Däremot anser regeringen att det är viktigt att höja miniminivån på säkerheten inom EU. Detta kan med fördel göras genom koordinering, utbildning och utbyte av goda exempel snarare än tvingande lagstiftning. Förtroende är en av grundförutsättningarna för samarbete och informationsdelning.

Regeringen anser att det är tveksamt på vilket sätt arbetet med nationella strategier skulle bli effektivare genom lagstiftandeåtgärder på EU-nivå. Dessutom kräver effektiva nät- och informationssäkerhetsåtgärder ofta ett snabbt lokalt agerande snarare än ett EU-centraliserat samordnat agerande.

Regeringens sammanfattande bedömning är att målet med en hög gemensam nivå av nät- och informationssäkerhet i hela unionen inte uppnås med hjälp av tvingande lagstiftning på EU-nivå. Att stärka unionens gemensamma nät- och informationssäkerhet kan snarare uppnås genom icke tvingande åtgärder, samverkan mellan medlemsstaterna och ett aktivt nationellt arbete. Sådana åtgärder som beskrivs i kommissionens förslag bör vara varje medlemsstats ansvar i enlighet med subsidiaritetsprincipen.

Utskottets ställningstagande

Utskottet vill framhålla att nät- och informationssäkerheten blir allt viktigare för vår ekonomi och vårt samhälle. Den är också en förutsättning när man ska skapa en tillförlitlig miljö för världshandeln med tjänster. Informationssystemen kan dock påverkas av säkerhetsincidenter som beror på t.ex. den mänskliga faktorn, naturfenomen, tekniska fel eller it-attacker. Bristande nät- och informationssäkerhet kan ha negativ inverkan på viktiga tjänster som är beroende av nätens och informationssystemens integritet. Detta kan hindra företag från att fungera, ge upphov till stora finansiella förluster och få negativa konsekvenser för den samhälleliga välfärden.

Syftet med förslaget till direktiv är att säkerställa en hög gemensam nivå av nät- och informationssäkerhet (NIS). Detta innebär att man förbättrar säkerheten för internet och de privata nät och informationssystem som behövs för att våra samhällen och ekonomier ska fungera. Detta kommer att uppnås genom att medlemsstaterna åläggs att öka sin beredskap och förbättra sitt samarbete med varandra och genom att operatörer av kritisk infrastruktur, inom områden som energi och transport, och viktiga leverantörer av informationssamhällets tjänster (t.ex. e-handelsplattformar och sociala medier), liksom offentliga förvaltningar åläggs att vidta ändamålsenliga åtgärder för att hantera säkerhetsrisker och rapportera allvarliga incidenter till de behöriga nationella myndigheterna.

Förslaget till direktiv ålägger alla medlemsstater att se till att de har en miniminivå av nationell kapacitet genom att inrätta nationella myndigheter för nät- och informationssäkerhet, inrätta incidenthanteringsorganisationer (Cert) och anta nationella strategier för nät- och informationssäkerhet samt nationella samarbetsplaner för nät- och informationssäkerhet.

De behöriga nationella myndigheterna ska samarbeta inom ett nätverk. Genom detta nätverk ska medlemsstaterna utbyta information och samarbeta på grundval av den europeiska planen för samarbete inom detta område för att bekämpa nät- och informationssäkerhetshot och nät- och informationssäkerhetsincidenter.

Företag inom specifika kritiska sektorer och offentliga förvaltningar kommer att åläggas att bedöma de risker som de står inför och vidta ändamålsenliga åtgärder som står i proportion till hoten för att garantera nät- och informationssäkerheten. De ska vara skyldiga att underrätta de behöriga myndigheterna om alla incidenter som utgör ett hot mot deras nät och informationssystem och som på ett allvarligt sätt påverkar kontinuiteten för kritiska tjänster och tillhandahållandet av varor.

Regeringen anser att flera av de föreslagna åtgärderna på ett effektivt sätt kan bidra till ökad säkerhet på europeisk och nationell nivå. Regeringen anser emellertid att förslagen i direktivet är för omfattande, långtgående och oproportionerligt kostsamma i förhållande till vad som kan förväntas uppnås. Förslagen rör dessutom flera sektorer och nivåer i sam-

hället. En grundläggande inriktning bör vara att förslagen i direktivet genomförs utifrån de förutsättningar som finns i respektive medlemsstat. Att genomföra åtgärderna bör inte vara tvingande.

Det är inte möjligt att nu göra en komplett bild av vilka bestämmelser som redan gäller för alla dem som träffas av den reglering som kommissionen nu föreslår. En sådan inventering förutsätter ett omfattande utredningsarbete. Utgångspunkten är att det ser olika ut i respektive sektor och att inga eller få i dag har krav på sig att rapportera it-incidenter (det finns krav för teleoperatörer enligt lagen om elektronisk kommunikation att rapportera incidenter). Det kan även noteras att nya åtaganden för den kommunala sektorn innebär en inskränkning av den kommunala självstyrelsen och kan utlösa den kommunala finansieringsprincipen.

BILAGA 1

Förteckning över prövade dokument

Europeiska kommissionens förslag till Europaparlamentets och rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen, KOM(2013) 48.

BILAGA 2

Motiverat yttrande från Sveriges riksdag

Regeringen anser att flera av de föreslagna åtgärderna på ett effektivt sätt kan bidra till ökad säkerhet på europeisk och nationell nivå. Regeringen anser dock att förslagen i direktivet är för omfattande, långtgående och oproportionerligt kostsamma i förhållande till vad som kan förväntas uppnås. Förslagen rör dessutom flera sektorer och nivåer i samhället. En grundläggande inriktning bör vara att förslagen i direktivet genomförs utifrån de förutsättningar som finns i respektive medlemsstat. Att genomföra åtgärderna bör därför inte vara tvingande.

Regeringens sammanfattande bedömning är att målet med en hög gemensam nivå av nät- och informationssäkerhet i hela unionen inte uppnås med hjälp av tvingande lagstiftning på EU-nivå. Att stärka unionens gemensamma nät- och informationssäkerhet kan snarare uppnås genom icke tvingande åtgärder, samverkan mellan medlemsstaterna och ett aktivt nationellt arbete. Regeringen anser att det är tveksamt på vilket sätt arbetet med nationella strategier skulle bli effektivare genom lagstiftning på EU-nivå. Dessutom kräver effektiva nät- och informationssäkerhetsåtgärder ofta ett snabbt lokalt agerande snarare än ett EU-centraliserat samordnat agerande.

Riksdagen instämmer i regeringens bedömning. Riksdagen anser att åtgärder av det slag som föreslås i förslaget till direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i unionen bör vara varje medlemsstats eget ansvar i enlighet med subsidiaritetsprincipen. Riksdagen finner således att kommissionens förslag i KOM (2013) 48 strider mot subsidiaritetsprincipen.

Tryck: Elanders, Vällingby 2013