U 71/2020 rd

Statsrådets skrivelse om kommissionens förslag till Europaparlamentets och Rådets direktiv om motståndskraft hos kritiska enheter

I enlighet med 96 § 2 mom. i grundlagen översänds till riksdagen Europeiska kommissionens förslag till Europaparlamentets och Rådets direktiv om motståndskraft hos kritiska enheter (COM (2020) 829 final).

Helsingfors, 28 januari 2021

Inrikesminister Maria Ohisalo

Konsultativ tjänsteman Eero Kytömaa

INRIKESMINISTERIET PROMEMORIA EU/2020/1795
21.1.2021

EUROPEISKA KOMMISSIONENS FÖRSLAG TILL EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV OM MOTSTÅNDSKRAFT HOS KRITISKA ENHETER

1 Bakgrund

Kommissionen offentliggjorde den 16 december 2020 ett förslag till Europaparlamentets och Rådets direktiv om motståndskraft hos kritiska enheter (COM (2020) 829 final). Förslaget är till sin karaktär delvis ny reglering på unionsnivå. De bärande temana i utkastet till direktiv är förståelsen om hot- och störningsspektrets omfattning och det föranledda behovet att övergå från fysiska skyddsåtgärder till att säkerställa en störningsfri drift. I statsrådets skrivelse hänvisas till direktivförslaget med förkortningen CER-direktivet (Critical Entities Resilience Directive).

Enligt kommissionen är huvudsyftet med CER-direktivet att garantera att den inre marknaden fungerar i fråga om kritiska tjänster inom tillämpningsområdet för direktivet. Syftet med förslaget är att förbättra motståndskraften hos de med tanke på EU nödvändiga tjänsterna och bevara för samhället livsviktiga och ekonomiska funktioner genom fastställande av bestämda kritiska sektorer som tillhandahåller sådana tjänster.

EU har redan länge identifierat betydelsen av att skydda kritiska infrastrukturer för den europeiska verksamhetsförmågan. Redan 2006 till exempel påbörjade EU ett europeiskt program för skydd av kritisk infrastruktur (EPCIP). År 2008 trädde direktivet om kartläggning och klassificering av europeisk kritisk infrastruktur och bedömning av behoven att stärka skyddet av denna (ECI-direktivet). Detta tillämpas endast på vissa energi- och trafikinfrastrukturer i samband med vilka en störningssituation på ett avsevärt sätt påverkar två eller ett flertal medlemsländer. Till följd av direktivets begränsade tillämpningsområde har många medlemsländer genomfört sina egna åtgärder för att skydda kritiska infrastrukturer i stället för att direktivet hade styrt utvecklingen av dessa skyddsåtgärder.

Enligt kommissionen är det uppenbart att de aktuella ramarna för skydd av kritiska infrastrukturer inte är jämförbara och inte heller tillräckliga för att skydda Europas kritiska infrastruktur och tjänster i anknytning till den. Med beaktande av det ökande ömsesidiga beroendet mellan infrastrukturerna och betydelsen för handlingsförmågan på den inre marknaden beslutade kommissionen att reformera direktivet om skydd av infrastrukturer.

Kommissionen framhäver att miljön för de kritiska enheterna verkar har förändrats betydligt. För det första är riskerna och hoten som Europa möter mer pluralistiska än 2008. För det andra möter aktörerna i kritiska system, till exempel tjänsteoperatörer nya utmaningar när ny teknologi införs vilka ofta gäller systemens sårbarhet. Ny teknologi öppnar också möjligheter för fientlig statlig verksamhet som försöker utnyttja den sammanvävda infrastrukturens sårbarheter. För det tredje ökar den nya teknologin ytterligare det ömsesidiga beroendeförhållandet emellan infrastruktur- och tjänsteoperatörer vilket kan leda till en snabb utvidgning av störningar från en sektor till ena annan och eventuellt medföra betydande störningar i ett flertal medlemsstater eller på unionsnivå.

Enligt kommissionen har utmaningarna i anknytning till det ömsesidiga beroendeförhållandet mellan kritiska enheter hittills inte identifierats tillräckligt i unionens lagstiftning. Det finna enligt kommissionen ett flertal grunder för detta. För det första är infrastruktur- och tjänsteoperatörerna inte helt medvetna eller i tillräcklig utsträckning beredda på konsekvenserna av ett dynamiskt risklandskap inom sin egen bransch. Å andra sidan skiljer sig åtgärderna som fokuserar på en förbättrad krishanteringsförmåga avsevärt i medlemsländerna och i branscherna. För det tredje finns det inte en tillräcklig jämförbar bedömningsram för kritiska enheter så det uppträder betydande avvikelser i fråga om beredskap och övervakning i de enskilda medlemsstaterna. Kraven och stödet som staten erbjuder aktörerna varierar från medlemsstat till medlemsstat vilket medför hinder för den gränsöverskridande gemenskapen. Sålunda är det möjligt att rentav en enskild infrastruktur- och tjänsteoperatörens otillräckliga beredskap för att åtgärda en störning kan medföra en allvarlig risk för driften på den inre marknaden.

Kommissionen konstaterar också att förutom att den oklanderliga driften på inre marknaden äventyras så kan gränsöverskridande störningar på europeisk nivå medföra betydande negativa konsekvenser för medborgare, företag, regeringar och miljön. Kommissionen framhäver att störningar i enskilda sektorer kan påverka till exempel européernas möjligheter att resa och arbeta fritt samt till exempel att få tillgång till nödvändiga offentliga tjänster, såsom hälsovård.

Kommissionen framhäver också att störningar, till exempel omfattande elavbrott och allvarliga trafikolyckor, kan försämra känslan av säkerhet och befolkningens förtroende i infrastruktur- och tjänstesystemens driftförmåga samt i myndigheterna som i sista hand ansvarar för övervakningen av systemen och tryggande av befolkningens verksamhetsförmåga.

2 Mål och huvudsakligt innehåll

CER-direktivförslaget är en del av ett stort paket som omfattar den nya cybersäkerhetsstrategin och en uppdatering av direktivet om nätverks- och informationssystem (förslag till Europaparlamentets och rådets direktiv för att garantera en hög nivå av cybersäkerhet inom den Europeiska unionen och om upphävande av direktivet 2016/1148, NIS 2). Förslaget baserar sig på den nya säkerhetsunionstrategin 2020–2025, som kommissionen offentliggjorde den 24.7.2020, och i vilken det efterlyses ett övergripande sätt att närma sig som tar hänsyn till aktuella och framtida risker samt de ömsesidiga beroendeförhållandena mellan den fysiska och digitala infrastrukturen. Dessa åtgärder stöder också målen för EU:s program mot terrorism.

Syftet med direktivförslaget är att förbättra utbudet av nödvändiga tjänster på den inre marknaden genom att fokusera på åtgärder som både bevarar och förbättrar med tanke på samhällena kritiska operatörers motståndskraft. Åtgärderna omfattar många sektorer och strävan är att med hjälp av dem ingripa i aktuella och kommande risker i nätet och utanför det på ett systematiskt och kompletterande sätt.

Enligt kommissionen är en fungerande inre marknad beroende av tjänsterna som de kritiska enheterna producerar och som behövs för att bevara den samhälleliga och ekonomiska verksamheten. När det gäller samhällets funktionsförmåga ska de kritiska enheterna vara resilienta, det betyder att de ska kunna motsätta, hålla ut och anpassa sig och återhämta sig från störningar som de påverkas av och som kan leda till allvarliga, störningar mellan sektorerna rentav till gränsöverskridande störningar.

Enligt kommissionen är förslaget i linje med förslaget till direktiv om nätverks- och informationssystem NIS 2 och utgör en systematisk och nära synergi med åtgärderna för att nå en hög gemensam cybersäkerhetsnivå i hela unionen.

Kommissionen framhäver dessutom att förslaget till CER-direktiv återspeglar det nationella sättet att närma sig frågan i allt flera medlemsländer i vars beredskapsåtgärder det sektoriella och gränsöverskridande ömsesidiga beroendeförhållandet framhävs och i vilka krisresiliensåtgärderna endast är ett element för att förebygga och minska risker vid sidan om kontinuitetshantering och återhämtning av affärsverksamheten.

Med CER-direktivet ersätter kommissionen ECI-direktivet (2008/114EC) om skydd av kritisk infrastruktur i Europa som enligt kommissionen är föråldrat, med tanke på tillämpningsområdet för snävt och som inte längre svarar mot hoten av i dag till vilka förutom naturkatastrofer också hör bland annat statlig hybridpåverkan, hot inom inre kretsar, terrorism, pandemier och industriolyckor. Genom CER-direktivet eftersträvar kommissionen en kartläggning av hela hotspektret och skydd av digitala och fysiska infrastrukturer som en enda helhet.

Genom direktivet eftersträvas en utvidgning av metodvalet från att ha omfattat enbart skyddsåtgärder till åtgärder som utvecklas med tanke på kontinuitetshanteringen. Vid sidan om skyddsåtgärderna har bland annat riskhantering och förmågan att återhämta sig själv från störningar lyfts fram. I utkastet till direktiv identifierats förutom anknytningen till den fysiska och digitala infrastrukturen också både sektorövergripande ömsesidiga beroendeförhållanden och ömsesidiga beroendeförhållanden som överskrider medlemsländernas gränser.

I direktivförslagets tillämpningsområde ingår tio sektorer som täcker trafik, energi, banker, finansmarknader, hälsa, vatten - och avfallsvattenförsörjning, digital infrastruktur, offentliga förvaltning och rymden.

I förslaget bevaras direktivet som regleringsinstrument men som rättsgrund föreslår kommissionen FEUF artikel 114, som gäller åtgärder som anknyter till den inre marknadens genomförande och funktion. I och med ändringen av den rättsgrunden övergår man från enhälligt beslutsfattande till majoritetsbeslutsfattande. De främsta ändringarna med tanke på innehållet gäller tillämpningsområdet, identifieringen kritiska enheter och åligganden för medlemsländerna och kritiska enheter.

I direktivförslaget reformeras den nuvarande gruppen Critical Infrastructure Protection Point of Contact bestående av sakkunniga från medlemsländerna förnyas och namnet ändras till expertgruppen för kritiska enheters motståndskraft (Critical Entities Resilience Group CERG). Gruppens uppgift är att assistera kommissionen i verkställande av direktivet och kommissionens handlingsmodell för horisontella grupper (182/2011) tillämpas fortsättningsvis.

2.1 Konsekvenser för medlemsländerna

Direktivförslaget förutsätter att medlemsländerna identifierar sektoriella kritiska funktioner och namnger de kritiska enheter som tillhandahåller dessa utifrån gemensamma europeiska kriterier och en nationell riskbedömning.

Medlemsländerna förutsätts också ha en nationell strategi som stärker de kritiska enheternas motståndskraft. I strategin ska bland annat nationella mål och prioriteter definieras med beaktande av gräns- och sektorsöverskridande beroendeförhållanden; roller, uppgifter och ansvar av dem som deltar i verkställandet samt koordinering mellan de ansvariga myndigheter söm följer CER- och NIS-direktiven för att främja informationsutbytet och övervakningen.

Direktivet förutsätter att de kritiska enheterna som medlemsstaterna identifierar utarbetar egna riskbedömningar och planer för krishållbarhet. Krismotståndskrav för de kritiska enheterna gäller förebyggande av störningar, fysiskt skyddande av infrastruktur, risk- och krishanteringsarrangemang, kontinuitetshantering och säkerhetsutredningar om personal.

I direktivförslaget föreslår kommissionen att särskild övervakning riktas till strategiskt betydande enheter som producerar tjänster som gäller minst en tredjedel av medlemsländer.

Kommissionen framhäver också samarbete med partnerländerna eftersom ömsesidiga beroendeförhållanden inte slutar vid EU:s yttre gränser. I det föreslagna direktivet fastställs möjligheten för sådant samarbete till exempel för riskanalyser som utförs inom EU-området.

2.2 Förslagets förenlighet med unionens övriga politik

Det föreslagna direktivet har gränsytor för EU:s andra sektorsspecifika och mångsektoriella mål som har ställts upp bland annat för minskning av katastrofrisker och anpassning till klimatförändringen, räddningstjänst, direkta utländska investeringar, cybersäkerhet och bestämmelser om finansieringstjänster. Enligt kommissionen har den europeiska gemensamma lagstiftningsramen motiverats med en identifiering av relationerna och de ömsesidiga beroendeförhållandena mellan infrastrukturens kritiska enheter, på grund av deras gränsöverskridande karaktärs skull och för att garantera kritiska tjänster.

Med ett allmänt och samordnat sätt att närma sig strävar kommissionen efter att säkerställa att de kritiska enheterna som medlemsstaterna identifierar har kvar handlingsförmåga vid en störning. Eftersom det är fråga om horisontell lagstiftning gäller en eventuell sektorsvis lagstiftning fortfarande och direktivförslaget kompletterar den. Direktivförslaget till exempel förutsätter att nationella kraven iakttas (utarbetande av strategi och riskbedömning) men eventuella överlappande krav enligt enhet beror på den sektoriella regleringen. Ökningen av ömsesidiga beroendeförhållanden och gränsöverskridande effekter talar enligt kommissionen för en utvidgning av tillämpningsområdet för lagstiftningen. Samtidigt framhäver kommissionen vikten av samordning med den sektoriella lagstiftningen så att eventuella överlappningar kan undvikas.

I förslaget har enligt kommissionen särskilt beaktats synergierna med förslaget till direktiv NIS 2 vars mål är att stärka både unionens och medlemsstaternas nationella cybersäkerhetsnivå när det gäller sektorer och enheter som betraktas som kritiska genom att föra in riskhanteringsåtgärder vid eventuella cybersäkerhetsstörningar.

Dessutom har man enligt kommissionen i CER-direktivet beaktat gemenskapens regelverk för den inre marknaden vilken gäller finansieringstjänster och ställer omfattande krav på finansieringssammanslutningar när det gäller att hantera operativa risker och för en fortsatt affärsverksamhet. Därför skulle man tillämpa endast kraven i direktivets del II på finansieringstjänsternas sektor. Det föreslagna direktivet begränsar inte heller tillämpningen av konkurrensregler.

Tjänsternas nätverk är tätt inflätade i varandra och en enhet i en medlemsstat kan tillhandahålla tjänster i ett flertal medlemsländer eller i hela EU. Detta leder till att en störning som påverkar en operatör kan ha vittgående konsekvenser för andra sektorer och överskridande regler. En eventuell allmäneuropeisk störning förutsätter åtgärder på hela EU-nivån.

Direktivförslaget omfattar också gränssnitt med unionens civilskyddsmekanism (EU/1313/2013/EU). Civilskyddsmekanismen omfattar med tanke på direktivförslaget relevanta element (riskutvärderingar, medlemsländernas beredskap för riskhantering) men det råder

trots det skillnader mellan direktivförslagets tillämpningsområde och tillämpningsområdet för beslutet om civilskyddsmekanismen. I direktivförslaget konstateras det att det med tanke på unionens civilskyddsmekanism kan utvecklas synergier i anknytning till förebyggande och hantering av katastrofer. Enligt kommissionens konsekvensanalys är förslagen i det nya direktivet förenhetliga med förslaget till ändring av unionens civilskyddsmekanism.

I riskbedömningen enligt artikel 4 i direktivförslaget ska riskbedömningar som genomförts enligt andra relevanta bestämmelser i unionens lagstiftningen beaktas, samt risker som föranletts av beroendeförhållanden mellan vissa branscher och tillgängliga uppgifter om risksituationer. Som en beaktansvärd riskbedömning enligt EU-föreskrifterna anges en skyldighet enligt artikel 6 i beslutet om civilskyddsmekanism enligt vilken medlemsländernas ska utveckla riskbedömningar, riskhanteringsplanering och hantering av katastrofriskerna på nationell och regional nivå. I förslaget till beslut gällande reformen av civilskyddsmekanismen som nu behandlas av EU eftersträvas en förstärkning av förebyggande och beredskapsåtgärder med mål för katastrofberedskap och katastrofåtergång som bestäms på EU-nivå.

3 Granskning av direktivet artikel för artikel

Direktivets syfte, tillämpningsområde och definitioner (artiklarna1–2)

I 1 artikeln i direktivet föreskrivs om direktivets syfte och tillämpningsområde inom ramen för vilket medlemsstaterna åläggs en skyldighet att uppfylla och övervaka åtgärderna i syfte att förbättra kritiska enheters motståndskraft. Artikel 1 innehåller också beskrivningar av direktivets förhållande till den övriga unionslagstiftningen och förfarandena för utbyte av konfidentiell information inom ramen för direktivet.

Utan att begränsa tillämpningen av FEUF artikel 346 ska konfidentiella uppgifter delges kommissionen och övriga relevanta myndigheter om informationsutbytet behövs för tillämpningen av detta direktiv. I arrangemangen av utbytet av information tryggas de kritiska enheternas datasäkerhet och kommersiella intressen. I artikel 2 ingår en förteckning över definitioner som ska tillämpas.

Nationella åtgärder för förbättring av kritiska enheters motståndskraft (artiklar 3–9)

I artikel 3 konstateras att medlemsstaterna ska ta fram en nationell strategi för att stärka enheternas motståndskraft mot störningar inom 3 år efter att direktivet trädde i kraft. Artikel 3 definierar detaljerat omständigheter som ska beaktas i strategin. Strategin ska åtminstone omfatta följande delar a) strategiska mål och insatsområden för utveckling av systemens krismotståndskraft, med beaktande av gränsöverskridande och multisektionella ömsesidiga beroendeförhållanden, b) förvaltningsram för att nå strategiska mål och insatsområden, inklusive beskrivning av olika myndigheters roller och ansvar, c) beskrivningar av åtgärder för förbättring av krishållbarhet inklusive nationell riskbedömning, handlingsmodell för identifiering av kritiska enheter och stödåtgärder inriktade på dem, d) verksamhetsram för intensifiering av samordningen mellan behöriga myndigheter.

I artikel 4 konstateras att de behöriga myndigheterna ska utarbeta en förteckning över väsentliga tjänster och regelbundet genomföra en bedömning av alla relevanta risker som kan påverka tillgången till dessa väsentliga tjänster och identifieringen av kritiska enheter. I bedömningen ska bland annat beaktas observationer som lyfts fram i den nationella riskbedömningen, särskilt

med tanke på ömsesidiga beroendeförhållanden. Medlemsstaterna ska säkerställa att de väsentliga delarna av riskbedömningen delges både de kritiska nationella enheterna och kommissionen.

i artikel 5 konstateras att medlemsstaterna ska exakt ska identifiera de kritiska enheterna inom de branscher som direktivet fastställer. Artikeln bestämmer omständigheter som ska beaktas i identifieringsprocessen, till exempel att medlemsstaterna sa föra en aktuell lista över nationellt identifierade kritiske tjänster i enlighet med direktivet och därmed förbundna enheter. På samma sätt förutsätts medlemsstaterna informera enheterna om skyldigheterna som förutsätts i direktivet.

I artikel 6 åläggs medlemsstaten meddela kommissionen större störningar i den kritiska enheten. På samma sätt auktoriserar artikeln kommissionen att ge anvisningar efter att ha konsulterat den i direktivet inrättade expertgruppen för kritiska enheters motståndskraft som består av representanter för medlemsländerna.

I artikel 7 föreskrivs att medlemsstaterna ska specificera de enheter inom bank- och finansieringsbranschen och den marknads- och digitala infrastruktur som enligt den nationella bedömningen räknas som kritiska. Dessa aktörer ska också informeras om att de har identifierats som nationellt kritiska enheter. Inom de ovan nämnda branscherna är den sektorspecifika regleringen den primära styrande normen när det gäller åtärdernaör att utveckla motståndskraften.

I artikel 8 föreskrivs att namngivna behöriga myndigheter i medlemsstaterna och nationella kontaktpunkter ska ha tillräckliga resurser för att ordna bedömnings-, övervaknings- och rapporteringsverksamhet i enlighet med direktivet för organisering av det gränsöverskridande samarbetet, inklusive samarbetet som genomförs inom ramen för direktivförslaget NIS 2. Den nationella kontaktpunkten ska regelbundet rapportera sina åtgärder till kommissionen.

Artikel 9 gäller nationella åtgärder med vilka man stöder kritiska enheter som identifierats i enlighet med direktivet bland annat genom att utveckla informationsutbytet mellan myndigheterna och enheterna.

Åtgärder för utveckling av kritiska enheters motståndskraft (artiklar 10–13)

De kritiska enheterna ska regelbundet bedöma identifierade och betydande risker inom sin bransch med beaktande av den nationella riskbedömningen och andra relevanta datakällor. I artikel 11 föreskrivs om tekniska och organisatoriska åtgärder som enheterna genomfört i syfte att förbättra krishållbarheten, inklusive rapporteringsskyldigheter och rätten att utfärda författningar för verkställande som ska beviljas kommissionen. Med stöd av artikel 11(4) skulle man ge kommissionen befogenhet att använda delegerade förordningar för att ändra eller komplettera denna artikels första paragraf.

I artikel 12 föreskrivs om de kritiska enheternas rätt att begära säkerhetsutredningar om sin personal som arbetar med sensitiva uppgifter eller som man överväger att rekrytera för dessa uppgifter. Direktivets artikel 12 skulle utöka medlemsstaternas skyldigheter att överlämna uppgifter ur kriminalregister i Ecris-samarbetet (Europeiska informationssystemet för utbyte av uppgifter ur kriminalregister) i enlighet med rådets rambeslut 2009/315/RIF samt göra sökningar om tredjelandsmedborgare i Ecris-TCN-systemet (centraliserat system för identifiering av medlemsstater som innehar uppgifter om fällande domar mot tredjelandsmedborgare och statslösa personer) i enlighet med förordning 2019/816.

Artikel 13 gäller medlemsstaternas arrangemang med vilket de säkerställer att kritiska enheter utan dröjsmål underrättar den behöriga myndigheten om betydande störningssituationer eller om situationer som kan utvidgas till betydande störningssituationer. Artikeln definierar också den centraliserade kontaktpunktens verksamhet för att förmedla information till de övriga medlemsstaterna.

I artiklarna 14 och 15 föreskrivs om identifieringen av särskilt betydande europeiska kritiska enheter och om åtgärderna för att skydda dem. Artiklarna gäller enheter som identifierats som kritiska i minst en tredjedel av Europeiska unionens medlemsstater. Den medlemsstat på vars territorium enhetens verksamhet leds ansvarar för att göra de nödvändiga anmälningarna både till enheten och till kommissionen. I artikel 15 beskrivs de övervakningsarrangemang som tillämpas på särskilt kritiska enheter samt övriga åtgärder, som i huvuddrag följer de förfaranden som beskrivs i artiklarna 5 och 6 med tillägget att även kommissionen föreslås få befogenhet att utöva insyn i åtgärderna för att utveckla motståndskraften mot störningar hos en särskilt betydande enhet.

Samarbete och rapportering (artiklarna 16–17)

I artikel 16 beskrivs rollen och uppgifterna för expertgruppen för motståndskraften mot störningar hos kritiska enheter (CERG). Gruppen bildas av företrädare som medlemsstaterna och kommissionen utsett inom sex månader från direktivets ikraftträdande. Kommissionens företrädare är gruppens ordförande. Gruppens uppgift är att stödja och möjliggöra samarbete och informationsutbyte på strategisk nivå. Enligt artikeln kan kommissionen anta genomförandeakter som kommittén behandlar i enlighet med granskningsförfarandet.

I artikel 17 föreskrivs om kommissionens stödåtgärder till både medlemsstater och kritiska enheter i syfte att säkerställa att de kritiska enheterna och medlemsstaterna fullgör sina skyldigheter i enlighet med direktivet under beaktande av gränsöverskridande och tvärsektoriella störningssituationer.

Tillsyn och verkställande (artiklarna 18–19)

I artikel 18 i förslaget till direktiv konstateras medlemsstaternas ansvar och uppgift att säkerställa direktivets nationella genomförande, inklusive samarbete i de områden som avses i direktivförslaget NIS 2.

Artikel 19 i direktivförslaget förutsätter att medlemsstaterna genomför de nödvändiga arrangemangen för förordnande av sanktioner till de kritiska enheter som medlemsstaterna identifierar och som inte fullgjort de åtgärder som föreskrivs i direktivet. Medlemsstaternas uppgift är att med åtgärder i enlighet med artikel 19 säkerställa att de kritiska enheterna iakttar fullgör de åtgärder som nämns i direktivet.

Slutbestämmelser (artiklarna 20–26)

I artikel 20 i direktivet konstateras att kommissionen biträds av en kommitté i enlighet med förordning (EU) 182/2011. Artikel 21 ger kommissionen befogenhet att anta delegerade akter under de förutsättningar som föreskrivs i artikeln. I artikel 22 föreskrivs att kommissionen lämnar en berättelse till Europaparlamentet. Europaparlamentet och rådet utvärderar i vilken omfattning medlemsstaterna genomfört de nödvändiga åtgärderna för efterlevnad av direktivet.

I artikel 23 konstateras att ECI-direktivet 2008/114/EG hävs från och med datumet för CER-direktivförslagets ikraftträdande.

I artikel 24 konstateras att medlemsstaterna inom den frist som meddelas i förslaget ska anta och publicera nödvändiga lagar, förordningar och administrativa föreskrifter

och underrätta kommissionen om detta.

I artikel 25 konstateras att CER-direktivet träder i kraft den tjugonde dagen efter att den publicerats i Europeiska unionens offentliga tidning.

I artikel 26 konstateras att direktivet riktats till alla medlemsstater.

4 Förslagets rättsgrund, subsidiaritets- och proportionalitetsprincipen och förhållande till grundlagen

CER-direktivförslagets rättsgrund är FEUF artikel 114 som gäller åtgärder som anknyter till den inre marknadens genomförande och funktion. Syftet med FEUF artikel 114 är att närma lagstiftningen i medlemsstaterna när det finns sådana skillnader mellan dem som kan begränsa inre marknadens grundläggande friheter och kan på så sätt direkt påverka inre marknadens funktion.

Förslaget behandlas i Europaparlamentets och rådets medbeslutandeförfarande i normal lagstiftningsordning. Rådet beslutar om förslagets godkännande med kvalificerad majoritet. Ändring av bestämmelsegrunden för ECI-direktivets FEUF artikel 352 (f.d. artikel 308 FEG) till FEUF artikel 114 är motiverad enligt kommissionen då direktivets mål, tillämpningsområde och innehåll förändras. Avsikten har dessutom varit att göra förslaget enhetligt med direktivförslaget om nätverks- och informationssystem (NIS2).

Kommissionen betraktar direktivförslaget som förenligt med proportionalitets- och subsidiaritetsprinciperna. Kommissionen anser det motiverat att medlemsstaterna går in för ett ömsesidigt likartat angreppssätt för att förbättra motståndskraften mot kriser hos tjänster på den inre marknaden och för att reglera och övervaka verksamhet som gäller dem. Denna verksamhet överskrider ofta medlemsstaternas gränser, vilket redan nu bidrar till att skapa utmaningar för den effektiva och föregripande verksamheten i syfte att trygga den allmänna ordningen och ekonomiska verksamheten på den inre marknaden.

Gällande proportionalitetsprincipen fäster kommissionen uppmärksamhet på att efterlevnaden av direktivet i vissa fall kan kräva avsevärda investeringar. I sådana fall är dessa investeringar dock motiverade enligt kommissionen eftersom de främjar förbättringen av både den operativa och systemiska motståndskraften mot kriser. Dessutom anser kommissionen att den extra belastningen som direktivet eventuellt medför för stater, unionen och dess medborgare är motiverad och rimlig då den relateras till de eventuellt betydande kostnader som orsakas av stora störningar som äventyrar tjänster som anknyter till kritiska samhälleliga funktioner och den ekonomiska funktionsförmågan hos operatörer i enskilda medlemsstater.

De bakgrundsutredningar (säkerhetsutredningar/-prövningar) om personalen som avses i direktivförslagets artikel 12 anknyter till behandling av personuppgifter vid vilken man ska iaktta bestämmelser om skyddet av personuppgifter. Kraven på skyddet av personuppgifter innehåller bland annat dataminimeringsprincipen och kravet på proportionalitet. Kommissionen har inte

bedömt konsekvenserna för de grundläggande rättigheterna av de föreslagna specialbestämmelserna på ett mer omfattade sätt. Vid utredning av arbetstagares bakgrund ska man enligt förslaget särskilt utnyttja också kriminalregisteruppgifter som fås från andra medlemsstater genom Ecris-systemet.

Föreslagna bestämmelser om säkerhetsutredningar är betydelsefulla med tanke på 10 § i grundlagen. I enlighet med 1 mom. i grundlagen preciseras skyddet av personuppgifter i lagstiftning. Enligt grundlagsutskottets etablerade praxis begränsas lagstiftarens flexibilitet inte bara av denna bestämmelse utan också av det att skyddet av personuppgifter omfattas delvis av skyddet för privatlivet som tryggas i samma moment. Allt som allt gäller det att lagstiftaren ska trygga denna rättighet på ett sätt som kan anses acceptabelt i systemet för grundläggande rättigheter (se t.ex. GrUU 13/2016 rd, s. 3—4). Grundlagsutskottet har framhävt hot på grund av behandling av känsliga uppgifter. Utskottet anser att med stora databaser som innehåller känsliga uppgifter finns det allvarliga risker med anknytning till datasäkerhet och missbruk av information som även kan utgöra ett hot mot personens identitet (GrUU 14/2018 rd, s. 5, GrUU 13/2016 rd, s. 4, GrUU 14/2009 rd, s. 3/I). I skäl 51 i EU:s allmänna uppgiftsskyddsförordning framhävs också att speciella personuppgifter som avses i artikel 9 i förordningen och som är särskilt känsliga med tanke på grundläggande rättigheter och friheter ska tryggas särskilt noggrant eftersom sammanhanget för behandlingen av personuppgifter kan orsaka betydande risker för grundläggande rättigheter och friheter. Utskottet har på grund av detta fäst särskilt uppmärksamhet på att det finns skäl att begränsa behandling av känsliga uppgifter till det nödvändigaste genom exakta och specifika bestämmelser (GrUU 14/2018 rd, s. 5, GrUU 3/2017 rd, s. 5). Det framgår inte av kommissionens förslag om behandlingen av uppgifter som avses i den föreslagna artikeln 12 kan omfatta uppgifter som hör till specifika personuppgiftsgrupper. De kriminalregisteruppgifter som avses i föreslaget är dock konstitutionellt känsliga uppgifter. Dessa uppgifter ska enligt förslaget också utbytas mellan medlemsstaterna för utredning av arbetstagarnas bakgrund. Det är också svårt att bedöma noggrant i förslaget vilka persongrupper omfattas av utredningar. Föreslaget påverkar dock skyddet av grundläggande rättigheter, särskilt skyddet av privatlivet, på ett mer omfattande sätt än vad som framgår i förslaget. Dessutom finns det skäl att bedöma eventuella konsekvenser för näringsfriheten i enlighet 18 § i grundlagen vid den vidare behandlingen av bestämmelseförslaget.

Kommissionens förslag kan anses vara förenligt med subsidiaritets- och proportionalitetsprincipen. Trots att de argument som anfördes är inte så detaljerade kan de inte anses vara otillräckliga för bedömning av ärendet. Statsrådet anser inte att förslaget strider mot Finlands grundlag eller de konventioner om grundläggande och mänskliga rättigheter som binder Finland.

Statsrådet förhåller sig preliminärt positivt till kommissionens förslag till direktivets rättsgrund men bedömer ärendet när beredningen framskrider. Direktivförslaget kan anses anknyta till samordningen av medlemsstaternas lagstiftning och till utvecklingen av den inre marknaden samt skyddet av kritiska infrastrukturaktörer och förbättring av dessas motståndskraft mot kriser. Genom direktivförslaget säkerställs också att medlemsstaterna tillämpar ett enhetligt sätt att identifiera enheter som är kritiska för samhällena. Förslaget beaktar också nationella särdrag, såsom medlemsstatsspecifika risknivåer.

5 Konsekvenser

5.1 Konsekvenser för lagstiftningen

Direktivet sätts i verkställighet i EU:s medlemsländer med nationell lagstiftning. Av CER-direktivförslaget följer nya krav på organisering av verksamhet, såsom myndighetsuppgifter som

gäller identifieringen av kritiska enheter och övervakningen. I dagens läge har nationellt kritisk infrastruktur, kritiska sektorer eller enheter inte definierats i Finland på lagstiftningsnivå.

Genomförandet av direktivet förutsätter en mer ingående utvärdering av de nationella lagstiftningsmässiga konsekvenserna och av de skyldigheter som åläggs myndigheter och privata företag i olika branscher. Granskning och utveckling av de nationella beredskapssystemen är aktuella även på grund av effekterna av coronakrisen.

I CER-direktivförslagets tillämpningsområde ingår tio sektorer som täcker trafik, energi, banker, finansmarknader, hälsa, vatten- och avloppsvattenförsörjning, digital infrastruktur, offentliga förvaltning och rymden. Tillämpningsområdet placeras mellan samhällets livsviktiga funktioner som identifieras i samhällets säkerhetsstrategi och i den modell för övergripande säkerhet som betjänar den, de sektorer som identifierats i syfte att trygga försörjningsberedskapen och försörjningsberedskapspoolernas branscher. Bland dem finns dessutom en sektor, rymden, som för närvarande inte ingår i de funktioner eller sektorer som identifierats.

Som begrepp har försörjningsberedskap i den form som den förstås i Finland ingen motsvarighet inom EU. Med försörjningsberedskap avses i Finland att med tanke på undantagsförhållanden och allvarliga störningar som kan jämföras med undantagsförhållanden trygga de ekonomiska funktioner och därtill hörande tekniska system som är nödvändiga för befolkningens utkomst, landets näringsliv och landets försvar (lag om tryggande av försörjningsberedskap 1390/1992). Statsrådet uppställer de allmänna målen för försörjningsberedskapen. Med tanke på organiseringen av försörjningsberedskapen är det viktigt att sammanpassa direktivet och den nationella bestämmelsegrunden som gäller försörjningsberedskap.

Försörjningsberedskapen bygger på en fungerande internationell marknad, såsom EU:s inre marknad, på en konkurrenskraftig ekonomi samt på en mångsidig industriell och annan produktionsmässig bas.

Försörjningsberedskapscentralen har till uppgift att upprätthålla och utveckla landets försörjningsberedskap. Finlands system för försörjningsberedskap bygger på försörjningsberedskapsorganisationen. Den är ett nätverk som upprätthåller och utvecklar försörjningsberedskapen i Finland i enlighet med principen för partnersamarbete mellan offentliga och privata aktörer. För enheter i den privata sektorn är samarbetet definitionsmässigt frivilligt. Utöver med frivilligt partnersamarbete tryggas försörjningsberedskapen i vissa branscher även med hjälp av förpliktande bestämmelser.

Det bör också noteras att direktivet, om det träder i kraft, skulle höja den allmänna nivån av motståndskraft mot kriser i Europeiska unionens medlemsländer, inklusive sådana där det finns funktioner och beroendeförhållanden som är betydande för Finlands försörjningsberedskap.

Uppfyllandet av de skyldigheter som i direktivutkastet föreslås för medlemsstaterna bedöms förutsätta en exakt definition av behöriga myndigheter samt utveckling av nya förmågor.

Direktivförslagets tillsynsroll som gäller de kritiska enheternas riskbedömningar och handledning och övervakning av de kritiska systemens motståndskraft mot kriser kommer att kräva kompetens inom bland annat riskhantering, verksamhetsstyrning och kvalitetshantering. Kraven kan riktas också till kompetens inom datasäkerhet och dataskydd.

Identifieringen av kritiska system enligt direktivet påminner om definitionen av kritiska enheter för försörjningsberedskapen. Eftersom sektorerna i direktivförslaget dock skiljer sig märkbart

från de gällande kritiska sektorerna för försörjningsberedskapen, är det viktigt att definiera förhållandet mellan dessa två begrepp.

Direktivet medför skyldigheter för nationellt identifierade kritiska system och deras operatörer. Denna helhet måste utvärderas på nytt i samband med verkställandet av direktivet. Det är också möjligt att direktivförslaget och utvidgningar som NIS2-direktivförslaget innehåller medför sådana resurs- och andra konsekvenser också för myndigheter som bör bedömas som helhet.

De skyldigheter som direktivutkastet ställer kräver intensivt samarbete mellan myndigheter samt rapportering inom medlemsstater, mellan medlemsstater och mellan medlemsstaterna och kommissionen. Eftersom de uppgifter som rapporteras gäller samhällets säkerhet och funktionssäkerhet är det mycket viktigt att skydda dem såväl i medlemsstaterna som i kommissionen. Det är i detta skede svårt att definiera hur känsligt material som består av uppgifter om direktivets skyldigheter är, men behandlingen av det kan redan nu antas kräva särskilda åtgärder, som kommissionen bör ge mer information om.

Artikel 12 i direktivförslaget har i den föreslagna formen direkta konsekvenser för lagstiftning i Finland. Dessa riktas åtminstone till säkerhetsutredningslag (726/2014) och lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018). Skyldigheter i artikel 12 i direktivförslaget kan genomföras i enlighet med säkerhetsutredningslag förutom EU-kriminalregisteruppgifter (Art 12(2)(b)). På grund av säkerhetsutredningslagens struktur är inkludering av dessa uppgifter möjlig endast vid grundläggande säkerhetsutredningar men troligen skulle utredningar omfatta också personer som enligt lagens systematik omfattas av en begränsad säkerhetsutredning. Utvidgande av kriminalregisteruppgifter är svårt utan att de samtidigt utvidgas för alla begränsade säkerhetsutredningar.

Föreslaget kan ha konsekvenser också för annan reglering som gäller utredning av arbetstagarnas bakgrund eller pålitlighet och som i Finland omfattar säkerhetsutredningslag och reglering som gäller kriminalregister. Dessutom vid den vidare behandlingen av bestämmelseförslaget bör man bedöma dess förhållande till beredskapslag (1552/2011).

5.2 Konsekvenser för ekonomin

Det föreslagna direktivet påverkar Europeiska unionens budget. Kommissionen bedömer att de utgifter som krävs för att stöda verkställandet av förslaget uppgår till 42,973 miljoner euro under perioden 2021–2027. Det är tänkt att ca. 37,8 miljoner euro av kostnaderna ska täckas genom fonden för inre säkerhet, under rubrik 5 (återhämtningsförmåga, säkerhet och försvar) i den fleråriga budgetramen. Kommissionen bedömer att de administrativa utgifterna blir 5,2 miljoner euro, och dessa täcks under rubrik 7 (EU:s allmänna förvaltning) i den fleråriga budgetramen. De totala kostnaderna består av kostnader för följande: Kommissionens stödåtgärder, projekt och undersökningar samt rådgivningsresor ordnade av kommissionen, kommittéförfarandet för expertgruppen för motståndskraft, kommitténs regelbundna möten och övriga möten.

Enligt kommissionen kan förslagets ekonomiska konsekvenser för EU:s budget finansieras i sin helhet genom omfördelningar under den aktuella rubriken i den fleråriga budgetramen. I kommissionens förslags motiveringar (Legislative Financial Statement) presenterar man en mer detaljerad fördelning av finansiering per budgetens rubriker och år.

Fonden för inre säkerhet delas in i ett så kallat tematiskt verktyg, som administreras av kommissionen, och nationella program, som verkställs av medlemsstaterna. Kommissionen tänker använda båda verktygen i verkställandet av direktivet. Till de nationella programmen hör ett

krav på nationell finansiering (0–25 %), som man bör förbereda sig för i de nationella budgetarna. Behovet kan dock inte ännu bedömas. Nationella åtgärder som orsakas av verkställandet av direktivet kan till tillämpliga delar finansieras från fonden för inre säkerhet.

Förslaget medför sannolikt kostnader både för staten och för operatörerna av kritiska system, beroende på i vilken omfattning de frågor som läggs fram i direktivförslaget redan har beaktats i de nuvarande nationella arrangemangen. I kommissionens förslag bedöms kostnadseffekterna för nationella myndigheter eller den privata sektorn inte närmare. Exempelvis helheten kring riskbedömningar anses ge kostnadseffekter för enheter som identifierats som kritiska, vars storlek kan bedömas först i ett senare skede.

De nationella behöriga myndigheternas och kontaktpunktens uppgifter är nya och medför sannolikt ett behov av resurser, och kostnadseffekterna av detta är inte möjliga att bedöma ännu i detta skede. Om de nya uppgifter som direktivet förutsätter exempelvis skulle kunna inkluderas i befintliga myndigheters uppgifter, skulle kostnadseffekten sannolikt vara mindre än om man grundar en helt ny myndighet för verksamheten.

Dessutom föreslaget om utredning av arbetstagarnas bakgrund skulle ha resurseffekter åtminstone på Skyddspolisen och Försvarsmaktens Huvudstab som är behöriga att utföra säkerhetsutredningar i Finland. Dessutom kan förslaget ha konsekvenser för Transport- och kommunikationsverket för eventuella företagssäkerhetsutredningar.

Direktivets skyldigheter att utvidga Ecris- och Ecris-TCN-samarbetet som gäller utbyte av kriminalregisteruppgifter skulle medföra både datasystem- och personalkostnader för Rättsregistercentralen. Precisa bedömningar om kostnader för Rättsregistercentralen kan inte göras i detta skede.

6 De övriga medlemsstaternas ståndpunkter

De övriga medlemsstaternas ståndpunkter är ännu inte kända.

7 Den nationella behandlingen av förslaget och behandlingen av förslaget i Europeiska unionen

Direktivförslaget och det relaterade utkastet till statsrådets skrivelse har varit på remiss i ett skriftligt förfarande i sektionen för juridiska och inre ärenden (EU 7), konkurrenskraftssektionen (EU 8), kommunikationssektionen (EU 19) och transportsektionen (EU 22) i kommittén för EU-ärenden.

Behandlingen av kommissionens förslag i rådet har ännu inte börjat. Europaparlamentet har inte ännu inlett behandlingen av förslaget.

8 Ålands befogenheter

Enligt 18 § i självstyrelselagen för Åland (1144/1991) har landskapet lagstiftningsbehörighet i fråga om ärenden som gäller landskapets förvaltning samt myndigheter och inrättningar som är underställda den, samt med vissa begränsningar lagstiftningsbehörighet i ärenden som gäller näringsverksamhet. Enligt lagens 27 § har riket lagstiftningsbehörighet i ärenden som gäller handelssjöfart, luftfart, standardisering, statliga myndigheters organisation och verksamhet samt televerksamhet. Statsrådet bedömer i den fortsatta beredningen hur direktivförslaget påverkar Ålands ställning.

9 Statsrådets ståndpunkt

Statsrådet anser att det är centralt att utveckla EU:s motståndskraft mot kriser på ett heltäckande sätt. Det är särskilt viktigt att kritiska enheters fysiska och digitala motståndskraft mot kriser främjas starkt i EU och medlemsländerna. På så sätt förbättras också EU:s och medlemsländernas beredskap för hybridhot. Den föränderliga säkerhetsmiljön och den pågående COVID-19-pandemin har visat att EU med enhetliga metoder måste definiera och identifiera de enheter som är kritiska för samhällenas funktionsförmåga och förbättra deras motståndskraft mot kriser bland annat genom att utveckla skyddsåtgärder, bättre identifiera inbördes beroendeförhållanden mellan medlemsstaterna samt förhindra oförutsedda konsekvenser av kombination av information.

Statsrådet anser att det är viktigt att se skyddet av kritiska system som en helhet och att kontinuitetshantering och utveckling av motståndskraften mot störningar har en central roll i förbättringen av säkerheten och funktionsförmågan hos Europas kritiska fysiska och digitala infrastruktursystem. Statsrådet stöder EU:s helhetstänkande, där CER-direktivförslaget är en del av ett större paket som även omfattar den nya cybersäkerhetsstrategin och en uppdatering av direktivet om nätverks- och informationssystem.

CER-direktivförslagets mål är att förbättra verksamheten inom enheter som är livsviktiga för samhället eller tillhandahållandet av tjänster som är kritiska för upprätthållandet av den ekonomiska verksamheten på den inre marknaden, och på så sätt förbättra den inre marknadens funktion även i krislägen. Samtidigt identifieras olika enheters och sektorers inbördes beroendeförhållanden, som även kritiska enheter i Finland har kopplingar till. Statsrådet anser att förbättrad funktionssäkerhet hos kritiska tjänster på den inre marknaden även bidrar till att upprätthålla och utveckla Finlands försörjningsberedskap.

Statsrådet konstaterar att förslaget i fråga om utgångspunkter och principer skiljer sig från Finlands försörjningsberedskapssystem, men att förslaget kan anses förbättra motståndskraften mot kriser på EU-nivå och samarbetet mellan EU-länderna. När beredningen framskrider gör statsrådet en närmare bedömning av direktivförslagets konsekvenser för den nationella lagstiftningen samt förslagets konsekvenser för företagen och förvaltningen, i synnerhet i fråga om det nationella försörjningsberedskapssystemet.

CER-direktivet beaktar de kritiska systemens kopplingar till cybervärlden. Statsrådet ser det som bra att direktivförslaget är enhetligt med NIS 2-direktivförslaget, som reglerar centrala enheters cybersäkerhet och digitala infrastruktur. Båda förslagen innebär att samarbetet och informationsutbytet såväl nationellt som över gränserna kommer att öka, vilket förbättrar förståelsen för de fysiska och digitala systemens inbördes beroendeförhållanden. Man borde diskutera också geodata, platsbunden information, som är ett kritiskt element för informationssamhället och alltid kombineras med andra viktiga objektsuppgifter. Geodata skapar en fullständig bild om samhällens funktioner och deras lägen. Denna helhet bör skyddas på ett mer omfattande sätt. Statsrådet lyfter också fram att särskild uppmärksamhet bör fästas vid att hålla ägarskapet och bestämmanderätten inom unionen när det gäller kritiska enheter.

Direktivförslaget stöder medlemsländernas nationella åtgärder och myndighetsverksamhet. Det är viktigt att planera förslagets skyldigheter för både medlemsstater och kritiska enheter så att skyldigheterna inte i onödan ökar den administrativa bördan eller kostnaderna. Beslut om eventuell nationell finansiering fattas i anslutning till beredningen av planen för de offentliga finanserna och statsbudgeten. Statlig finansiering som åtgärderna förutsätter genomförs inom ramarna för statsfinanserna, vid behov genom omfördelning av anslagen.

När beredningen framskrider fäster statsrådet uppmärksamhet vid proportionaliteten i medlemsstaternas rapporteringsskyldigheter. I enlighet med fördragen ansvarar varje medlemsstat fortfarande för nationell säkerhet. Statsrådet anser att de befogenheter som delegeras till kommissionen ska vara specifika, proportionella, ändamålsenliga och väl motiverade.

Statsrådet förhåller sig preliminärt positivt till kommissionens förslag till direktivets rättsgrund men bedömer ärendet när beredningen framskrider. Direktivförslaget kan anses anknyta till samordningen av medlemsstaternas lagstiftning och till utvecklingen av den inre marknaden samt skyddet av kritiska infrastrukturaktörer och förbättring av dessas motståndskraft mot kriser. Genom direktivförslaget säkerställs också att medlemsstaterna tillämpar ett enhetligt sätt att identifiera enheter som är kritiska för samhällena. Förslaget beaktar också nationella särdrag, såsom medlemsstatsspecifika risknivåer.

Ekonomiska och lagstiftningskonsekvenser med anknytning till bakgrundsutredning som avses i direktivförslaget bör bedömas närmare. Dessutom bör de konsekvenser av detta förslag som begränsar grundläggande rättigheter bedömas noggrant under behandlingen av förslaget. Under förhandlingar är det viktigt att fästa uppmärksamhet på att den nationella lagstiftningen tillämpas på säkerhetsutredningar och det kan finnas skillnader mellan olika källregister och behöriga myndigheter som används för dem. Man ska försöka bidra till att i verkställandet finns det tillräckligt med nationell flexibilitet. Särskilt den allmänna lagen om behandling av personuppgifter som tillämpas på utredning av arbetstagarnas bakgrund och användningen av EU-kriminalregisteruppgifter borde bestämmas på nationell nivå.