**LAGRÅDET**

Utdrag ur protokoll vid sammanträde 2021-04-01

**Närvarande:** F.d. justitierådet Eskil Nord samt justitieråden Inga-Lill Askersjö och Petter Asp

**Kompletterande bestämmelser till EU:s cybersäkerhetsakt**

Enligt en lagrådsremiss den 24 mars 2021 har regeringen (Försvarsdepartementet) beslutat inhämta Lagrådets yttrande över förslag till

1. lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt,
2. lag om ändring i lagen (2021:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

Förslagen har inför Lagrådet föredragits av rättssakkunniga Karin Byström.

Förslagen föranleder följande yttrande.

Förslaget till lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt

3 §

Bestämmelsen i andra stycket i paragrafen ger upplysning om att det i en EU-förordning, som gäller krav för ackreditering och marknadskontroll i samband med saluföring av produkter, finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse. Lydelsen kommer att gälla endast under tiden 28 juni 2021−16 juli 2021. Vid sistnämnda tidpunkt kommer nämligen förordningen att byta namn genom att orden ”och marknadskontroll i samband med saluföring av produkter” utgår.

I lagrådsremissen föreslås att ändringen av ordalydelsen i bestämmelsen ska ske genom en ändringslag (förslag 2.2 i lagrådsremissen). Ändringslagen reglerar således endast ett namnbyte på en EU-förordning i en upplysningsbestämmelse. Förfarandet är i och för sig formellt korrekt, men enligt Lagrådets mening leder en sådan ordning enbart till att lagstiftningen blir svårare att överskåda. Den som ska kontrollera ändringar i lagen kommer alltid att vara tvungen att passera denna ändring, utan att den kommer att ha någon betydelse.

När det gäller en ändring av förevarande slag skulle en mer ändamålsenlig ordning kunna vara att ändringen genomförs i form av en övergångsbestämmelse till den nya lagen. I 3 § andra stycket i den nya lagen kan den bestämmelse som föreslås i ändringslagen tas in. I övergångsbestämmelserna kan därefter föreskrivas ”Bestämmelsen i 3 § andra stycket har fram till 16 juli 2021 följande lydelse” och följas av den lydelse som föreslås i 3 § andra stycket i

den nya lagen i lagrådsremissen. Ändringslagen blir härigenom överflödig.

5 §

Enligt förslagen i lagrådsremissen ska den nationella myndigheten för cybersäkerhetscertifiering ha möjlighet att med stöd av denna paragraf besluta om förelägganden mot tillverkare, leverantörer och organ för bedömning av överensstämmelse. Ett sådant föreläggande kan avse också förbud. I 8 § 6 finns en anslutande bestämmelse som anger att en sanktionsavgift ska kunna tas ut av den som överträder ett beslut om föreläggande som innebär ett förbud.

Ett föreläggande kan alltså riktas mot och en avgift tas ut av en tillverkare eller en leverantör som innehar ett certifikat och av något skäl har meddelats ett förbudsföreläggande. Det framgår emellertid inte om avsikten också är att ett föreläggande ska kunna riktas mot någon som saluför en produkt som certifierad, trots att något certifikat inte finns. Syftet med EU:s cybersäkerhetsakt är enligt artikel 1 bl.a. att säkerställa en väl fungerande inre marknad (inom den aktuella sektorn). Det är sannolikt att det syftet inte uppnås om regleringen omfattar endast leverantörer som innehar certifikat och som av någon anledning förelagts ett förbud, men inte omfattar dem som inte har något certifikat men ändå saluför en produkt som certifierad.

Enligt Lagrådets mening bör denna fråga klargöras i det fortsatta lagstiftningsarbetet.

7 §

Av bestämmelsen framgår att den nationella myndigheten för cybersäkerhetscertifiering får återkalla ett certifikat som har utfärdats av myndigheten eller, i vissa fall, av ett organ för bedömning av överensstämmelse. För att ett certifikat ska kunna återkallas fordras att ”certifikatet inte uppfyller kraven i cybersäkerhetsakten eller en europeisk ordning för cybersäkerhetscertifiering”. Vad som avses med detta, dvs. att certifikatet inte uppfyller nyss nämnda krav, framstår som mycket oklart. Någon ledning ges inte i författnings-kommentaren till bestämmelsen.

En möjlig tolkning är att bestämmelsen tar sikte på den situationen att det har tillkommit nya normer på EU-nivå som innebär nya krav vilka certifikatet inte uppfyller (jfr lagrådsremissen s. 30 och SOU 2020:58 s. 207 där det talas om att ett certifikat inte ”längre” uppfyller kraven). Det är emellertid också möjligt att förstå bestämmelsen så att den därutöver − eller i stället − tar sikte på certifikat som på något sätt varit felaktiga från början.

I tillägg är det näraliggande att fråga sig om inte ett certifikat borde kunna återkallas om det visar sig att en viss produkt, tjänst eller process som har certifierats inte uppfyller de krav som ställs för att erhålla certifikatet. Det framstår emellertid – eftersom lagtexten tar sikte på själva certifikatets överensstämmelse med vissa angivna normer – som mycket tveksamt om lagtexten kan anses omfatta ett sådant fall.

Oklarheterna går visserligen tillbaka på den bestämmelse i EU:s cybersäkerhetsakt (artikel 58.8 e) som mer eller mindre ordagrant har förts över till paragrafen. Det bör dock i den fortsatta beredningen utvecklas i författningskommentaren hur regleringen ska förstås.

Något hinder på EU-rättslig grund mot att åtminstone i huvudsak ange regeringens bedömning av vad paragrafen är avsedd att omfatta kan inte anses finnas. Tvärtom synes detta vara nödvändigt för att åstadkomma en rimlig stabilitet i rättstillämpningen.

8 §

I paragrafen regleras när den nationella myndigheten för cybersäkerhetscertifiering ska besluta att ta ut en sanktionsavgift.

*Punkt 1* gäller det fall då någon har utfärdat en EU-försäkran om överensstämmelse enligt artikel 53.2 i EU:s cybersäkerhetsakt, trots att vissa krav inte är uppfyllda. En sådan försäkran avser enligt artikeln att tillverkaren eller leverantören tar ansvar för att IKT-produkten, IKT-tjänsten eller IKT-processen överensstämmer med de krav som anges i den europeiska ordning för cybersäkerhets-certifiering som gäller för dessa. I punkt 1 anges emellertid att sanktionsavgift även ska utgå om kraven enligt EU:s cybersäkerhets-akt inte är uppfyllda. Eftersom den försäkran som avses i artikel 53.2 inte innefattar detta måste – om sanktionsavgift ska kunna utgå vid överträdelse av kraven i EU:s cybersäkerhetsakt och det inte kan anses täckas av övriga punkter i 8 § − det regleras på annat sätt. Bestämmelsens ordalydelse bör också justeras, bl.a. för att klargöra vad som avses med ”motsvarande europeiska ordning”. Lagrådet föreslår att bestämmelsen ges följande lydelse.

1. har utfärdat en EU-försäkran om överensstämmelse enligt 53.2 i EU:s cybersäkerhetsakt trots att kraven enligt den europeiska ordning som gäller för IKT-produkten, IKT-tjänsten eller IKT-processen inte är uppfyllda,

Enligt *punkt 2* ska sanktionsavgift tas ut av den som lämnat oriktiga eller ofullständiga uppgifter av betydelse vid ansökan om cybersäkerhetscertifiering enligt artikel 56.7 i EU:s cybersäkerhetsakt

och motsvarande europeisk ordning för cybersäkerhetscertifiering. I artikel 56.7 finns emellertid inte någon reglering av ansökan och det är inte heller klart om sådana bestämmelser kommer att tas in i de europeiska ordningarna. Även i denna punkt är det oklart vad som avses med ”motsvarande europeisk ordning”. Enligt Lagrådets mening saknas emellertid skäl att i aktuell bestämmelse föreskriva var ansökan om cybersäkerhetscertifiering regleras och föreslår därför att bestämmelsen ges följande lydelse.

2. har lämnat oriktiga eller ofullständiga uppgifter av betydelse vid ansökan om cybersäkerhetscertifiering,

I *punkt 5* föreslås att sanktionsavgift ska få tas ut av den som bryter mot villkor för utfärdande, bibehållande, fortsättande och förnyelse av europeiska cybersäkerhetscertifikat eller mot villkor för inskränkning eller utvidgning av tillämpningsområdet för certifiering enligt EU:s cybersäkerhetsakt eller motsvarande europeisk ordning för cybersäkerhetscertifiering. Även i denna bestämmelse, liksom i övriga punkter i paragrafen där uttrycket förekommer, är det oklart vad ”motsvarande europeisk ordning” syftar på. Men inte heller här finns skäl att ha koppling till cybersäkerhetsakten eller de europeiska ordningarna. Bestämmelsen kan därför avslutas med orden ”tillämpningsområdet för certifieringen”. Därutöver bör bestämmelsen ändras på så sätt att uppräkningen av villkor i första ledet bör sammanbindas med ”eller” i stället för ”och”.

Beträffande *punkten 6* se Lagrådets synpunkter under 5 §.

*Punkten 7* ger den nationella myndigheten möjlighet att ta ut en avgift av den som använder ett återkallat certifikat. Det framstår som klart att detta gäller gentemot den som i Sverige använder ett certifikat som återkallats av den nationella myndighet som regeringen kommer att bestämma enligt 2 §. Men det framgår inte vad som gäller i den

situationen att en tillverkare eller leverantör på den svenska marknaden använder ett certifikat som återkallats av en behörig myndighet i någon annan medlemsstat.

Certifieringen inom unionen bygger på att ett certifikat som utfärdats av en behörig myndighet inom unionen gäller inom den inre marknaden. Därmed följer också att en återkallelse som en sådan myndighet beslutar innebär att certifikatet inte längre gäller inom denna marknad.

Eftersom kravet i punkt 7 för att avgift ska kunna tas ut endast är att ett certifikat har återkallats med stöd av angiven artikel i cybersäkerhetsakten, förefaller det sannolikt att även certifikat som återkallats av ett annat lands myndighet kan omfattas av punkten, men frågan bör belysas i det fortsatta lagstiftningsarbetet.

10 och 11 §

I 10 § anges vad som särskilt ska beaktas vid bestämmande av en sanktionsavgifts storlek. Av 11 § framgår vidare att myndigheten får ”besluta att sätta ned eller avstå från att ta ut en sanktionsavgift” under vissa förutsättningar.

Det som i den sistnämnda paragrafen anges som ett ”beslut att sätta ned” avgiften är i praktiken inget annat än ett integrerat moment i den bedömning som ligger till grund för ett beslut om sanktionsavgiftens storlek enligt 10 §. Vid tillämpning av 10 § är det fråga om en bedömning där man kan beakta omständigheter som går i såväl skärpande som mildrande riktning. Vid den bedömningen måste i mildrande riktning sådana omständigheter som tas upp i 11 § − att överträdelsen är ringa och att det finns ”särskilda skäl” − kunna beaktas (jfr s. 69 i lagrådsremissen där det framgår att uppräkningen

i 10 § inte är avsedd att vara uttömmande och att myndigheten vid bestämmande av sanktionsavgiftens storlek bör beakta samtliga relevanta omständigheter). Det förhållandet att fråga inte är om ett särskilt beslut om nedsättning bör på ett bättre sätt återspeglas i lagtexten.

Motsvarande problem uppstår inte i de fall det blir aktuellt att besluta om att helt avstå från att ta ut en sanktionsavgift, eftersom det när ett sådant beslut fattas inte behövs någon bedömning av sanktionens storlek.

En möjlighet att komma till rätta med det nu beskrivna problemet är att utforma 11 § på följande sätt.

> Den nationella myndigheten för cybersäkerhetscertifiering får besluta att avstå från att ta ut en sanktionsavgift om överträdelsen är ringa, om det finns särskilda skäl eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften. Om det inte bedöms finnas skäl att avstå från att ta ut sanktionsavgift ska nu nämnda omständigheter i stället beaktas vid bestämmande av avgiftens storlek.

Om detta förslag inte kan godtas kan den variant som används i bl.a. 32 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster utgöra ett alternativ. Där används lokutionen att sanktionsavgiften ”får efterges helt eller delvis” i stället för att myndigheten ”får besluta att sätta ned eller avstå”. Men också detta alternativ är problematiskt eftersom det innebär att den omständigheten att överträdelsen är ringa (vilket otvetydigt är en omständighet som måste kunna beaktas enligt 10 §) framställs som ett skäl för att delvis efterge sanktionsavgiften, när det i själva verket är en integrerad del av bedömningen av hur stor sanktionsavgiften ska vara.

Lagrådets förslag bygger på förutsättningen att ”beslut att sätta ned” avgiften inte uteslutande tar sikte på att göra det möjligt att gå under den miniminivå, 10 000 kr, som anges i 9 §. Det framstår emellertid som osannolikt att så skulle vara fallet, men det framgår inte klart av remissen. Huruvida 11 § överhuvudtaget avses ge en möjlighet att bestämma sanktionsavgiften till ett belopp som understiger 10 000 kr framgår inte heller av remissen. Det bör klargöras i det fortsatta lagstiftningsarbetet.

12 §

Av paragrafen följer att det är möjligt att påföra en sanktionsavgift för en viss gärning även om gärningen omfattas av ett vites-föreläggande, under förutsättning att en ansökan om utdömande av vitet inte har gjorts. Bestämmelsen anger emellertid inte att påförandet av en sådan avgift hindrar en efterföljande ansökan om utdömande av vite. Som Lagrådet har noterat i sitt yttrande över lagrådsremissen Anpassningar till EU:s förordningar om medicinteknik – del 2, förekommer bestämmelser som är utformade på detta sätt i lagstiftningsfloran. Lagrådet vill dock även i detta ärende uppmärksamma den mer principiella frågan om regleringen inte borde täcka också den sist nämnda situationen.

20 §

Bestämmelsen i första stycket i paragrafen bör justeras så att det blir klart att ”enligt EU:s cybersäkerhetsakt och enligt denna lag” även syftar på beslut av den nationella myndigheten. Lagrådet föreslår att bestämmelsen ges följande lydelse.

Beslut enligt EU:s cybersäkerhetsakt och enligt denna lag av den nationella myndigheten för cybersäkerhetscertifiering eller av organ för bedömning av överensstämmelse får överklagas till allmän förvaltningsdomstol.

Förslaget till lag om ändring i lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt

Om Lagrådets förslag om en övergångsbestämmelse till 3 § lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt godtas, ska förevarande förslag till ändringslag utgå.