Kommerskollegium
National Board of Trade Sweden

Enheten för handel och tekniska regler
Heidi Lund

YTTRANDE
2021-01-21 Dnr 2020/01578-2

Försvarsdepartementet
Endast via e-post.

Kommerskollegiums synpunkter på betänkandet "EU:s cybersäkerhetsakt - kompletterande nationella bestämmelser om cybersäkerhetscertifiering"(SOU 2020:58)

Er referens: Fö2020/00954

Kommerskollegium ansvarar för frågor som rör utrikeshandel, EU:s inre marknad och handelspolitik. Kommerskollegiums uppdrag är att verka för frihandel. Det innebär att myndigheten verkar för fri rörlighet på den inre marknaden och för liberaliseringar av handeln mellan EU och omvärlden samt globalt. Myndigheten har tagit del av ovan rubricerade remiss och vill lämna följande synpunkter.

Generella synpunkter

Kommerskollegium har tagit del av betänkandets förslag med syfte att uppnå en hög nivå av cybersäkerhet och cyberresiliens inom unionen, att säkerställa en fungerande inre marknad och presentera förslag för en svensk implementering av cybersäkerhetsakten. En höjd cybersäkerhet inom EU kan främja medlemsstaterna, företagen och konsumenter. Detta förutsätter dock att de åtgärder som ska tillämpas är effektiva, ändamålsenliga för sitt syfte och kan följas upp av myndigheterna med effektiv tillsyn. Beaktat befintliga fragmenterade regelverk och starka nationella intressen är en harmonisering av cybersäkerhetsreglering komplext, inte minst för att beakta handelsberoenden som EU och dess medlemsstater har gentemot tredje land. Utöver detta är internationella handelsregelverk t.ex. i form av WTO:s avtal för tekniska handelshinder (TBT-avtalet) inte anpassat när det gäller förmågan att skapa upprättelse för de som påverkas när cyberreglering skapar tekniska handelshinder. Detta då regulativa åtgärder för förbättrad cybersäkerhet betraktas av fler länder som en fråga om nationell säkerhet. Det är dock trots allt viktigt att frågor om förenlighet med bl.a. WTO:s regelverk utreds, och särskilt för eventuella kommande nationella ordningar för cybercertifieringar. Detta saknas i betänkandet.

Box 6803, 113 86 Stockholm
Besöksadress: Drottninggatan 89
Telefon: 08-690 48 00, fax: 08-30 67 59
E-post: kommerskollegium@kommerskollegium.se www.kommerskollegium.se

Beaktat de konsekvenser som tillämpningen av cybersäkerhetsförordningen kan komma att ha, ser Kommerskollegium att den nationella strategin och samverkan inom den samma, som föreslås i betänkandet[1], är mycket viktiga svenska ställningstaganden avseende tillämpning av cybersäkerhetsakten för att beakta både förstärkt cybersäkerhet och en fungerande handel. Detta kräver dock att intressenter med djup kunskap om och förståelse både cybersäkerhet och handelsregelverk omfattas av och inkluderas i det nationella arbetet.

Cybersäkerhetsförordningens handelseffekter

Som en expertmyndighet för utrikeshandel och handelspolitik ser Kommerskollegium att de kontrollordningar som ska tillämpas för höjd cybersäkerhet för IKT (informations- och kommunikationsteknologi) bör baseras på en kravställning som tagits fram transparent i öppna fora för att noggrant beakta konsekvenserna av föreslagna åtgärder[2]. Detta förutsätter ett brett samråd och en tydlig konsekvensanalys som bekräftar att de förslagna ordningarna är effektiva för sitt syfte, också i förhållande till de investeringar som görs för att ta fram, genomföra och tillämpa dem.

Utifrån betänkandet[3] går det ännu inte att fullt ut överblicka konsekvenserna av cybersäkerhetsakten för olika aktörer innan antagandet av genomförandeakter. Detta skapar osäkerhet både när det gäller effekter för handeln och effekter avseende cybersäkerhet, särskilt då cybersäkerhetscertifiering är kostsamt och inte kan anses garantera cybersäkerhet i IKT. Som Kommerskollegium framhållit tidigare visar en cybercertifiering endast på sårbarheter i IKT vid certifieringstillfället - de faktiska cybersäkerhetsriskerna är snarare kopplade till den miljö i vilket IKT används.[4]

Kommerskollegium vill också uppmärksamma att cybersäkerhetsreglering i form av cybercertifieringskrav väl kan utgöra en utmaning utifrån ett tillsynsperspektiv och marknadskontroll. Det kan finnas risk för att en del av incidentrapportering från medlemsstater inte nödvändigtvis kommer ske transparent utifrån nationella

[1] Se sid 20-21 i betänkandet.
[2] Enligt EU:s standardiseringsförordning 1025/2012. Mandatet som Enisa och ECCG fått att självständigt föreslå certifieringsordningar skiljer sig från när europeiska certifieringskrav och kopplade tekniska specifikationer och standarder tas fram på andra områden som täcks av inre marknadslagstiftning och där KOM ger mandat till de europeiska certifieringsorganen att ta fram standarder och där medlemsstaterna är till större grad involverade i kravställningen.
[3] Se sid.21 i SOU2020:58.
[4] Se Kommerskollegium, *The Cyber Effect- The Implications of Cybersecurity Regulation on International Trade*, 2019

säkerhetsintressen, dvs. då medlemsstater kan bedöma att vissa alvarliga cyberincidenter utgör ett ”hot mot rikets säkerhet” och därför inte kan eller bör kommuniceras utåt. I praktiken kan detta leda till att en fullständig bild av cyberincidenter är svårt att få vilket också försvårar efterföljande regulativa korrigeringar. Som betänkandet också för fram saknas i dagsläget en formell författningsreglerad tillsynsmodell för cybersäkerhet vilket gör att det finns stora osäkerheter hur det omfattande ramverket ska kunna följas upp.

Ordning för bedömning av överensstämmelse och standarder samt handelspåverkan

När det gäller den föreslagna nationella ordningen för bedömning av överensstämmelse skiljer sig den från den som gäller på andra produktområden där det nationella ackrediteringsorganet (i Sverige Swedac) tar ställning till europeiska ordningar för bedömning av överensstämmelse samt bedömer kompetensen av organ för bedömning av överensstämmelse. Kommerskollegium ser att det är viktigt att den roll som Swedac idag[5] har för att värna om den inre marknaden inte går förlorad genom ny organisation, dvs. att nationell implementering av ordningar för bedömning av överensstämmelse noggrant utvärderas i förhållande till europeiska och internationella regelverk och standarder och att kontrollordningarna diskuteras i förhållande till internationella strukturer.

Så längre de europeiska certifieringsordningarna under cybersäkerhetsakten är frivilliga att tillämpa torde föreslagna ordningarna inte utgöra ett större problem från ett handelsperspektiv. Dock utgör de osäkerheter som diskuterats ovan viktiga frågor ifall det visar sig att ordningarna är ineffektiva för sitt syfte t.ex. i brist av ordentlig samordning och konsekvensanalys.

Kommerskollegium önskar vidare att det närmre hade utretts vilken myndighet eller aktörer som ska värna om handelseffekterna av cybersäkerhetsakten då de uppgifter som Försvarets Materielverk har begränsas till nationella säkerhetsintressen. Som Kommerskollegium ser det ska cybersäkerhetsakten höja cybersäkerhet för kommersiell IKT, inte endast varor inom kritisk infrastruktur, och ser därför att förslagen bör beakta internationella handel och således i första hand bygga på

[5] Förordning (2009:895) med instruktion för Styrelsen för ackreditering och teknisk kontroll, se 1-2 §.

harmonisering genom internationella standarder för att undvika handelshinder.

Som Kommerskollegium påpekat tidigare har cyberreglering även en handelspåverkan som bör tas i beaktande vid reglering och cybersäkerhetspolicies. Det framgår inte t.ex. på vilket sätt övergripande frågor om svensk handel och handelspolitik som är kopplade till informationssäkerhetsreglering och standardisering tas hand om och till vilken grad dessa frågor behandlas i Informationssäkerhetsrådet och de olika fora för privat-offentlig samverkan som nämns i betänkandet.[6] Betänkandet beskriver mer ingående endast privat-offentlig samverkan på EU-nivå inom ESCO och NIS-arbetet.

När det gäller standardiseringens roll till stöd för cybersäkerhetscertifiering beskriver yttrandet att det är Enisa som kommer ta fram den ram som standardiseringsorganisationerna har att förhålla sig till. Kommerskollegium ser att det är viktigt att dessa förslag utarbetas i samråd med berörda intressenter.

Kommerskollegium ser att de tekniska specifikationer och standarder som tas fram till stöd för förordningen kan komma att påverka såväl nationell säkerhet, andra cybersäkerhetsfrågor (så som t.ex. personlig integritet, bedrägerier) som handel. Med anledning av detta är transparenta processer och ett balanserat deltagande viktiga faktorer. Kommerskollegium ser därför att utformandet av ramar i kommande förslag inte endast lämnas till Enisa utan tydliggörs redan från början.

I skäl 76 i cybersäkerhetsförordningen anges att avvikelser från principerna i bilaga II i EU:s standardiseringsförordning[7] kan anses nödvändiga i vissa motiverade fall. Kommerskollegium ser det som viktigt att dessa undantag tillämpas restriktivt för att undvika uppkomsten av tekniska specifikationer som framtagits på ett icke-transparent vis. Kollegiet ser att utan brett samråd med medlemsstater, näringsliv och andra intressenter finns det risk för dyra[8] och ineffektiva ordningar som också kan skapa handelshinder.

Betänkandet redogör för att Enisa rekommenderar att EU:s löpande arbetsprogram för standardisering anpassas till unionens löpande arbetsprogram för europeisk cybersäkerhetscertifiering. Kommerskollegium ser att detta är positivt om det även medför att tekniska specifikationer på cybersäkerhetsområdet beaktar de principer som fastslås i standardiseringsförordningen. Detta är även viktigt för

[6] Se sid 116, SOU 2020:58.
[7] Förordning (EU) 1025/2012
[8] Se sid. 93 i betänkandet (SOU 2020:58).

eventuella standarder som tas fram till stöd för kommande genomförandeförordningar.

Handel med tredje land

När det gäller cybersäkerhetsaktens tillämplighet utgör en fungerande handel mellan EU:s inre marknad och tredje land en viktig förutsättning för interoperabilitet och resiliens. Målsättningen med cybersäkerhetsakten är att adressera fragmentering på den inre marknaden genom enhetliga kontrollordningar. Förslaget är dock inte tydligt på vilket sätt förslaget ser till att handeln av IKT mellan EU och dess medlemsstater och tredje land, och som är av avgörande vikt för mindre exportberoendeland som Sverige, ska kunna fortgå och skapa fortsatta förutsättningar för ömsesidigt erkännande av bedömning av överensstämmelse utan tekniska handelshinder.

När det gäller effekter på internationell handel förtydligar betänkandet att den europeiska cybersäkerhetscertifieringsordningen skapar en EU-intern ordning vars effekter på reglering och marknadspåverkan inte kunnat utvärderas inom ramen för betänkandet. Beaktat att cyberreglering redan idag utgör en utmaning från ett handelsperspektiv och bevisligen skapar handelshinder och genom att det är av yttersta vikt att Sveriges handel med tredje land fungerar på ett strategiskt viktigt område som IKT stödjer Kommerskollegium betänkandets ansats om att det finns många osäkerheter som bör analyseras närmare särskilt i det kommande delbetänkandet som ska ta ställning till bindande kravställning. Kommerskollegium skulle gärna velat se en mer noggrann konsekvensanalys som tar ställning till hur väl certifieringen (beaktat investeringar som kommer behöva göras både av företag och myndigheter) kan anses höja cybersäkerheten (även beaktat möjlighet att utöva tillsyn av tillämpningen) av samt på vilket sätt certifieringen kommer eventuellt påverka handel mellan Sverige och tredje land.

Den konsultation som genomfördes under sommaren 2020 av kommissionen[9] med ett förslag till cybersäkerhetcertifieringsordning presenterade inte heller någon konsekvensanalys som skulle ha möjliggjort lättillgänglig information för att bedöma de faktiska effekterna för olika intressenter och tredje land, vilket Kommerskollegium bedömer som anmärkningsvärt.

[9] https://www.enisa.europa.eu/topics/standards/Public-Consultations/

Sammanfattningsvis ser Kommerskollegium att det finns flera viktiga frågeställningar som försvårar en bedömning hur implementering av cybersäkerhetsakten kommer landa. Från ett handelsperspektiv ser myndigheten att följande frågor särskilt bör bedömas mer noggrant:

Processen för att ta fram krav (tekniska specifikationer och standarder) för cybersäkerhetscertifiering.

Med tanke på att effekterna av cybersäkerhetsaktens implementering på många områden är okända bör Sverige verka för att kommande bindande krav tas fram öppet i en transparent process enligt EU:s standardiseringsförordning. Även om denna del inte diskuteras inom ramen för detta betänkande ser Kommerskollegium att myndigheten redan i detta skede vill uppmärksamma vikten av denna fråga. Att följa kraven på en öppen kravställning ger också fler intressenter inom medlemsstater möjlighet att granska och utvärdera mer noggrant vilka effekter regleringen kommer ha på olika aktörer. Betänkandet, som baseras på nuläget, visar många osäkerheter som kan komma ha stor påverkan på Sverige både ur ett säkerhets- och handelsperspektiv utan att båda aspekter kan vägas in under implementering.

Cybersäkerhetsaktens handelseffekter och svensk implementering

Det är viktigt att de krav som ställs är förenliga med internationella regler och att de krav som ställs och kommer att ställas på medlemsstaterna kommuniceras till samhället. Det behöver därför vara tydligt vad dessa krav innebär ur ett handelsperspektiv och i förhållande till internationella handelsavtal och förhandlingar. För att säkerställa det behöver expertmyndigheter och aktörer inom svenskt näringsliv i större grad blir involverade i och få insyn i implementeringsarbetet med cybersäkerhetsakten.

WTO-rätt och anmälningsplikt för tekniska föreskrifter

Inom ramen för Kommerskollegiums uppgifter vägleder kollegiet myndigheter kring procedurer och regelverk som följer av Sveriges EU- och WTO-medlemskap eller av andra internationella överenskommelser; däribland anmälningsskyldighet enligt direktiv (EU) 2015/1535 varav Kommerskollegium vill uppmärksamma om följande.

Förenlighet med WTO-rätt

Kommerskollegium saknar en utförligare analys av förslagets förenlighet med WTO:s regelverk. Så som utredningen själva föreslår i avsnitt 14.6 rekommenderar Kommerskollegium därför att en utförligare bedömning

görs av förslagets förenlighet med WTO:s regelverk i slutbetänkandet, och särskilt för eventuella kommande nationella ordningar för cybercertifieringar.

Framförallt önskar kollegiet en bedömning av förslagets förenlighet med följande bestämmelser.

WTO:s regelverk inkluderar bl.a. WTO:s reviderade Allmänna tull- och handelsavtal (*General Agreement on Tariffs and Trade 1994*, Gatt) och WTO:s allmänna tjänstehandelsavtal (*General Agreement on Trade in Services*, Gats) som innehåller grundläggande regler för internationell handel vad gäller exempelvis import och export av varor och tjänster. Framförallt finns det bl.a. regler som gör det otillåtet att diskriminera mellan varor och tjänster från olika WTO-medlemmar (*reglerna om mest gynnad nation*),[10] eller mellan importerade och inhemskt producerade varor och tjänster (*reglerna om nationell behandling*).[11] Vidare innehåller t.ex. artikel X:3 i Gatt en bestämmelse om att varje avtalsslutande part på ett enhetligt, opartiskt och rimligt sätt ska tillämpa alla sina lagar, föreskrifter, beslut och avgöranden avseende bl.a. krav eller restriktioner på import. Om regleringen exempelvis skulle innebära att importerade varor i praktiken behandlas sämre än inhemska varor vid tillämpningen, skulle det kunna vara i strid med bestämmelsen.

Vidare efterfrågas i slutbetänkandet en bedömning av det s.k. s*äkerhetsundantaget* och dess tillämplighet.[12] Det är en undantagsbestämmelse relaterad till nationell säkerhet, som finns som en yttersta säkerhetsventil i flera av WTO-avtalen och som ger WTO-medlemmar möjlighet att vidta åtgärder som strider mot de relevanta avtalen som medlemmen anser är nödvändiga för att skydda sina *väsentliga säkerhetsintressen*. I bestämmelsen förtydligas det att den avser åtgärder som bl.a. vidtas i ”krigstid eller vid andra kritiska lägen i de internationella förbindelserna”.[13] Även om möjligheterna att vidta åtgärder som anses nödvändiga för att skydda väsentliga säkerhetsintressen synes relativt vidsträckta, rekommenderas det dock inte att de används i onödan eller missbrukas. Det bör noteras att bestämmelserna ska tillämpas i god tro**,** vilket framförallt innebär att det

[10] Artikel I i Gatt avseende varor respektive artikel II i Gats avseende tjänster.
[11] Artikel III i Gatt avseende varor respektive artikel XVII i Gats avseende tjänster.
[12] T.ex. Artikel XXI(b) i Gatt och Artikel XIV bis i Gats. I WTO:s avtal om tekniska handelshinder (TBT-avtalet) finns inget generellt säkerhetsundantag, men i avtalets preambel nämns att ingen WTO-medlem bör hindras från att vidta åtgärder som är nödvändiga för att skydda väsentliga säkerhetsintressen. I TBT-avtalet finns även vissa undantag från anmälningsskyldigheten av åtgärder vid tvingande problem relaterade till bland annat nationell säkerhet. I artikel 2.2, som stadgar att tekniska föreskrifter inte får vara mer handelshindrande än nödvändigt för att uppfylla ett legitimt syfte, nämns nationell säkerhet som ett exempel på ett legitimt syfte
[13] Artikel XXI(b) i Gatt och artikel XIV bis i Gats.

vidtagna åtgärder på ett rimligt sätt ska kunna skydda skyddsintressena.[14] Åtgärderna ska också ha vidtagits i ”krigstid eller vid andra kritiska lägen i de internationella förbindelserna”, vilket ska bedömas objektivt.[15]

Beroende på syftet med och cybersäkerhetsbehovet för en särskild typ av IKT-produkt eller IKT-tjänst skulle även andra undantagsbestämmelser i WTO-regelverket kunna vara tillämpliga för att rättfärdiga åtgärder som är i strid med regelverket. Både Gatt och Gats innehåller t.ex. undantag för åtgärder som är nödvändiga för skydd av den allmänna moralen.[16] Vidare innehåller Gats t.ex. ett undantag för åtgärder som är nödvändiga för skydd av den allmänna ordningen samt nödvändiga för att säkerställa efterlevnad av lagar eller förordningar som inte är oförenliga med bestämmelserna i avtalet i övrigt inklusive de som rör t.ex. skydd av privatlivet för enskilda personer i samband med behandling och spridning av personuppgifter och säkerhet.[17]

För tillämpning av de allmänna undantagsbestämmelserna behöver åtgärderna även uppfyller det övergripande kravet i den inledande meningen i artikel XX i Gatt respektive XIV i Gats. Den inledande meningen stadgar att åtgärderna inte får tillämpas på ett sätt som skulle innebära ett medel för godtycklig eller oberättigad diskriminering mellan länder där samma förhållanden råder eller en förtäckt inskränkning av internationell handel.

Anmälan av nationella tekniska föreskrifter

Enligt 20 § 6 p. i förordningen (1996:1515) med instruktion för Regeringskansliet ska Regeringskansliet anmäla förslag till författningar i enlighet med de procedurer som följer av Sveriges EU-medlemskap eller av andra internationella överenskommelser, bland annat enligt proceduren i anmälningsdirektivet för tekniska föreskrifter ((EU) 2015/1535).[18]

Tekniska föreskrifter enligt anmälningsdirektivet är bl.a. krav på varors egenskaper eller provning, begränsningar av varuanvändning, bestämmelser om återvinning av varor samt vissa förbudsbestämmelser.[19]

---

[14] Se panelrapporten i *Russia – Measures Concerning Traffic in Transit*, WT/DS512/7, 5 april 2019, och panelrapporten i *Saudi Arabia – Measures concerning the protection of intellectual property rights*, WT/DS567/R, 16 juni 2020.
[15] Panelrapporten i *Saudi Arabia – Measures concerning the protection of intellectual property rights*, WT/DS567/R, 16 juni 2020, para. 7.244.
[16] Artikel XX(a) i Gatt, respektive artikel XIV(a) i Gats.
[17] Artikel XIV(a) och (c)(ii) i Gats.
[18] Andra procedurer är de i enlighet med tjänstedirektivet (2006/123/EG) samt Världshandelsorganisationens (WTO) TBT-avtal (Agreement on Technical Barriers to Trade).
[19] Anmälningsdirektivet artikel 1.1(f).

Tekniska föreskrifter som genomför EU-lagstiftning behöver inte anmälas,[20] med undantag för om EU-lagstiftningen ger medlemsländerna ett stort utrymme för olika nationella lösningar och medlemsstaten väljer att utnyttja detta utrymme.[21]

I utredningen föreslås två nationella regleringar *Förslag till lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt (cybersäkerhetsakten)* och *Förslag till förordning med kompletterande bestämmelser till EU:s cybersäkerhetsakt*. Syftet med förslagen är att komplettera EU:s förordning om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten). Lagen och förordningen innehåller vissa processuella bestämmelser och bemyndiganden.

Som Kommerskollegium förstår det uppställs dock inga nationella krav direkt på produkter eller användningen av produkter. Kommerskollegium bedömer därför att de remitterade förslagen inte omfattas av anmälningsplikt enligt direktiv (EU) 2015/1535. Kommerskollegium vill dock uppmärksamma om att eventuella kommande nationella ordningar för cybersäkerhetscertifiering för IKT-produkter eller tekniska specifikationer eller andra nationella krav för IKT-produkter kan omfattas av anmälningsplikt.

Ärendet har beslutats av enhetschefen Christofer Berg efter föredragning av ämnesrådet Heidi Lund. I ärendets beredning har utredarna Emilie Eriksson, Anders Karlsson, Sophia Tannergård och Felinda Wennerberg deltagit.

Stockholm som ovan

Christofer Berg
Enhetschef

Heidi Lund
Ämnesråd

[20] 11 § förordningen om tekniska regler.
[21] EU-domstolens dom i mål C-443/98, *Unilever* (2000) p. 29.