Kommerskollegium
National Board of Trade Sweden

Enheten för handel och tekniska regler
Heidi Lund

Välj ett objekt.
2021-12-20 Dnr 2021/01453-2

Försvarsdepartementet
Endast via e-post

Remiss av SOU 2021:63 Sveriges säkerhet - behov av starkare skydd för nätverk- och informationssystem

Er referens: Fö2021/00796

Kommerskollegiums uppdrag

Kommerskollegium ansvarar för frågor som rör utrikeshandel, EU:s inre marknad och EU:s handelspolitik. Kollegiets uppdrag är att verka för frihandel. Det innebär att vi verkar för fri rörlighet på den inre marknaden och för liberaliseringar av handeln mellan EU och omvärlden samt globalt. Kommerskollegium har tagit del av förslagen i SOU 2021:63 Sveriges säkerhet – behov av starkare skydd för närverks- och informationssystem. Utredningens uppdrag innefattar att bedöma om det finns anledning att införa nationella särskilda krav på att IKT-produkter, -tjänster och -processer, som ingår i ett nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet, ska vara certifierade enligt en nationell särskilt anpassad certifieringsordning utformad för säkerhetskänslig verksamhet. I uppdraget ingår även att överväga om det finns anledning att införa krav på godkännande från en myndighet för att sådana IKT-produkter, -tjänster och -processer ska få tas i drift i viss eller all säkerhetskänslig verksamhet.

Kommerskollegium önskar lämna följande synpunkter förslaget.

Övergripande synpunkter

När det gäller EU:s strategier för ökad cybersäkerhet, och i synnerhet EU:s cybersäkerhetsakt, har Kommerskollegium tidigare lämnat synpunkter på cyberregleringens handelseffekter i vårt remissvar på delbetänkandet (SOU 2020:25)[1] som är relevanta även i förhållande till betänkandet om Sveriges säkerhet. Kommerskollegiums tidigare yttrande lyfte särskilt:

- Vikten av att beakta behovet av en öppen, transparent och behovsanpassad regelgivning då effektivitet och effekter för införlivade regler ännu är svåra att förutspå på området

[1] Dnr 2020/01578-2.

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

- Vikten av att beakta cybersäkerhetsregleringens internationella dimension med effekt på handel och förenlighet med internationella åtaganden (internationell handel med tredje land, WTO-förenlighet, och ömsesidigt erkännande av certifikat)
- Vikten av att beakta utmaningen med tillsyn över cyberreglering, där metodiken ännu inte är utvecklad
- Vikten av att beakta att cyberreglering av IKT har en handelspåverkan, inte minst för att samma IKT som används inom den privata sektorn ofta används också inom kritisk infrastruktur[2]

Kommerskollegium framhöll i sitt remissvar också att de tekniska specifikationer och standarder som tas fram till stöd för EU:s cybersäkerhetsakt kan komma att påverka såväl nationell säkerhet och andra cybersäkerhetsfrågor (så som t.ex. personlig integritet, bedrägerier) som handel. Med anledning av detta argumenterade vi för att transparenta processer och ett balanserat deltagande är viktiga faktorer.

Varureglering och handel

Kommerskollegium ser att regler för cybersäkerhet bör beaktas vid åtgärder för nationell säkerhet då dessa, som ovan noteras, kan ha märkbara handelseffekter på kommersiell IKT som kan komma att träffas av regleringarna. Kommerskollegium noterar att betänkandet till viss del beaktat konsekvenser för marknadens aktörer.

Kollegiet önskar här särskilt framhålla att cybersäkerhetscertifiering, med de kostnader som de innebär, inte bör förväxlas med säkerhet, dvs. den ska inte ses som jämförbar med den (produkt)säkerhet som certifiering av produkter levererar på andra varuområden. Detta då cybercertifiering endast visar sårbarheter vid en given tidpunkt, vilket inte är en garant för cybersäkerhet. Här behövs även andra typer av krav, beroende på bransch och produkt, i form av tekniska föreskrifter t.ex. kring mjukvaruuppdateringar och eventuellt nya verktyg för tillsyn.

Kommerskollegium stödjer därmed betänkandets ansats att marknads- och handelsrelaterade frågor behöver analyseras ytterligare innan det kan bli aktuellt med nationella ordningar på området. Man behöver särskilt beakta riskerna för regelfragmentering och sämre regler ifall man vid nationell reglering väljer att avvika från bred konsensusbaserad internationell standard, med eventuellt både konkurrensnackdelar och handelshinder som följd. Från ett handelsperspektiv är internationella eller regionala standarder alltid att föredra.

När det gäller förslaget kring nationell sammanställning över certifierade och rekommenderade IKT-produkter, -tjänster och -processer vill Kommerskollegium uppmärksamma att sådan sammanställning kan väl bli ett handelshinder och det är viktigt att den om möjligt baseras på transparenta kriterier och inte blir diskriminerande. En sådan lista kräver mycket arbete för att vara så uppdaterad att den inte skapar onödiga handelshinder. Behovet av en uppdaterad lista uppmärksammas på sidan 420 i betänkandet, men då utifrån ett behov att ha aktuella säkerhetskriterier.

---

[2] Se Kommerskollegium, *The Cyber Effect- The Implications of IT-security regulation on International Trade*, 2018

Bedömning av anmälningsskyldighet enligt direktiv (EU) 2015/1535
Som Kommerskollegium förstår det reglerar författningsförslagen i betänkandet hur verksamhetsutövare och samrådsmyndigheter ska agera i tillsynen av informationssystem, samt en ökad efterlevnad av säkerhetsskyddslagstiftningen. Kommerskollegium bedömer att författningsförslagen inte behöver anmälas enligt direktiv (EU) 2015/1535 eftersom de inte innehåller några tekniska krav på produkter eller informationssamhällets tjänster. Anmälningsplikt enligt direktivet aktualiseras således inte. Trots att de nuvarande regleringarna inte är anmälningspliktiga enligt direktivet vill kollegiet uppmärksamma Regeringskansliet om att framtida regleringar kan, vid konkreta regelförslag, komma att bli föremål för anmälningsplikt enligt direktivet samt enligt WTO:s TBT-avtal (WTO Agreement on Technical Barriers to Trade).

Bedömning av anmälningsskyldighet enligt tjänstedirektivet
Av 20 § p 6 förordningen (1996:1515) med instruktion för Regeringskansliet följer att Regeringskansliet ska anmäla förslag till författningar i enlighet med informationsförfaranden som följer av Sveriges medlemskap i EU. Ett sådant förfarande föreskrivs i tjänstedirektivet (direktiv 2006/123/EG) avseende nya eller förändrade krav på tjänsteverksamhet.

Betänkandet innehåller bl.a. förslag på att införa ett krav på att verksamhetsutövare under säkerhetsskyddslagen ska göra en särskild säkerhetsskyddsbedömning samt en lämplighetsprövning inför att ett informationssystem tas i drift. Båda dessa bedömningar ska dokumenteras. Begreppet ”verksamhetsutövare” under säkerhetsskyddslagen är såvitt kollegiet förstår ett vitt begrepp som även kan omfatta enskilda aktörer. Kollegiet kan därför inte utesluta att förslaget innebär ett nytt eller förändrat krav på tjänsteverksamhet.

Enligt tjänstedirektivet ska samtliga krav som är tillämpliga på tjänsteutövare som är etablerade i ett annat land inom EU/EES och som tillfälligt tillhandahåller tjänster i Sverige anmälas.[3] Om de föreslagna reglerna kan komma att tillämpas på företag som inte är etablerade här, utan bara bedriver tillfällig verksamhet i Sverige, gör kollegiet bedömningen att de remitterade bestämmelserna är anmälningspliktiga enligt tjänstedirektivet.

Enligt tjänstedirektivet måste krav på tjänsteverksamhet kunna motiveras av tvingande hänsyn till allmänintresset, samt vara proportionerliga i förhållande till sitt syfte.[4] En sådan motivering kommer att efterfrågas i samband med anmälan. Kollegiet svarar gärna på eventuella frågor kring anmälningsförfarandet.

Övriga synpunkter/kommentarer

När det gäller åtgärder för att stärka cybersäkerhet synes det att betänkandet har fångat upp problembilden men att åtgärderna begränsas till hjälp, stöd och

[3] Artikel 39.5 tjänstedirektivet.

[4] Artiklarna 15.3 samt 16.1 tredje stycket.

rådgivning till den offentliga verksamheten. Uppföljande verksamhet fungerar endast om aktörerna har en förutsättning att agera rätt från början. Här tolkar Kommerskollegium att det finns en stor kompetens- och resursbrist. I sammanhanget bör även outsourcing och molntjänster vara viktiga med antagandet att dessa kan vara utmanande att hantera för höjd cybersäkerhet.

Ärendet har beslutats av enhetschefen Christofer Berg efter föredragning av ämnesrådet Heidi Lund. I ärendets beredning har chefsjuristen Christian Finnerman samt utredarna Erik Alendal, Anders Karlsson, Hanna Pettersson, Charlie Olofsson och Sophia Tannergård deltagit.

Stockholm som ovan

Christofer Berg
Enhetschef

Heidi Lund
Ämnesråd