Kommerskollegium
National Board of Trade Sweden

Enheten för handel och tekniska regler
Heidi Lund

YTTRANDE
2023-02-15 Dnr 2022/01892-2

Infrastrukturdepartementet

Kommerskollegiums synpunkter på Europeiska kommissionens förslag till förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020

Er referens: I2022/01758

Kommerskollegium ansvarar för frågor som rör utrikeshandel, EU:s inre marknad och handelspolitik. Kommerskollegiums 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. Myndigheten har tagit del av ovanrubricerande remiss och vill lämna följande synpunkter:

Kommerskollegium stödjer förslaget till förordning med syfte att främja förutsättningar för utvecklingen av säkra produkter med digitala element så att sårbarheter i hårdvaru- och programvaruprodukter minskar och för att skapa bättre förutsättningar för användare att ta hänsyn till cybersäkerheten. Vi ser som särskilt positivt att förslaget understryker behovet till ett livscykelperspektiv i säkerhetstänket för varor med inbyggd digital teknik, med fokus att öka transparensen och spårbarhet i efterlevnad, då cybersäkerhetssårbarheter och brister inte enbart kan lösas med t.ex. krav för certifiering. Vi ser också en fördel i att förslaget utgår från nya metoden som regleringsteknik så kraven på cybersäkerhet blir lättare för marknadens aktörer att följa.

Förslagets omfattning - otydligheter

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

Bland marknadens aktörer har det uttryckts att det finns otydlighet gällande förslagets omfattning, t.ex. kring definitionen av fjärrbehandling av data samt fri programvara med öppen källkod. Vi ser det därför som positivt att förslaget tydliggjort att program som nättjänst (SaaS) inte omfattas, detta för att undvika överlapp med NIS2 Direktivet. Däremot finns det fortfarande oklarheter när det gäller hemsidor.[1]

Vi ser det också som positivt att förslaget inte omfattar fri programvara med öppen källkod som utvecklas eller tillhandahålls utanför ramen för kommersiell verksamhet för att inte stå i vägen för innovation eller forskning. Dock ser vi att förslaget bör tydliggöra definitionen av kommersiell verksamhet.[2] samt klargöra hur definitionen ej färdigställd programvara (artikel 4.3) förhåller sig till fri programvara med öppen källkod[3] för att inte skapa otydligheter för företag.

Märkning och överensstämmelse med krav

Förslaget innehåller instiftandet av CE-märkning för cybersäkerhet. Även vi förstår motiveringen för detta, ställer vi frågan om det är möjligt att ställa krav på cybersäkerhet på samma sätt som för traditionella industrivaror – särskilt när det gäller förmåga att följa upp, kontrollera och utöva tillsyn av varor (som vi ser att CE-märkningen är förknippad med). Våra kontakter med olika intressenter tyder på att det fortfarande saknas kompetens vid myndigheter när det gäller cybersäkerhet i produkter. Vi undrar med andra ord om tillräckliga efterlevnadsmekanismer som en CE-märknings skulle kräva, faktiskt är på plats.

Rapporteringsskyldigheter

Förslaget inför nya rapporteringsskyldigheter för tillverkarna. Varuområdet omfattar redan idag en mängd olika rapporteringskrav (NIS2, DORA och GDPR) och utifrån perspektiven för god regleringssed

[1] T.ex., om en hemsida skulle bli ansluten till en applikation (härefter: app) via API (applikationsprogrammeringsgränssnitt) så skulle appen omfattas men inte själva mjukvaran. Här ser vi att det behövs mer tydlighet.

[2] Enligt t.ex. Internet Society är det är oklart om den nuvarande definitionen även innefattar icke-vinstdrivande/ideella organisationer som även tillhandahåller stödtjänster, säkerhetkonsultföretag som sponsrar säkerhetsverktyg som öppen källkod till stiftelser, samt individuella utvecklare som tar en mindre avgift för att lägga till funktioner.

[3] Förslaget bör tydliggöra hur artikel 4.3 om fri rörlighet förhåller sig förenligt till skäl 10, då bestämmelserna över ej färdigställd programvara kan tolkas att innefatta även fri programvara med öppen källkod. Det har rekommenderats av t.ex. Internet Society att fri programvara läggs till som undantag i artikel 4.3: : ”…förutsatt att [*programvaran är fri med öppen källkod*] eller att programvaran endast tillhandahålls under den begränsade tid som krävs för testningsändamål…”

och regelförenkling vill vi lyfta vikten att granska överlappningar mellan olika system, alternativt slå ihop olika system för att minska företagens regelbörda och onödiga kostnader. Cybersäkerhetsområdet är betingat med kopplingar till nationell säkerhet och det är viktigt att rapporteringen verkligen leder till transparens men också kan följas upp- något som kan vara mer utmanande på cyberområdet än för andra typer av incidentrapporteringar.

Standarder och gemensamma specifikationer

EU har de senaste åren ökat sin ansats att arbeta med strategiskt med standardisering. Förutom att kunna ta fram standarder för stöd av lagstiftning på ett tidsenligt och effektivt sätt, påverkas även den europeiska standardiseringen av säkerhets- och geopolitiska utmaningar.

Som vi lyft i andra remissvar[4] ställer vi oss frågande till krav som inte följer av de principer och processer som instiftas av standardiseringsförordningen (EU 1025/2012) med krav på öppenhet och transparens, t.ex., gemensamma specifikationer som nämns i förslaget. Detta kan bidra till ökad fragmentering och riskerar att EU ökar sin isolering från andra marknader på viktiga områden där interoperabilitet och gemensamma internationella lösningar är att föredra för en fungerande handel. Vi vill därför framhålla att internationella standarder ska användas så långt som möjligt i kravställning.

Digital reglering- utmaningar

Vår bedömning är att digital reglering rent allmänt är extremt komplext och ökar dessutom markant de regulativa skyddshänsynen som träffar en individuell vara med inbyggd digital teknik (produktsäkerhet, cybersäkerhet, motståndskraft, personlig integritet). Likväl är egenskaper i mjukvarubaserade produkter i sig svåra att följa upp, kontrollera och utöva tillsyn över, och således mer utmanande att reglera och standardisera. Förslaget om programvarubeteckning för sårbarhetsanalys synes som ett viktigt verktyg för att bygga in livscykelperspektivet men frågan är om den spårbarhet som efterfrågas är görlig i praktiken t.ex. för att bekräfta ansvar. Oftast är leveranskedjorna oerhört komplexa och samma mjukvara som används för olika användarfall behandlas av stort antal aktörer. Förslaget kommer också ställa omfattande krav på tredjepartscertifiering på marknaden- även om ambitionen att bidra till

[4] Se Kommerskollegiums yttrande om förordning om batterier 2020/01926-2.

ökad konkurrenskraft och säkerhet är förståelig är finns det få bevis att den maskineri som nu sätts i verkan verkligen kommer garantera bättre cybersäkerhet. Detta kan med andra ord ha både sämre säkerhet och konkurrenskraft som följd, särskilt beaktat andra system som tillämpas utanför Europa.

Förslaget redogör också för kopplingar med kraven i förlaget till rättsakten om artificiell intelligens där vår uppfattning är att marknadens aktörer inte nödvändigtvis är medvetna om att deras AI innovation faller inom reglering och hur AI ska hanteras och/eller har svårt att bedöma om den faller inom de föreslagna reglerna.[5]

När det gäller förslaget är det således mycket svårt att bedöma huruvida de olika varuregelverk som gäller och de digitala horisontella regler som tas fram samspelar. Vi kan därför dela oron som finns bland marknadens aktörer kring otydlighet och eventuellt överlappande regler.

Från ett handelsperspektiv innebär nya regler både kostnader och en administrativ börda för företagen – detta gäller särskilt när det gäller krav på cybersäkerhet. Det som är viktigt i sammanhanget är att regler som tas fram också kan följas upp på ett sätt som skapar lika villkor för företagen och faktiskt resulterar i ökad cybersäkerhet. Även om förslaget lyftet proportionalitet är det osäkert hur väl kraven leder till överensstämmelse ä(cybercertifiering garanterar t.ex. inte cybersäkerhet utan visar bara sårbarheter i en vara vid en given tidpunkt[6]) faktiskt kan följas upp av myndigheter (finns det kapacitet för livscykelperspektivet i myndigheternas marknadskontroll).

När det gäller digital reglering som ska samspela mellan marknader är det också viktigt att cybersäkerhetskrav beaktar regler utanför EU och skapar förutsättningar för ömsesidigt erkännande av krav, när så möjligt för att förebygga handelshinder. Avtal om ömsesidigt erkännande nämns i förslaget men resonemanget bör eventuellt utvecklas något mer för att beakta fungerande handel med tredje land utifrån de långtgående kraven som nu föreslås inom EU.

[5] Se Kommerskollegium, Innovation, AI, Technical Regulation and Trade. Questioning the Invisible Hand in the Digital Economy, 2023.
[6] Se Kommerskollegium, The Cyber Effect- The Implications of IT-security regulation on international trade, 2018 och Kommerskollegiums remissvar avs. SOU 2021-63, Dnr 2022/01892-2.

Ärendet har avgjorts av Vikarierande enhetschefen Linda Bodén i närvaro av ämnesrådet Heidi Lund, föredragande. I ärendets beredning har utredarna Catherine Persson och Felinda Wennerberg bidragit.

Stockholm som ovan

Linda Bodén
Vikarierande enhetschef

Heidi Lund
Ämnesråd