National Library of Sweden

Datum	Dnr.
2021-07-01	KB 2021-526

Infrastrukturdepartementet
i.remissvar@regeringskansliet.se
i.esd.remisser@regeringskansliet.se

Yttrande över Europeiska kommissionens förslag till förordning om harmoniserade regler för artificiell intelligens, Proposal for a Regulation laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts (COM (2021) 206), I2021/01304

Kungliga biblioteket • Besöksadress: Humlegårdsgatan 26, Humlegården, Stockholm
Box 5039, SE-102 41 Stockholm, Sweden • Telefon/Phone +46 10 709 30 00 • E-post/e-mail: kungl.biblioteket@kb.se • www.kb.se • Org.nr. 202100-1710

National Library of Sweden

Innehåll

Sammanfattning

Den 21 april 2021 presenterade kommissionen sitt förslag till en förordning om harmoniserade regler för artificiell intelligens (AI), inom ramen för strategin för det digitala Europa, (Förslaget). I faktapromemoria 2020/21:FPM109 har regeringen redogjort för sin uppfattning om Förslaget samt sin målsättning att Sverige ska vara ledande i att ta tillvara möjligheterna som användningen av AI innebär. Kungliga biblioteket (KB) delar regeringens uppfattning. KB agerar i enlighet med regeringens målsättning och har inrättat ett AI-labb, benämnt KB-labb, som utvecklar AI-modeller för forskningens infrastruktur. KB konstaterar med tillfredsställelse att Förslaget undantar "the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU" (artikel 52.3). Förslaget innehåller andra begrepp och definitioner som likaledes är betydelsefulla men inte är helt entydiga, t.ex. begreppet "harm" i kontexten forskning och som bör definieras. KB:s AI-modeller publiceras som öppen data och finns tillgängliga och vidareutnyttjas av såväl den offentliga som den privata sektorn. Av detta följer att det är av synnerlig vikt att KB:s stora digitala samlingar kan användas som träningsdata vid utveckling av AI-modeller utan de krav som ställs på högrisk AI-system i Förslaget, t.ex. CE-märkning. Förslaget är dock inte tydligt om KB omfattas av krav på högrisk AI-system när de AI-modeller som KB har utvecklat tillämpas av andra aktörer i högrisk AI-system. Därför förordar KB att det i Förslaget tydliggörs, att när en institution såsom KB utvecklar AI-modeller i forskningssyfte och dessa AI-modeller vidareutnyttjas av andra och tillämpas i högrisk AI-system ska inte KB som en följd därav komma att omfattas av artiklar för högrisk AI-system, t.ex. CE-märkning. Det är av synnerlig vikt att nämnda undantag formuleras på sådant sätt och att Förslaget i övrigt utvecklas i syfte att AI-system kan bidra till KB:s uppdrag att främja den svenska forskningens kvalitet och en demokratisk samhällsutveckling.

KB:s ställningstagande och skälen för dessa

Eftersom Kungliga biblioteket (KB) utvecklar "AI system" och är en "provider" samt tillgängliggör AI-system ("placing on the market") faller KB:s verksamhet med "AI system" i princip inom Förslagets tillämpningsområde. Beroende på hur Förslagets definitioner av begrepp med mera tolkas kan KB anses omfattas av Förslaget i mer eller mindre utsträckning. Förslaget definierar en rad begrepp och dessa definitioner är inte helt entydiga. Som exempel är det KB:s tolkning att KB inte använder AI-system för något högriskområde i Förslagets mening, men å andra sidan utvecklar KB och publicerar AI-modeller i vetenskapligt syfte som används av andra än KB. Detta ger upphov till oklarheter om hur KB ska tolka Förslaget och ytterst om KB omfattas av högrisk AI-system. Därför utvecklar KB nedan hur myndigheten ser på Förslaget i olika avseenden utifrån sitt uppdrag. Som kommer att framgå finns det beröringspunkter mellan forskning och

utveckling av AI-system inom offentlig och privat sektor eftersom det förra många gånger är en förutsättning för det senare.

KB:s kommentarer och ställningstaganden

Forskning – ”harm” (sida 8 och skäl 16), ”deep fakes” 5.2.4. TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS (TITLE IV),”research” (skäl 16) samt artikel 52.3

”Harm” (sida 8)

Begreppet ”harm” bör definieras.

Skäl för KB:s ställningstagande

KB med sina betydande datamängder har, framför allt genom KB-labb, utvecklats till en nationell resurs för utveckling och träning av AI-system för forskning. Med detta i beaktande är det av central betydelse att Förslaget inte hämmar en effektiv infrastruktur för forskning. KB:s verksamhet med AI-system för forskning innefattar inte en interaktion med människor. Men det är omöjligt att förutse hur forskning kommer bedrivas i framtiden samt om och i vilken utsträckning det kommer ske med stöd av AI-system i interaktion med människor och vilka risker som i sådana fall kan uppkomma och som möjlig konsekvens vad för slags skada (”harm”) som är förenad med risken. Därför är innebörden av ”harm” i skäl 16 av särskild betydelse. Av Förslaget sida 8 framgår att aktörer har framfört att begreppet ”harm” bör definieras och KB instämmer.

”Deep fakes” sida 14

Förslaget bör kompletteras med ett undantag för forskning.

Skäl för KB:s ställningstagande

Relevant i detta sammanhang är att Förslaget reglerar risker förenade med tillämpningen av AI och “deep fakes” (se 5.2.4. TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS (TITLE IV) sidan 14 i Förslaget). Om Förslaget i detta avseende skulle vara tillämpligt på forskning, skulle det vara till men för forskning och utveckling av AI och men även avseende en ökad förståelse av AI och t.ex. de risker som är förenade med AI. Förslaget anger undantag men det är oklart om det inkluderar forskning. Detta är en brist i Förslaget och KB bedömer att det kommer få negativa konsekvenser för forskningen om AI.

”Research” (t.ex. skäl 16 och artikel 52.3)

Begreppet forskning i Förslaget bör överensstämma med vad som är forskning enligt svensk rätt och omfatta forskning och utvecklingsarbete, d.v.s. såväl vetenskaplig och konstnärlig forskning som utvecklingsarbete på vetenskaplig

eller konstnärlig grund, dock inte sådan forskning eller sådant utvecklingsarbete som utförs inom ramen för högskoleutbildning på grundnivå eller på avancerad nivå.

Skäl för KB:s ställningstagande

KB konstaterar med tillfredsställelse att Förslaget undantager ”the right to freedom of the sciences” (artikel 52.3). KB noterar härvid att det inte kan uteslutas att begreppet ”sciences” har en annan innebörd än vad som framgår av svensk rätt. I svenska författningar är begreppet forskning annorlunda formulerat jämfört med Förslaget (se Högskolelagen (1992:1434), lag (2019:504) om ansvar för god forskningssed och prövning av oredlighet i forskning och lag (2003:460) om etikprövning av forskning som avser människor). Det vore olyckligt om Förslagets definition av forskning utesluter det som är forskning enligt gällande svensk rätt. I annat fall finns det en risk att AI inte kommer till nytta inom svensk forskning.

KB som kulturarvsinstitution - ”deep fakes” 5.2.4. TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS (TITLE IV) och artikel 52.3

”Deep fakes” (sid 14)

Förslaget bör kompletteras med ”the right to freedom of the arts”

Skäl för KB:s ställningstagande

Relevant i detta sammanhang är att Förslaget reglerar risker förenade med tillämpningen av AI och “deep fakes”. Om Förslaget i detta avseende skulle vara tillämpligt på den kreativa sektorn, kommer det vara till men för yttrandefriheten och den konstnärliga friheten. Visserligen står det i Förslaget att undantag ska kunna ges för ”freedom of expression” men Förslaget nämner inte ”the right to freedom of the arts”.

Artikel 52.3

Det är av synnerlig vikt att undantaget i Förslaget för ”the right to freedom of expression and the right to freedom of the arts” definieras på ett sådant sätt och Förslaget i övrigt vidareutvecklas så att det kan främja KB som en nationell resurs för den kreativa sektorn och den svenska kulturens utveckling och därmed berika KB:s samlingar samt en demokratisk samhällsutveckling.

Skäl för KB:s ställningstagande

KB:s samlingar har varit och är en inspirationskälla för journalister, författare och kulturskapare m.fl. i den kreativa sektorn. Genom AI-system kan KB:s digitala samlingar på ett helt annat sätt komma till användning för denna sektor. Detta är av en fundamental betydelse för KB:s uppdrag, eftersom samlingarnas tillväxt är

beroende av vad den kreativa sektorn producerar – ett ekosystem. Konstnärlig frihet (eller frihet för konstnärligt uttryck) kan definieras som "friheten att föreställa sig, skapa och distribuera olika kulturella uttryck utan statlig censur, politisk inblandning eller påtryckningar från icke-statliga aktörer."[1] Generellt beskrivs konstnärlig frihet såsom omfattningen av den självständighet som konstnärer får för att skapa konst fritt. Dessutom gäller konstnärlig frihet "medborgarnas rätt att få tillgång till konstnärliga uttryck och delta i kulturlivet - och [representerar] därmed en av de viktigaste frågorna för demokrati."[2] I detta perspektiv är det väsentligt att Förslaget inte hämmar den konstnärliga friheten. I stället bör Förslaget främja kreativa uttryck. För KB är det mycket viktigt att vad som inte regleras av Förslaget framgår med önskvärd tydlighet. Därför bör undantagen för ”the right to freedom of expression and the right to freedom of the arts and sciences” utvecklas, framförallt i skälen till Förslaget.

KB:s AI-modeller som används av offentlig och privat sektor i högrisk AI-system – artiklar om högrisk AI-system och regulatoriska sandlådor

KB förordar att det i Förslaget tydliggörs, att när en institution såsom KB utvecklar AI-modeller i forskningssyfte och dessa AI-modeller vidareutnyttjas av andra och tillämpas i högrisk AI-system ska inte KB som en följd därav komma att omfattas av artiklar för högrisk AI-system, t.ex. CE-märkning. I de fall KB samarbetar med offentliga myndigheter och privata aktörer är det även väsentligt att möjlighet ges till regulatoriska sandlådor.

Skäl för KB:s ställningstagande

De AI-modeller som KB utvecklar i forskningssyfte tillämpas även av myndigheter och i privat sektor. För dessa aktörer kan det i förekommande fall vara fråga om högrisk AI-system och krav på CE-märkning åläggas dem. För KB är det av avgörande betydelse att den myndighet/organisation som vidareutvecklar AI-modeller som KB har utvecklat har att efterleva kraven på högrisk AI-system, inte KB. I annat fall bedömer KB att forskningen kommer hämmas genom att de krav som ställs på högrisk AI-system även indirekt träffar KB och därmed forskningen. Förslaget är dock inte tydligt i detta avseende. Om KB skulle omfattas av kraven på högrisk AI-system inklusive CE-märkning, skulle konsekvenserna för KB bli mycket negativa och påverka forskningen menligt.

[1] UNESCO, United Nations Educational, Scientific and Cultural Organization (2018) https://unesdoc.unesco.org/ark:/48223/pf0000260592 (20210623)

[2] Ole, Reitov (29 April 2013) https://freemuse.org/news/un-report-on-the-right-to-artistic-expression-and-creation-now-available/ (20210623)

National Library of Sweden

Angående CE-märkning av samlingsbaserade modeller framtagna vid KB-labb

KB-labbs samlingsbaserade modeller och nyttoeffekter

Som en del av KB:s uppdrag att tillhandahålla en effektiv forskningsinfrastruktur utvecklar och tränar KB-labb artificiella neuronnät med generella förmågor till förståelse av text, bild och ljud. Neuronnäten tränas på dataset framtagna ur KB:s samlingar och kallas därför för samlingsbaserade modeller.

Modellerna innehåller ingen data och är inte primärt framtagna för att analysera/behandla den data de är tränade på, utan annan data som inte finns på KB. Modellernas generella förmågor är inte i sig direkt tillämpbara utan måste kombineras med ett system med någon funktionalitet eller tränas ytterligare för en speciell funktion eller domän för att kunna användas. Modellerna möjliggör alltså forskning och/eller funktionalitet/applicering i verksamheter i och utanför KB.

KB-labbs mest använda modell, KB-BERT, laddas ned av olika användare cirka 25 000 gånger i månaden. Penetrationen i samhället är alltså mycket hög.

KB-labb förbereder nu utveckling och träning av nästa generation samlingsbaserade modeller med högre kapacitet. Samhällsnyttan förväntas därmed flerfaldigas.

Förslag på CE-märkning för högriskapplicering av artificiell intelligens

I Förslaget beskrivs olika nivåer av risk beroende på appliceringens karaktär. För KB-labbs interna arbete och KB:s egen tillämpning av AI-system (AI-modeller) är risken obefintligt till låg. En del av tillämpningen av AI-system (AI-modeller) sker utanför KB. I dessa fall används AI-modeller som KB-labb har utvecklat som en grundförmåga vilken senare vidareutvecklas av andra än KB och inte av KB-labb. I det sammanhanget klassas appliceringens risk och i förekommande fall kan det bli fråga som högrisk. I dessa fall ska AI-appliceringen, enligt Förslaget, CE-märkas, vilket medför krav på en viss typ av dokumentation och test av appliceringens kvalitet och säkerhet. Frågan är dock om kraven på CE-märkning ska ha någon inverkan (direkt eller indirekt) på KB. I korthet: ska KB-labb CE-märka de samlingsbaserade modeller som labbet tar fram?

Oaktat att KB bedömer att Förslaget om högrisk och t.ex. CE-märkning inte reglerar KB-labb vill KB anföra följande:

Vetenskaplig utvärdering av KB-labbs modeller jämfört med CE-märkning

Det kan tyckas praktiskt och resurseffektivt att KB-labb CE-märker sina modeller i syfte att alla myndigheter/organisationer som använder modellerna slipper göra detta. Problemet är dock att variationer i säkerhet och kvalitet är unika för varje applikation, dels i en rent matematisk mening, dels för att kvalitetsvariationer och avvikelser i funktionalitet uppstår i förhållande till den aktuella appliceringen. Det

som är en variation/avvikelse i en applikation kan i en annan applikation var en omistlig funktionalitet. Förutom att det för KB-labb skulle innebära att KB skulle vara tvungen att göra tusentals CE-märkningar, en för varje applikation, är det för KB-labb okänt vilka tillämpningar som kan komma att utvecklas. Ett krav på CE-märkning på KB-labbs modeller skulle med andra ord omöjliggöra KB-labbs arbete med samlingsbaserade modeller. KB, genom KB-labb och i samarbete med akademin, utvärderar däremot de samlingsbaserade modellerna vetenskapligt. Det är en mer djupgående utvärdering än den som föregår en CE-märkning. Samtidigt är den vetenskapliga utvärderingskontexten i sig ett forskningsfält, där både utvärderingsmetoder och utvärderingsresultat är i ständig förändring med hänsyn till de framsteg forskningen gör.

Applikationer där CE märkning utförd av KB/KB-labb skulle kunna bli tillämplig

I de fall KB är med och tar fram själva appliceringen av AI-system förändras förutsättningarna. Det kan inträffa om KB i samarbete med t.ex. en annan myndighet tränar en modell för en specifik uppgift. Applikationen blir då enstaka/fåtalig och känd för KB-labb. I det fallet kan KB/KB-labb utföra CE-märkning. Men det skulle innebära ytterligare administration för KB och tillkommande kostnader samt hämma utvecklingen. I stället bör sådan utveckling av AI-system ske i det som i Förslaget beskrivs som ”regulatoriska sandlådor” och den myndighet som ska använda AI-modellen i sitt AI-system ansvara för CE-märkning.

Övrigt

KB förordar att ärendena om behandling av personuppgifter vid AI och text- och datautvinning (TDM) och behandling av personuppgifter i forskningsdatabaser bereds färdigt i närtid samt att en översyn av hur Infosoc-direktivet har genomförts i svensk rätt görs snarast möjligt.

Skäl för KB:s ställningstagande

Parallellt med att Förslaget förhandlas bereds alltjämt i regeringskansliet ärendena om dels KB:s behandling av personuppgifter vid AI/TDM, dels behandling av personuppgifter i forskningsdatabaser - en långsiktig reglering av forskningsdatabaser. Vidare bereds i regeringskansliet en översyn av inskränkningarna i upphovsrättslagen. Samtliga dessa ärenden har en avgörande betydelse för KB i sin tillämpning av AI i forskningens infrastruktur.

Genom storskalig digitalisering på KB och leveranser av digitala dokument enligt lag om elektronisk pliktleverans uppstår de facto en eller flera databaser på KB som ska kunna användas i forskningens infrastruktur med stöd av AI/TDM. Att

behandling av personuppgifter för AI/TDM[3] och behandling av personuppgifter i forskningsdatabaser[4] alltjämt bereds i regeringskansliet har en hämmande effekt på användning av AI system och TDM i forskningen och begränsar i avsevärd mån KB:s möjlighet att utföra sitt uppdrag.

När det gäller upphovsrätten pågår en översyn av upphovsrätten och inskränkningar som är påkallad oaktat Förslaget. Sverige har inte genomfört artikel 5.2.c i Infosoc-direktivet konformt med EU-direktivet. Ett genomförande av nämnda artikel i enlighet med sin ordalydelse skulle i väsentlig mån främja regeringens ambition att Sverige ska vara ledande i att ta tillvara möjligheterna som användningen av AI kan ge.

Konsekvenser för KB

I Förslaget anges att detta kommer att medföra kostnader och nya uppgifter för myndigheter på nationell och EU-nivå. I Förslaget förtydligas att myndigheterna ska ha tillräcklig kompetens och kapacitet för att leva upp till de krav som ställs i Förslaget. Kommissionen bedömer att det kommer att kräva vissa men inte omfattande personalresurser. I detta sammanhang hänvisar KB till sin bedömning ovan att Förslaget är oklart i de fall AI-modeller som KB har utvecklat vidareutnyttjas av andra organisationer och tillämpas i högrisk AI-system och om de krav som därvid ställs på högrisk AI-system även innebär att de måste uppfyllas av KB. Med hänsyn till denna otydlighet i Förslaget kan konsekvenserna för KB bli betydligt mer omfattande än vad Förslaget ger intrycket av och det kan därför inte uteslutas att kostnaderna som är förenade med Förslaget kommer att bli betydligt större.

Beslut i detta ärende har fattats av riksbibliotekarie Karin Grönvall, efter föredragning av verksjurist Jerker Rydén, biträdande riksbibliotekarie Lars Ilshammar och föreståndare för KB-labb Love Börjeson. Beslutet har signerats elektroniskt och saknar därför namnunderskrifter.

Karin Grönvall,

Riksbibliotekarie

Jerker Rydén,

Verksjurist

---

[3] https://www.regeringen.se/49d383/contentassets/4a47100e9cc54017810552ae888541c1/promemoria-personuppgiftsbehandling-i-forskningsbibliotekens-verksamhet.pdf (20210701)

[4] https://www.regeringen.se/49c0cd/contentassets/2570b2abef8c48f084bbddb48ed2300b/sou-2018_36_webb.pdf (20210701)