Infrastrukturdepartementet
Enheten för samhällets digitalisering
i.remissvar@regeringskansliet.se

Remissvar Europeiska kommissionens förslag till förordning om harmoniserade regler för artificiell intelligens (dnr I2021/01304)

Linköpings universitet (LiU) har beretts tillfälle att yttra sig över Europeiska kommissionens förslag till förordning om harmoniserade regler för artificiell intelligens och lämnar följande synpunkter.

Sammanfattningsvis har LiU följande synpunkter på remissen:

- Det är av yttersta vikt att forskningen fortsätter vara fri, givet att erforderliga etiska prövningar gjorts. Därför anser vi att meningen i (16) på sidan 22 ”Research for legitimate purposes in relation to such AI systems should not be stifled by the prohibition, if such research does not amount to use of the AI system in human-machine relations that exposes natural persons to harm and such research is carried out in accordance with recognised ethical standards for scientific research.” bör ändras till “Research for legitimate purposes in relation to such AI systems should not be stifled by the prohibition, if such research is carried out in accordance with recognised ethical standards for scientific research.”

- Vi välkomnar delen som säger att ”researchers, should be able to access and use high quality datasets within their respective fields of activities which are related to this Regulation.” (45). Tillgången till högkvalitativa relevanta data är av yttersta vikt för forskningen.

- Det är viktigt att skilja på utveckling/forskning och användning. Lagstiftningen bör i första hand koncentrera sig på användningen.

- Vi välkomnar att mycket i förslaget följer de etiska riktlinjer som högnivågruppen tagit fram.

- Vi välkomnar att samma regler ska gälla oberoende av var systemet har utvecklats.

Vidare har LiU från ett ämnesexpertperspektiv följande synpunkter på remissen:

- Ett generellt problem med lagstiftningen är att den fokuserar för mycket på teknik, vilket gör att man kan kringgå regleringen genom att undvika att få sin tekniska lösning klassad som AI. Som ett konkret exempel borde de fall som förbjuds enligt Artikel 5 inte vara beroende av vilken teknik som används. Generellt anser vi att lagstiftningen bör vara teknikneutral.

- Förslaget till lagstiftning dikterar på flera ställen på ett olämpligt sätt hur ett system ska implementeras, snarare än vilka egenskaper systemet ska ha, t.ex. Artikel 12. Det här riskerar att låsa in AI-system till sämre lösningar än vad som annars skulle varit möjligt (och därmed riskera att inte uppnå den önskade effekten).

- Definitionen av AI enligt Annex I är i grunden bra, de två första kategorierna följer vanliga läroböcker inom AI, medan den tredje punkten gör att definitionen innefattar i stort sett all mjukvara då de allra flesta använder statistik, optimering eller sökning i någon form. Definitionen skulle bli mer rimlig om den sista punkten ströks. (Ett annat sätt att se på det är att då nästan alla AI-tekniker bygger på sökning i någon form, skulle det troligen räcka med sista punkten.

- Ett annat generellt problem med lagstiftningen är att den högst troligen har många oönskade konsekvenser. Även om intentionen är att relativt få tillämpningar ska klassas som högrisk, finns det t.ex. en uppenbar risk att det dels finns sidoeffekter av lagstiftningen som gör att tillämpningar indirekt påverkas och dels att företag inte vågar ta risken att klassa fel och därmed agerar som om deras tillämpningar är högrisk. T.ex. kommer troligen väldigt många tillämpningar att räknas som högrisk-AI på grund av skrivningar som (40) på sidan 28 ”it is appropriate to qualify as high-risk AI systems intended to assist judicial authorities in researching and interpreting facts and the law”. Som exempel, om en domare använder ett översättningsprogram eller en sökmotor i sitt arbete skulle den kunna räknas som en högrisktillämpning.

- Generellt har de flesta AI-baserade verktyg väldigt många tillämpningar där det inte alltid är uppenbart vem som kommer använda dem till vad. Det är därmed svårt för den som tillhandahåller verktyget att veta hur det ska klassificeras. Två exempel ovan är översättningsprogram och sökmotorer.

- Vi håller med om att kvaliteten på data är väldigt viktigt (44) samt Art 10. Samtidigt försvårar existerande lagstiftning som GDPR möjligheterna att samla in data av högsta kvalitet och data som har samlats in får inte användas till annat, även om det skulle kunna bidra till att signifikant höja datakvaliteten. Alltså kommer man i många fall tvingas använda data av lägre

kvalitet. GDPR:s ”rätt att bli glömd” leder också till att data riskerar att försämras över tid. Vidare är det svårt att verifiera att ett system t.ex. inte diskriminerar såvida man inte har samlat in känslig information om användarna som man kan jämföra utfallet mot. Ett förtydligande kring hur dessa två delvis motstridiga lagar ska hanteras vore önskvärt.

- Kravet i Artikel 10(3) att data ska vara ”free of errors and complete” är i grunden omöjligt och bör strykas. Även i de få fall där det är teoretiskt möjligt, skulle det i praktiken ytterst sällan gå att uppnå, särskilt i relation till GDPR. Om en person kräver att få sin data borttagen eller inte ger sitt samtycke så blir data per definition ofullständigt. När det gäller fel så är det ofta inte entydigt vad som är rätt svar. Det är dessutom så att det som var rätt vid en tidpunkt, kan anses vara fel vid en senare (våra värderingar skiftar över tid, vetenskapsfronten flyttar på sig, osv).

- Generellt är det oklart hur den föreslagna lagstiftningen och GDPR ska kunna kombineras då den föreslagna lagstiftningen t.ex. kräver att man ska använda data med högsta möjliga kvalitet (44) och att man ska ha representativa data. Ett annat exempel är Artikel 12(4d) som kräver att man ska logga information om naturliga personer vars data man behandlar.

- Det är oklart hur den föreslagna lagstiftningen och den svenska lagstiftningen om offentlighetsprincipen ska kombineras. Det gäller dels myndigheters loggar över händelser, som kan innefatta potentiellt känsliga personliga data, och dels dokumentation som lämnas in för granskning som därmed vanligtvis blir offentliga samtidigt som de kan innehålla affärshemligheter.

- Reglering av AI har potential att främja innovation, däremot ser vi stora risker med att den juridiska osäkerhet som skapas genom att förslaget är beroende av tolkningar troligen kommer leda till hämmad innovation.

- För att minska riskerna för juridisk osäkerhet bör det finnas möjlighet för tillhandahållare av AI-system att ha en dialog med relevanta myndigheter och därmed få hjälp att tolka lagstiftningen och göra det möjligt att göra rätt från början, snarare än att i efterhand få reda på att de gjort fel med kraftiga sanktioner som resultat.

- Att följa den omfattande regleringen kommer troligen bli kostsamt för företag och organisationer, vilket kommer leda till ökade kostnader för slutanvändarna. Det är också troligt att trösklarna höjs för mindre och nya företag att ge sig in i branschen. Detta medför en risk att innovationsklimatet försämras och gynnar främst stora internationella företag som har råd att ta det stora kostnaderna som uppstår i samband med efterlevnaden av

regelverket.

- När tillämpningarna blir mer individanpassade kan det innebära att Art 12(3) ”post-market monitoring” medför att man måste övervaka individers användning av systemet, vilket riskerar att minska den personliga integriteten.

- Förslaget att användare måste använda AI-system”in accordance with instructions to use” Art 29(1) riskerar att lägga en alltför stor juridisk börda på användaren som troligen behöver förstå lagen och hur den förhåller sig till tillämpningen för att kunna använda systemet på ett korrekt sätt.

- Vi är positiva till användningen av Art 53 ”regulatory sandboxes” däremot är vi tveksamma till att hantera dessa på nationell nivå då de riskerar att bli väldigt olika och att vissa länder inte alls kommer att införa dessa.

Handläggningen av beslutet

Beslut i detta ärende har fattats av rektor vid rektors beslutsmöte i närvaro av studentrepresentanterna August Goldhahn och Beatrice Ronsten samt rektors sekreterare Maria Fält, efter föredragning av biträdande professorn Fredrik Heintz, som deltagit digitalt.

Jan-Ingvar Jönsson

Maria Fält på uppdrag av Fredrik Heintz

Sändlista:
Infrastrukturdepartementet, Enheten för samhällets digitalisering
Universitetsledningen
Universitetsdirektörens ledningsgrupp
Fakultets- och områdesstyrelser
Dekanerna
Prefekterna
Fakultetskanslierna
Överbibliotekarien
Internrevisionen
Berörda lokala fackliga organisationer
Studentkårerna
LiU-Nytt