Rymdstyrelsen
Swedish National Space Agency

REMISSVAR

2021-06-23

Dnr 2021-00172
Ert dnr I2021/01304

Infrastrukturdepartementet
Enheten för samhällets digitalisering

Remissvar avseende 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

Rymdstyrelsen har beretts tillfälle att yttra sig över följande förslag: Proposal for a Regulation laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts: I2021/01304 och vill härmed lämna följande synpunkter.

Sammanfattning

Rymdstyrelsen ställer sig i huvudsak positiv till förslaget av en harmonisering av regler för artificiell intelligens sker på europeisk nivå. Vi anser att AI kopplat till rymdverksamhet vare sig behöver förbjudas eller klassas som ett hög-riskområde, vilket är i enlighet med förslaget.

Rymdstyrelsen tycker det är mycket viktigt med principen att hantera risker och problem med AI **utan** att försvåra för innovationer och teknisk utveckling genom AI på ett sätt som riskerar att påverka europeisk konkurrenskraft negativt.

Synpunkter

Rymdstyrelsen konstaterar att rymdverksamhet påverkas mycket av artificiell intelligens. AI används i ökande utsträckning i rymdsammanhang på data från satelliter och andra rymdfarkoster. AI kommer också i ökande utsträckning användas i styrning av rymdfarkoster. Dessa rymdtillämpningar med AI använder

Postadress
Box 4006
SE-171 04 SOLNA, Sverige

Besöksadress
Hemvärnsgatan 15, Solna
Solna, Sverige

Telefon
08-40 90 77 00

Telefax
08-627 50 14

E-mail
rymdstyrelsen@snsa.se
rymdstyrelsen.se

inte personliga data kring individer som riskerar etiska problem. Det finns därför inte anledning att begränsa användandet av AI i rymdsektorn. Även om satelliter tar bilder på jorden så kommer vi inte under överskådlig tid få bilder där individer kan urskiljas.

Ur ett nationellt säkerhetsperspektiv kan data ändå vara känslig, enskilt, men framför allt i kombination med AI och annan information, av både öppen och sluten karaktär. Riskbedömning av rymddata bör därför även göras utifrån hur rymddata kan analyseras i kombination med annan data. Rymddata kan också vara en del i ett system som genererar säkerhetskänslig information med hjälp av AI, det är i det fallet den typen av systemet som skall risk-klassificeras med hög-risk och inte de ingående dataseten. Detta för att i möjligaste mån bibehålla innovationskraften i öppna data. Rymdstyrelsen har idag inte kunnat identifiera något sådant AI system som skulle leda till att det behöver förbjudas eller klassas som ett högrisksystem. Rymdstyrelsen förutsätter att berörda myndigheter som till exempel Försvarsmakten och Myndigheten för säkerhetsskydd och beredskap (MSB) behandlar detta vidare i den mån de finner det nödvändigt.

Vad gäller kontroll och styrning av rymdföremål så ställs mycket höga krav på tillförlitlighet på grund av att systemen normalt är kostsamma och med få undantag omöjliga att reparera. Styrning av rymdföremål är omgärdat av mycket hårda krav och standarder som ska uppfyllas innan de får skjutas upp i rymden. Även om dessa inte är lagstadgade så är de mycket omfattande.

Det internationella fördrag - Rymdfördraget (Outer Space Treaty) anger dessutom att Stater ska ansvara för nationell rymdverksamhet, oavsett om den bedrivs av statliga eller icke-statliga enheter. En stat är därför ansvarig för skador som orsakas av deras rymdföremål. Detta gör att nationella lagar, i vårt fall Rymdlagen, kräver att tillstånd erfordras för att skicka upp föremål i rymden, då måste aktörerna ge tillräckliga säkerhetsgarantier för att rymdföremålet kan styras på ett säkert sätt. Rymdområdet omgärdas därmed av tydliga riktlinjer och regler vilka kan appliceras oavsett om det är en AI eller annan reglerande mjukvara för styrning av rymdfarkoster.

Vi instämmer därmed med förslaget att AI kopplat till rymdverksamhet vare sig behöver förbjudas eller klassas som ett hög-riskområde.

Rymdstyrelsen tycker det är mycket viktigt med principen att hantera risker och problem med AI **utan** att försvåra för innovationer och teknisk utveckling genom

AI. Förslaget utgör kanske en rimlig ansats här även om det är svårt att se små företags möjlighet att hantera ett högrisksystem.

Detaljerade synpunkter

I förslaget punkt 35 (sid 26):
"AI systems used in education or vocational training, **notably** for determining access or assigning persons to educational and vocational training institutions or to evaluate persons on tests as part of or as a precondition for their education should be considered high-risk, since they may determine the educational and professional course of a person's life and therefore affect their ability to secure their livelihood."

I denna mening bör ordet "notably" tas bort eftersom det indikerar att det finns andra aspekter av "education or vocational training" som kan inbegripas i högrisksystem med strikta reglering och stora kostnader. Något liknande indikeras inte i Annex III punkt 3.

Utbildning är ett mycket viktigt område med stor potential att dra nytta av innovationskraften i AI samtidigt väldigt kostnadskänsligt. Vi tror intentionen är i denna riktning men för säkerhet skull bör ordet tas bort.

I förslaget punkt 49 (sid 30):
"High-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity in accordance with the generally acknowledged state of the art."

För att inbegripa lärande system bör det stå:

"High-risk AI systems should perform consistently **or improve** throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity in accordance with the generally acknowledged state of the art."

Kapitel 2 artikel 10 punkt 3 (sid 48):
Att ett data-set är helt fritt från fel "free of errors" kan i vissa fall vara omöjligt att visa eller bevisa. Är det inte tillåtet att använda eller utveckla system för AI då? Räcker det kanske med till exempel 99.9999 procent av data är korrekt.

På sidan 29 punkt 44 inleder man motsvarande text med ”sufficiently”: ”*Training, validation and testing data sets should be **sufficiently** relevant, representative and free of errors and complete in view of the intended purpose of the system.*”

Vi föreslår att man använder en liknande formulering i kapitel 2 artikel 10 punkt 3. Men för att vara extra tydlig anser vi att det är ”free of errors and complet” som behöver ordet ”sufficiently” därav den nya placeringen. ”Relevant” och ”Complete” kan stå utan med bibehållen mening.

“Training, validation and testing data sets shall be relevant, representative, **sufficiently** free of errors and complete.”

Företrädesvis ändras det både på *sidan 29 punkt 44* och i *kapitel 2 artikel 10 punkt 3*.

Kapitel 2 artikel 14 punkt 4 (a) (sid 51):
“(a) fully understand the capacities and limitations…”

Ordet “fully” kan här innebära orimliga krav i ett större komplexare system. Att kräva att enskilda individer har fullständig förståelse blir orimligt, jämför med ett stort flygplan som tex Airbus A380, dess piloter kan inte ha **fullständig** förståelse av systemet men kan ändå hantera det tillräckligt bra för att vi ska flyga med det.

Vi förstår intentionen och avsikten med formuleringen, men man bör också ta i beaktan att myndigheten som ska kontrollera detta kan sätta omöjliga krav med denna typ av formulering.

Kapitel 2 artikel 15 punkt 3 och 4 (sid 52):

I punkt 3:
”High-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems.”

I punkt 4:
“High-risk AI systems shall be resilient as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities.”

I båda dessa meningar anser vi att ordet ”resilient” blir problematiskt. Vi förstår intentionen, men det blir ändå väldigt otydligt hur detta ska tolkas. Ska systemet tolerera ett fel, ska det vara lika säkert som ett flygplan, kärnkraftverk eller bromsarna på en bil.

Samma problem gäller förstås i punkt fyra gällande cybersäkerheter. Hur ska en enhetlig myndighetskontroll av system med så skilda områden som i annex III hanteras. Olika områden med olika krav, olika nationella myndigheter som kan göra väldigt olika tolkningar.

Det är förstås svårigheten med denna typ av horisontellt förslag som ska täcka så många applikationsområden, det blir svårt att vara tydlig och konkret i denna typ av punkter eftersom, hur ”resilient” systemet ska vara beror på tillämpningsområdet.

Kanske skulle en formulering i liknande följande bidra till en något tydligare intention:

”Ett högrisksystem baserade på AI ska vara minst lika bra eller väsentligen bättre vad gäller förmågan att hantera fel (resiliens) som liknande eller jämförbara tjänster inom tillämpningsområdet”

Det skulle åtminstone ge en bättre vägledning.

TITEL VIII - Kapitel 3 artikel 64 punkt 1 (sid 77):
Vi kan inte se annat än att denna punkt riskerar att begränsa internationellt samarbete där man skulle kunna utnyttja ”federated learning” alltså att man tränar på separata data-set. Data hålls hemlig i respektive land – tex sjukhus som samarbetar men de kan inte dela data, bara det man lärt av data. På så sätt kan man få en mycket bättre modell som tränats på data från många sjukhus. Måste all data delas med kontrollerande myndighet kommer denna typ av samverkan begränsas och ett tillvägagångsätt med enorm potential tas bort för högrisksystem.

I stället för att myndigheter ska gå in och kontrollera enskilda data bör kontrollerande myndigheter fokusera på att systemen fungera i enlighet med kraven.

I detta ärende har generaldirektören beslutat efter föredragning av Vilgot Claesson.

För Rymdstyrelsens räkning

Anna Rathsman
Generaldirektör

Vilgot Claesson
Handläggare