Kontaktperson RISE
Susanne Stenberg och Håkan Burden
susanne.stenberg@ri.se och hakan.burden@ri.se
073 398 73 41 och 073 052 02 29

Remissyttrande från RISE avseende kommissionens förslag till begäran om europeiska standarder för AI

RISE, Research Institutes of Sweden, och ärendets beredning

RISE Research Institutes of Sweden är ett statligt ägt forskningsinstitut. Våra omkring 3 000 medarbetare driver och stöder innovationsprocesser och ungefär 120 test- och demonstrationsmiljöer för framtidssäkra teknologier, produkter och tjänster. Inom en av RISE fem divisioner, divisionen Digitala system, arbetar drygt 550 medarbetare med elektronik, informations- och kommunikationsteknik och mjukvaruutveckling, mobilitet, systemanalys, cybersäkerhet och artificiell intelligens. RISE driver en rad forskningsprojekt i samverkan med såväl privata som offentliga aktörer.

Beredningen av remissärendet omfattar Digitala systems ledningsgrupp med ansvarig divisionschef Charlotte Karlsson. Remissvaret är utfört av Håkan Burden och Susanne Stenberg, seniora forskare inom digitalisering, juridik och policy.

Förslaget, RISE rekommendation samt remissens innehåll

Remissen avser Kommerskollegiums begäran om synpunkter (dnr 2023/00434) inför Kommissionens beslut om begäran om europeiska standarder (Kommissionen, 2023) i relation till den föreslagna AI-förordningen (Kommissionen, 2021a). Kommissionen föreslår ett genomförandebeslut för att de europeiska standardiseringsorganen CEN och CENELEC ska ta fram europeiska standarder för AI-förordningens tekniska krav i kapitel 2 (artiklarna 8-15), kraven på kvalitetsstyrningssystem (artikel 17) samt EU-försäkran om överensstämmelse. Den sista begäran omfattar ett flertal artiklar – processerna samt kompetensen hos de som ska utföra granskningen av överensstämmelsen (såsom artiklarna 19, 33 och 48 samt bilagorna VI och VII).

RISE anser att förslaget kan accepteras.

Ställningstagandet motiveras av att när standarder är på plats finns mer detaljerade regler till vägledning för aktörer och verksamheter för hur AI-system i praktiken ska utvecklas och användas för att uppfylla de lagkrav som kommer gälla enligt den föreslagna AI-förordningen. Det stärker möjligheterna för näringsliv, offentlig sektor och civilsamhället att bidra till ansvarsfullt användande av AI-system på den europeiska marknaden.

Samtidigt är det arbete för standardisering som genom den föreslagna begäran om standarder kommer starta, inte endast av central betydelse för att AI-system ska fungera på ett säkert sätt utan också för hur samhällssystemet kommer fungera. Det beror på att det finns en dimension om etik och ansvarsfullt agerande från aktörer på marknaden, eftersom standarderna i det här

fallet också kommer att ha bäring på hur människors grundläggande rättigheter säkerställs i relation till ett AI-system.

Det är därför viktigt att beakta vems perspektiv och intressen som vägs in i standarderna, såsom användarens skyldigheter och ansvar för AI-system, vilket kopplar till förmågan att förstå när skadestånd kan krävas och hur, samt hur grundläggande rättigheter respekteras i relation till allt från maskinsäkerhet till rättssäker och effektiv myndighetsutövning. Vi utvecklar resonemangen i följande stycken om kopplingen mellan etik och standarder, användarperspektivet samt representation. Vi avslutar med två kortare kommentarer om vad vi ser som en obalans mellan omfattning i akter som ska komplettera varandra samt vad som ska styra kvalitetsarbetet gällande hög-risk AI-system.

Produktsäkerhet och grundläggande rättigheter

Ett utmärkande drag för de begärda standarderna är att de inte bara motiveras utifrån säkerhet och hälsa utan också utifrån de grundläggande rättigheterna så som de definieras i EUs stadga (OJEU, 2012). Certifiering och CE-märkning kommer därmed inkludera de grundläggande rättigheterna i ett sammanhang som traditionellt setts som en fråga om produktsäkerhet. Eller mer konkret – ett CE-märke kan nu omfatta både produktsäkerhet och de grundläggande rättigheterna (Burden & Stenberg, 2022).

Tabell 1 ger en översikt av hur vissa av lagkraven i den föreslagna AI-förordningen (2021) relaterar till de etiska riktlinjerna framtagna av EUs oberoende expertgrupp (HLEG, 2019), kommissionens begäran om standarder (2023) och pågående initiativ inom de internationella standardiseringsorganen ISO och IEC. Vi utgår från det förslag till AI-förordning som Ministerrådet förhandlat och framfört till Parlamentet (Rådet, 2022).

Aktör	***Bias***	***Human-in-the-loop***
HLEG (2019)	Systemen ska vara opartiska	Människan ska kunna intervenera
Rådet (2022)	Data ska vara representativ, relevant och i möjligaste mån felfri och komplett (artikel 10)	Mänsklig översyn ska motverka risker i relation till de grund-läggande rättigheterna (artikel 14)
Kommissionen (2023)	Begäran om standard för förvaltning och kvalitet för data inom AI	Begäran om standard för mänsklig översyn av AI-system
ISO / IEC	Standard: *Data Governance* Rapport: *Bias in AI*	Rapport: *Trustworthy AI* Rapport: *Human-system interaction*

Tabell 1: Från etik till standarder

I dialog med SIS, Svenska Institutet för Standarder, har vi förstått att CEN och CENELEC kommer i möjligaste mån utgå från existerande, internationella standarder som arbetas fram inom bland annat ISO och IEC. På så sätt blir de facto-kraven likalydande med de standarder som används på andra marknader. Som framgår i tabell 1 finns det idag inte internationella standarder för några av lagkraven som ställs genom AI-förordningen. Det är både en utmaning för CEN och CENELEC i relation till att få en standard på plats inför 30e april 2025, men

också en möjlighet för de som vill påverka hur standarderna ska formuleras och därmed också de facto-kraven för hög-risk AI-system.

Användarens skyldigheter

En aspekt att beakta i relation till *Human-in-the-Loop* och artikel 14 är relationen till användarens ansvar. Artikel 29 i den föreslagna AI-förordningen anger det ansvaret med att bland annat kräva att en användare ska kunna avgöra om utdata från AI-systemet är rimligt i relation till indata. CEN och CENELEC lyfter samma perspektiv utifrån vad en användare kan förväntas använda systemet till (N-012, 2022).

Standarder bör inte i första hand täcka de tänkta syftena av AI utan snarare *”reasonable forseeable use”* av berörda AI-system (N-013, 2022). Vi gör samma bedömning, vilket rimmar med vad vi lyft i relation till det föreslagna skadeståndsansvaret för produkter och AI-system och hur en användare ska kunna resonera om hur sannolikt det är att ett AI-systems utdata i relation till indata orsakat en viss skada (Burden & Stenberg, 2023). Att inte bara detaljera hur ett syfte kan uppnås utan också beakta hur ett system kan tänkas användas är en viktig förskjutning av perspektiv. Standarder som är begripliga för användare av AI-system blir därmed en central del av att säkerställa att användare kan uppfylla sina skyldigheter men också värna om sina rättigheter.

Representation

Hur ska då Sverige agera i relation till vems perspektiv som återspeglas i standarderna? Det kommer att kosta att engagera sig i arbetet - alltifrån medlemskap i en standardiserings-organisation, tid för att sätta sig in i standardiseringsinitiativen samt att delta på arbetsmöten och rösta i olika instanser. CEN och CENELEC nämner att det är viktigt att små och medelstora företag, konsumenter, medborgare, arbetstagare samt miljön representeras (N-103, 2022). Ur ett svenskt perspektiv kanske även offentlig verksamhet ska vara med på den listan då flera av de områden som anses utgöra hög risk och därmed ska uppfylla standarderna berör deras verksamhet? Exempel här är arbetsförmedlande system, system rörande migration, system för sociala förmåner samt utbildningsfrågor. Här kan offentlig sektor både ha rollen som tillhandahållare och/eller användare.

Övriga kommentarer

Den föreslagna AI-förordningen hänvisar till att AI-system som utgör säkerhetskomponenter i maskiner kommer utgöra hög risk. Den föreslagna maskinförordningen (Kommissionen, 2021b) använder istället begreppet *Machine learning*, ML. ML är en av flera AI-teknologier enligt AI-förordningen, men så är också logik- och kunskapsbaserade system. Det är alltså inte bara en fråga om terminologi utan även om omfattning. En fråga som behöver besvaras är hur en standard ska utformas som gäller för både AI-system och maskiner när omfattningen av vad som ska regleras skiljer sig åt i de båda föreslagna förordningarna?

Enligt artikel 17 i den föreslagna AI-förordningen ska ett kvalitetsstyrningssystem vara ett verktyg för att säkerställa en rimlig kvalitet på en produkt eller tjänst. Akten föreslår dessutom att omfattningen av det systemet ska vara beroende av storleken på organisationen så att små och medelstora företag inte får en orimlig administrativ börda. Även om motiveringen skulle vara rimlig ur ett innovationsfrämjande perspektiv anser vi att omfattningen av kvalitetsarbetet och tillhörande system ska motsvara vad som krävs för att nå en rimlig nivå av säkerhet för produkter och tjänster.

Sammanfattningsvis

Sverige bör acceptera begäran om standarder. Alternativet skulle vara att dra tillbaka förslaget om AI-förordning då förordningens utgångspunkt är att de övergripande lagkraven ska detaljeras genom standarder. Saknas de standarderna blir AI-förordningen svår att tillämpa.

Vi vill lyfta två övergripande synpunkter inför arbetet med att ta fram standarder för hög-risk AI-system. För det första, AI-förordningen berör både traditionella områden för produkt-säkerhet och etiska aspekter av AI med explicit koppling till de grundläggande rättigheterna. Dessutom berör standarderna också användare, inte bara tillhandahållare av, AI-system. Det är därför värt att överväga hur Sverige kan säkerställa en relevant representation i arbetet för berörda standarder.

För det andra, de standarder som tas fram för AI-system måste kunna tillämpas tillsammans med andra regulatoriska initiativ. Här är maskinförordningen ett exempel på hur horisontell och sektoriell standardisering behöver samexistera. Men det finns också beröringspunkter med synen på kvalitetsstyrning som en gemensam aspekt inom certifiering samt de övergripande motiveringarna inom det digitala årtiondet och den gröna given. Om arbetet med standarder för AI resulterar i krav som inte är förenliga med andra standarder riskerar arbetet med standarder att fallera.

RISE Research Institutes of Sweden

Digitala Divisionen

Håkan Burden och Susanne Stenberg
hakan.burden@ri.se och susanne.stenberg@ri.se

Referenser

Burden, H., & Stenberg, S. (2021). Remissyttrande från RISE avseende kommissionens förslag till förordning om regler för AI-system. 2021-06-24. https://www.ri.se/sites/default/files/2022-03/RISE%20yttrande%20om%20EU-kommissionens%20förslag%20till%20AI-regler.pdf

Burden, H., & Stenberg, S. (2022). Regulating Trust – An Ongoing Analysis of the AI Act. Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:ri:diva-61344

Burden, H., & Stenberg, S. (2023). Remissyttrande från RISE avseende kommissionens förslag till skadeståndsregler för produkter och för AI. 2023-02-17. https://www.ri.se/sites/default/files/2023-02/RISE%20yttrande%20om%20skadeståndsregler%20Ju2022-03499.pdf

HLEG (2019). INDEPENDENT HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE SET UP BY THE EUROPEAN COMMISSION ETHICS GUIDELINES FOR TRUSTWORTHY AI. Bryssel, Belgien. 08-04-2019.

Kommissionen (2021a). Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING OM HARMONISERADE REGLER FÖR ARTIFICIELL INTELLIGENS (RÄTTSAKT OM ARTIFICIELL INTELLIGENS) OCH OM ÄNDRING AV VISSA UNIONSLAGSTIFTNINGSAKTER, COM/2021/206 final. Bryssel, Belgien. 21-04-2021.

Kommissionen (2021b). Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om maskinprodukter COM/2021/202 final. Bryssel, Belgien. 21-04-2021.

Kommissionen (2023). COMMISSION IMPLEMENTING DECISION of XXX on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence. Ref. Ares(2023)1690984.

N-012 (2022). Annex to CEN and CENELEC feedback on the draft AI standardization request (“main paper”), Standardization Request Ad Hoc Group (SRAHG) on AI. Document N-012. 2022-06-29.

N-013 (2022). CEN and CENELEC feedback on the draft AI standardization request (“main paper”), Standardization Request Ad Hoc Group (SRAHG) on AI. Document N-013.

OJEU (2012). EUROPEISKA UNIONENS STADGA OM DE GRUNDLÄGGANDE RÄTTIGHETERNA. Europeiska unionens officiella tidning, C 326/391 2012/C 326/02. 26-10-2012.

Rådet (2022). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach. Council of the European Union, Brussels, Belgium. 25-11-2022.