Kontaktperson RISE
Susanne Stenberg
susanne.stenberg@ri.se
073 398 73 41

Remissyttrande från RISE avseende kommissionens förslag till förordning om regler för AI-system

RISE, Research Institutes of Sweden, och ärendets beredning

RISE 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 450 medarbetare med elektronik, informations- och kommunikations–teknik och mjukvaruutveckling, mobilitet, systemanalys, cybersäkerhet och artificiell intelligens. RISE bedriver en rad forskningsprojekt i samverkan med såväl privata som offentliga aktörer.

Beredningen av ärendet omfattar Digitala systems ledningsgrupp med ansvarig divisionschef Charlotte Karlsson. Remissvaret är utarbetat och utformat utifrån en inledande analys av de föreslagna reglerna. Detta arbete är utfört av Håkan Burden och Susanne Stenberg, seniora forskare inom mjukvaruutveckling, juridik och policyutveckling. I arbetet har vi haft möjlighet att få synpunkter från ett flertal aktörer (t.ex. forskare inom datavetenskap, två regionala myndigheter, start-ups, ett flertal statliga myndigheter och privata innovationsaktörer). Synpunkterna har bland annat inhämtats genom seminarier anordnade av AI.se, RISE AI-agenda och branschorganisationer.

Inledande kommentarer

De av kommissionen föreslagna reglerna är omfattande och i delar svåra att överblicka eller bedöma konsekvenserna av. Det finns inte någon konsekvensanalys redovisad i anslutning till de remitterade reglerna. Det står samtidigt klart att förslaget, om det genomförs, kommer att påverka många verksamheter. Istället för att i remissvaret lyfta mer generella synpunkter har RISE valt att beskriva en inledande analys av några utvalda delar av de föreslagna reglerna. Härigenom kan RISE som forskningsinstitut bidra till att svenska aktörer får en mer konkret bild av hur deras verksamhet kan komma att bli påverkad samtidigt som regeringen får underlag för att bedöma en svensk position till förslaget.

Remissens struktur

Yttrandet gäller EU-kommissionens förslag på reglering av AI [1]. Det är strukturerat på det viset att vi…
… för det första ställer den föreslagna förordningstexten i relation till kommissionens motivering till att reglera AI på den gemensamma marknaden,
… för det andra analyserar hur regleringen kan komma att påverka innovationssystemet och

framtida investeringar inom AI-sektorn men också på andra områden,
… för det tredje undersöker förslaget ur ett teknik-perspektiv för att se hur det kan påverka olika aktörers förmåga att förstå konsekvenserna av sin verksamhet samt hur proaktiva de kan vara i sina avtal,
… för det fjärde kan regleringen få effekter på svensk myndighetsutövning och pågående initiativ kring digitaliseringen av verksamheten, samt
… för det femte avslutar med att sätta förslaget i ett större perspektiv i relation till kommande och existerande reglering och hur det förskjuter mandaten inom EU och mellan EU-organen och svenska institutioner.

Indelningen är inte ortogonal, det finns beröringspunkter mellan avsnitten, däremot är fördelen med en gruppering att det ger teman att fundera över när man ska ta ställning till förslaget: Hur främjar vi innovation i relation till AI och vilken innovation vill vi främja? Vem ska ta ansvar för vad, när nya AI-system sätts på marknaden och hur kan och ska det regleras? Hur ska AI ses i relation till pågående initiativ kring digitaliseringen av myndighetsutövning? Samt, hur står förslaget i relation till vad det vill uppnå och visionen av EU?

Kommissionens motivering

I det här avsnittet lyfter vi vår syn på syftet med regleringen, vad som innefattas av hög-risk-begreppet och AI i relation till människan.

Syftet är ökad tillit till AI som teknologi

Ingressen nämner att det finns fyra mål med direktivet (Memorandum 1.1):

1) säkerställa att de AI-system som placeras/introduceras eller används på den gemensamma marknaden är säkra och respekterar grundläggande rättigheter och existerande regler,
2) skapa legal förutsägbarhet för innovation och investeringar,
3) utöka styrning och effektiv uppföljning av existerande regler inom grundläggande rättigheter och säkerhetskrav relevanta för AI-system, samt
4) tillhandahålla och utveckla en gemensam marknad för lagenliga, säkra och trovärdiga AI-applikationer och förhindra att spelreglerna fragmenteras inom marknaden

Samtidigt nämns hälsa, grundläggande rättigheter och säkerhet genomgående i förslaget. Från vårt perspektiv är det tydligt att grundläggande rättigheter återfinns i punkt 1) och 3) ovan. Annex III listar dessutom de AI-system som utgör en hög risk för medborgarna i relation till grundläggande rättigheter. Vi kan också se att säkerhet i relation till AI-produkter och –applikationer återfinns i punkt 1), 3) och 4). Annex II listar de produkter som kan innehålla eller utgöra hög-risk AI.

Det är oklart varför Annex III inte nämner att AI som används för fördelning av vård och omsorg är ett prioriterat område att värna. Inte heller arbetsmiljö och relevanta regler tas upp i annex III. Hälsa nämns enbart som ett explicit område i artikel 54.1.a.ii där det står att undantag kan beviljas från GDPR för att träna AI-system som kan bistå i proaktiva åtgärder, kontroll och behandling av sjukdom. Anser Kommissionen att hälsoområdet redan är tillräckligt reglerat i relation till AI, såsom finanssektorn är (Memorandum 1.2), eller finns det andra skäl till att hälsa inte får samma tyngd som grundläggande rättigheter och produktsäkerhet?

Eftersom tillgången till fundamental infrastruktur omfattas, hur kommer det sig att inte EUs resiliens i form av jordbruk och försörjningsberedskap är med i Annex III? Inom jordbruket kan AI-system användas för effektivare bevattning, beräknande av lämplig tid för skörd med minskat svinn som följd eller för att avgöra lämpliga användningsområden för olika marker [2]. AI som stöd åt den verksamheten lämnas oreglerad enligt förslaget. Däremot regleras AI som säkerhetskomponent i skogs- och jordbruksmaskiner.

Det är svårt att se hur kommissionen resonerat när den gjort sina urval av regler att hänvisa till. Är det produkter (annex II) och verksamhet (annex III) som man vill reglera egentligen, för att säkerställa att grundläggande rättigheter, säkerhet och hälsa inte kompromitteras genom tvivelaktig AI? En otydlighet i urvalet av de produkter och verksamheter som regleras riskerar att motverka syftet med regleringen, nämligen att skapa tillit till tekniken.

Hög-risk

Artikel 6 som definierar vad som anses vara hög-risk AI innehåller två otydligheter. Den första otydligheten återfinns i Artikel 6.1. En ordagrann läsning av texten ger att ett AI-system är att betrakta som utgörande hög-risk om det både

(a) är en del av eller utgör en egen säkerhetsprodukt i enlighet med appendix II, och
(b) är en del av eller utgör en egen säkerhetsprodukt i enlighet med appendix II och därmed behöver certifieras av en tredje part.

Eftersom alla system som uppfyller kraven för (b) även uppfyller kraven för (a) är antingen (a) redundant eller så är meningen att (a) eller (b) ska vara uppfyllt. Här hade det varit önskvärt med en klar formulering för att undvika redundanta definitioner alternativt tydliggöra skillnaden mellan (a) och (b). Går man till förklaringen bakom förslaget, ”Explanatory memorandum” (5.2.3) står det att ett AI-system anses utgöra en hög risk om det antingen är tänkt att användas som säkerhetssystem i relation till en produkt som kräver tredjeparts-certifiering eller används inom något av de områden som tas upp i annex III. Utifrån den förklaringen är en juridisk-teknisk lösning att stryka (a) från artikel 6.

Den andra otydligheten i relation till artikel 6 kommer ifrån Artikel 60 som refererar till artikel 51 som refererar till artikel 6.2, som i sin tur refererar till 6.1 med formuleringen “In addition to the high-risk AI systems referred to in paragraph 1”. Frågan är då, är det bara de AI-system som faller under 6.2 som syftas på i artikel 60 eller syftar man också på de system som faller under 6.1? Eftersom det är oklart vad som anses vara hög-risk AI enligt 6.1 är det därmed både oklart om 6.1 är en del av de system som refereras till i artikel 60 och vilka de systemen är i sådana fall.

Vi har offentliga aktörer i vårt nätverk som säger att de inte förstår definitionen och vad som utgör hög-risk i relation till AI och därför inte kan bedöma vad förslaget skulle få för effekt på deras verksamhet. Förslaget som det ligger verkar skapa mer förvirring än tydlighet om vad som regleras och vad det betyder för användarna av olika mjukvarusystem.

AI kräver annan reglering än mänsklig verksamhet

Definitionen i appendix I kommer nagelfaras i detalj av andra remissvar. Vi vill ändå lyfta två aspekter som vi ser som viktiga för att regleringen ska nå sitt avsedda syfte att öka medborgarnas tillit till tekniken. Den första aspekten är att en definition av AI som är otydlig eller inte motsvarar användarnas och/eller tillverkarnas syn kan leda till att man inte ser att regleringen gäller ens egen verksamhet eller att man inte tar regleringen på allvar eftersom den inte motsvarar den allmänna uppfattningen av vad AI är för teknologi. Att det inom EUs pågående arbete används olika definitioner av AI (se t.ex. [3]) gör det inte enklare att förstå vad AI är för nåt och vilka effekter av tekniken man vill reglera inom EU. Den andra aspekten är att mycket av det som faller under hög-risk AI enligt appendix III är okontroversiellt när det utförs av en människa. Det måste därför vara tydligt i regleringen varför det är riskabelt i sig att en AI utför en uppgift även om det skulle resultera i mer tillförlitlig och konsekvent verksamhet än om en människa utförde samma uppgift.

Artikel 5 listar aktiviteter som det är förbjudet att utföra med en AI. I artikel 5.1 nämns aktiviteter som redan idag är reglerade om de utförs av människor. Det är till exempel inte tillåtet att förvränga medborgares handlingar genom subliminala meddelanden så de skadar sig själva. Det är reglerat genom bland annat nationella regler för reklam, valpåverkan och den fria åsiktsbildningen. Frågan uppstår varför just de här verksamheterna behöver regleras igen

utifrån att de utförs av en AI? Är det för att det annars är oklart vem som är ansvarig för effekterna eller för att kunna utmäta andra konsekvenser vid överträdelser?

Innovationssystemet

Vi har fokuserat på hur olika verksamheter påverkas i och med om de faller under Old Approach Legislation (OAL) eller New Legislative Framework (NLF) samt regulatoriska sandlådor som en kompenserande åtgärd för att främja innovation.

Gamla och nya förfaringssätt

När det gäller produktsäkerhet och annex II utgår förslaget från två centrala begrepp – Old Approach Legislation (OAL) och New Legislative Framework (NLF). Enligt artikel 2.2 är produkter som regleras av EU-direktiv inom OAL, såsom UNECEs fordonstyper och det civila flyget, undantagna AI-regleringen och endast artikel 84 är tillämplig för dem. Däremot står inget i artikel 84 som reglerar vilket ansvar eller vilka rättigheter en tillverkare av sådana produkter har. Det är därför otydligt varför artikel 84 gäller för dessa produkter samt hur artikel 84 är tänkt att tillämpas.

Eftersom OAL inte berörs av AI-regleringen är det i dagsläget så att en produktutvecklare som har tillverkning inom både OAL och NLF kan välja att bedriva utveckling och forskning inom ett produktsegment för att undvika den regulatoriska börda som förslaget innebär. Det skulle kunna medföra att vi ser mer forskning och utveckling av AI-system inom fordonsbranschen istället för inom maskiner, trots att båda produkttyperna återfinns hos många aktörer inom EU. På så sätt gynnas en bransch i förhållande till en närliggande bransch genom förslaget.

OALs undantag från regleringen är explicit en tillfällig lösning. I Memorandum 1.2 och ingress-punkten (29) uttrycks en klar vilja att så fort det går få med de krav som förslaget innebär i kommande implementering eller delegerad reglering av de ursprungliga akterna.

EU har redan haft liknande processer för att inkorporera det generella produktansvaret [4] och Evidence Reporting Devices (tänk fordons motsvarighet till svarta lådor) i UNECEs arbete. EUs förfaringssätt har skapat spänningar i arbetet och flera parter har uttryckt att det kan vara enklare att bedriva forskning och utveckling utanför EU utifrån att regleringen skapar en osäker marknad. Ett exempel på det senare är hur man gick från att acceptera definitionen av svart låda såsom den används i USA till att iterativt införa ytterligare drygt 100 funktionella krav. Varje tillägg kan kräva en ny vända med avtal och förhandling mellan leverantörer och tillverkare, vilket driver kostnader och osäkerhet i utvecklingsarbetet. I tidigare införande av EU-regler har tidshorisonten varit en stötesten. Om vad som regleras och i vilken detalj det regleras ändras kontinuerligt och därmed de påverkade organisationerna måste anpassa sig mellan sina inplanerade inköpscykler blir kostnaderna stora när man vill följa regel-utvecklingen. Förslaget på reglering och hur det ska genomföras riskerar alltså att skapa ojämlika villkor för närliggande produktsegment, osäkerhet för de berörda aktörerna samt spänningar med andra internationella organisationer vars regler indirekt berörs.

Regulatoriska sandlådor

Förslaget tar upp att den ökade administrationen kring utvecklandet av AI-system som kan betecknas som utgöra hög risk kan missgynna små aktörer. Det är en bedömning vi också gör, framförallt som vi hört flera stora aktörer inom mjukvara och AI uttrycka att reglering är bra för det stabiliserar marknaden och gör det svårare för små aktörer att komma in med nya idéer. Kommissionens svar är att reglera hur regulatoriska sandlådor kan användas för att tillfälligt minska kraven på att små företag tar hela ansvaret för att all dokumentation finns på plats. I samarbete med nationella myndigheter kan istället en regulatorisk sandlåda skapas där myndigheten tar över en del av ansvaret. Hur det ska balanseras med andra uppdrag, såsom tillsyn av samma verksamhet, och få en harmoniserad tillämpning genom hela marknaden är inte specificerat. Från vårt perspektiv är det också osäkert om regulatoriska sandlådor har haft

en främjande effekt på innovationsklimatet och kan anses vara ett effektivt motmedel mot effekterna av ökad reglering.

Det finns andra vägar att gå för ett litet företag som bedriver utveckling av AI-system som anses utgöra en hög risk. Det kan vara möjligt att genom avtal skriva över rapporteringskraven på en större kund eller mottagare av systemet. Det skulle till exempel vara möjligt om utvecklaren gör affärer med ett multi-nationellt företag men skulle antagligen påverka ersättningen negativt. De mindre aktörerna skulle då behålla en direkt affär med sina parter utan att invänta en myndighets upprättande av en regulatorisk sandlåda och delaktighet i rapporteringen, men bli mer beroende av de större aktörerna som dominerar marknaden.

En annan väg framåt är att istället hänvisa till artikel 17.2 och att deras kvalitetssystem är i överensstämmelse med storleken på deras organisation. Är det en framkomlig väg behövs varken regulatoriska sandlådor och en förskjutning av förhandlingsutrymmet mellan aktörerna på marknaden där de större aktörerna gynnas på de mindres bekostnad kan undvikas.

Regulatoriska sandlådor ur ett myndighetsperspektiv tas upp i avsnittet Myndighetsutövning.

Ansvar i ett system-av-system

De system som används för att ta fram ett AI-system blir en del av dess produktionslina och/eller digitala innehåll (se t.ex. annex IV.2). Det får konsekvenser för vilken verksamhet som berörs av förslaget samt ställer frågor om deras ansvar.

Systemgräns

En utmaning med förslaget som det ligger är att system som utvecklas för andra ändamål än AI kan falla under regleringen om de används av andra för AI-utveckling. Rent konkret kan det röra sig om system som tillgängliggör data om aktuellt väglag [5] eller var utsläppspunkterna för avlopp ligger [6] och som sådana inte nödvändigtvis är hög-risk AI-system (eventuellt kan de vara AI-system i sig, beroende på hur definitionen i annex I tillämpas).

Om den data de tillhandahåller används för att träna eller testa ett AI-system skulle de vara en del av ett hög-risk AI-system eftersom hanterandet av vital infrastruktur täcks av annex III. Samma resonemang gäller också för utvecklare av digitala modeller, såsom digitala tvillingar, om de kan användas i eller av en AI som påverkar underhåll eller utveckling av infrastruktur. Ett annat exempel är tillhandahållare av befolkningsdata såsom beskattningsbar inkomst, antal folkbokförda på en adress eller prisutveckling på bostäder eftersom det kan användas för att beräkna försörjningsbidrag eller prioritera områden för särskilda satsningar (annex III.5 och III.8). Det blir alltså svårt för mjukvaruutvecklare och tillhandahållare av digitala resurser att veta om deras verktyg, tjänster och/eller produkter kommer ingå i en hög-risk AI framöver.

Samtidigt finns det en uttrycklig vilja att offentliga aktörer ska vara behjälpliga med att tillhandahålla data kring sin verksamhet och ett behov av förstudier och beslutsunderlag där simuleringar och statistiska modeller ingår. Här har vi två önskvärda trender som riskerar att hamna i konflikt med regleringen av AI såsom förslaget ligger.

Regleringens räckvidd

Det finns två konkreta exempel värda att beakta i relation till systemgränsen som utgår från etablerade kommersiella plattformar. Det första exemplet rör sociala plattformar med miljoner användare över hela världen och deras ansvar för spridandet av subliminala budskap. Det andra rör en plattform av samma storlek som i sitt erbjudande låter användare sprida och svara på jobbannonser.

I det första exemplet är det viktigt att spridandet av subliminala budskap ska regleras enligt förslaget ifall det görs genom användandet av en eller flera av de tre teknologier som listas i annex I. Det krävs inte att budskapet är framtaget av en AI, det kan vara en människa som av egen fri vilja författat det och i linje med fri åsiktsbildning sprider det, men vilka budskapet når

och på vilka grunder kan vara verket av en AI. Beroende på hur regleringen ska tillämpas skulle plattformen då kunna vara en förbjuden verksamhet för att den sprider folks åsikter.

I det andra exemplet är användandet av AI för att sprida jobbannonser eller välja ut vilka som ska få erbjudandet att betrakta som en hög-risk verksamhet när det utförs av en AI. Saknas då vederbörlig dokumentation och listning i kommissionens databas ska tillgängliggöraren av plattformen bötfällas.

Båda plattformarna är exempel på digitala tjänster EUs medborgare använder i sin vardag. Utifrån förslaget står då plattformsleverantörerna inför ett val. De kan anpassa sitt erbjudande så det blir lagligt och inte anses utgöra en hög risk enligt förslaget på AI-reglering, med risk för att tappa användare. De kan också välja att bestrida sitt ansvar för att testa i vilken utsträckning regleringen faktiskt går att tillämpa.

Avtal

Ett sätt för olika aktörer att avskriva sig ansvar för vad andra gör med deras digitala resurser är genom licenser och avtal. I vilken utsträckning de faktiskt kommer att gälla när regleringen tillämpas är ovisst. Det kan också få en hämmande effekt på viljan att använda resursen eftersom det kommer tillföra ytterligare reglering av hur och när den får användas. Risken är att organisationer blir mer försiktiga i hanterandet av samtliga digitala resurser för att försäkra sig om att inte hamna i en framtida situation där deras verksamhet ingår i vad kommissionen betecknar som ett hög-risk AI-system.

Kan man som underleverantör friskriva sig all inblandning i framtida utveckling som kan falla under beteckningen hög-risk AI? Kommer motparten gå med på det? Mycket av handlings-utrymmet kommer bestämmas av hur beroende parterna är av varandra om inget annat sägs. Då gynnas de starkare aktörerna på marknaden av förslaget.

Som anställd är det också relevant att veta i vilken utsträckning man är ansvarig för organisationens verksamhet och om den kan regleras genom anställningsavtal. Annex IV.3.g nämner att samtliga testloggar ska vara signerade av de som är ansvariga. Ansvariga för vad nämns inte; är det testet, AI-systemet eller organisationen? I vilken utsträckning kan en enskild anställd ta ett sådant ansvar och se konsekvenserna av sitt agerande utifrån organisationen och systemet som helhet?

Myndighetsutövning

Regleringen omfattar leverantörer och användare. En fråga är vad som gäller för till exempel aktörer inom offentlig sektor som användare av AI-system? Har de några skyldigheter?

Digitalisering

Går vi över till att sätta fokus på uppgifter som omfattar handläggning och beslut, behöver analysen omfatta att vad som ibland kallas “rules as code” är ett växande område inom offentlig förvaltning [7]. Målsättningen är här att automatisera repetitiva och enkla uppgifter för att frigöra personal till mer krävande uppgifter. Med den nuvarande definitionen av AI samt de områden som listas som hög risk för AI i annex III skulle exempelvis beräknande av ersättning vid vård av barn eller socialbidrag, rätt till bostadsbidrag och hanteringen av trängselskatt utgöra hög-risk AI-system och certifieras samt rapporteras till EUs centrala databas.

AI-system som används i verksamhet (”något av de områden”) som finns med i bilaga III är per definition AI-system med hög risk. För sådana system finns krav på bl.a. mänsklig tillsyn, certifiering och på att uppgifter om sådana AI-system ska vara registrerade i en kommissionens EU-databas om sådana. Områden som t.ex. utbildning, sysselsättning och tillgång till grundläggande privata och offentliga tjänster ingår i bilaga III. Det betyder att digitalisering inom sådan verksamhet kan behöva ta hänsyn till reglerna. En del av digitaliseringen av

offentlig sektor är en ökad möjlighet till dels digitalt informationsflöde mellan organisationer dels beslutsstöd i verksamheten.

Ett av områdena i bilaga III är rättskipning och demokratiska processer. Idag används databaser, som t.ex. Eurlex och olika företags databaser med bl.a. rättspraxis, av personal inom domstolarna för att hitta relevanta rättsfall. Det förekommer även att man använder andra sökverktyg för att hitta relevanta fall. Enligt vår tolkning av förslaget så skulle de nämnda rättsdatabasernas allmänt tillgängliga sökmotorer anses vara hög-risk AI-system när de används för att hitta relevanta rättsfall. Används dessutom populära sökmotorer och webbläsare av myndighetspersoner för att hitta regelverk faller även de systemen under definitionen av hög-risk AI.

Regulatoriska sandlådor

Artikel 3.43 anger att ”national competent authority” ska ansvara för tillsyn, anmälan samt marknadskontroll. Det är inte orimligt att det är olika nationella myndigheter som ansvarar för de olika uppdragen, på så sätt att en myndighet har ansvaret för tillsyn och anmälan medan den myndighet som redan har ansvar för ett direktiv fortsätter att ha det. Det betyder att t.ex. skulle Arbetsmiljöverket ansvara för marknadskontroll av maskiner, samt de AI-system som återfinns i dessa, istället för att Arbetsmiljöverket ansvarar för marknadskontroll av maskiner och en annan myndighet av de berörda AI-systemen. Risken är samtidigt att det sker en fragmentering så att olika myndigheter på nationell nivå gör olika tolkningar av sitt uppdrag och att marknadskontrollen av maskiner resulterar i andra krav på dokumentation av AI-system än vad som gäller för radioutrustning eller medicinsk apparatur.

Eftersom det är ”competent authorities” som får inrätta sandlådor är det också viktigt att man för varje direktiv och verksamhet är överens om vilken myndighet som får inrätta sandlådor för just den produkten eller verksamheten. Här finns också en utmaning i att det hittills har varit riksdagen som besluter om försöksverksamhet genom t.ex. en tidsbegränsad lag, vilket kan delegeras till myndighet genom en förordning. Nu ger EU den rätten till myndigheten istället, utan att be riksdagen om lov (artikel 53).

Övrigt

Vi har identifierat två aspekter som faller utanför våra teman men som ändå är värda att lyfta upp, CE-märkningen och avsaknaden av en definition av ”stand-alone” AI-system.

Artikel 16.1 anger att den som tillgängliggör ett hög-risk AI-system ska placera CE-märket på systemet för att visa att det överensstämmer med direktivet enligt artikel 49. Om det inte går att placera på själva systemet på grund av dess natur ska märket placeras på förpackningen eller den medföljande dokumentationen. Det förutsätter att dokumentationen följer med systemet oavsett hur det tillgängliggörs på marknaden. Om märket ska få samma effekt som för fysiska produkter, det vill säga vara synligt varje gång man interagerar med produkten, kommer användarna vara tvungna att gå via systemets dokumentation för att komma åt systemets funktionalitet, vilket kan få en effekt på användarupplevelsen. Effekten kommer variera beroende på vilka system som anses utgöra hög risk, men om plattformar för professionellas nätverkande och populära sökmotorer är att se som hög-risk AI kan det skapa frustration istället för tillit bland medborgarna.

Det är dessutom inte tydligt för medborgare om en CE-märkt maskin är det utifrån att den innehåller en hög-risk AI eller inte. Den kan lika väl vara CE-märkt som maskin. Eller för att den faller under radio-direktivet. Att produkten är CE-märkt kommer därför inte med automatik skapa tilltro till dess AI, eller öka medborgarnas tilltro till AI som teknologi.

Begreppet ”stand-alone” i relation till AI-system definieras inte i Artikel 3. Det är ett centralt begrepp, på samma sätt som ”safety component of a product or system”, för förståelse av vad regleringen kommer omfatta och bör därför få sin egen definition.

Den större bilden

Avslutningsvis, det är svårt att ta ställning till förslaget om reglering av AI-system i sig. Förslaget relaterar till en rad antagna regleringar rörande digitalisering, bland annat cyber-säkerhet [7], individers digitala integritet [8] och öppen data [9] som i sig är omfattande i innehåll och detaljer. Att se helheten av det liggande förslaget i relation till de reglerna tar tid. Förslaget relaterar också, explicit och implicit, till andra pågående initiativ som inte är antagna regleringar än. Exempel på sådana förslag är reglering av digitala tjänster [10], data governance [11], plattformar [12] och robotar [13]. Utifrån att de förslagen kan förändras innan de blir antagna finns det en osäkerhet kring hur helheten i form av reglering kommer se ut. Till det kommer att direktiven i annex II är under omarbetning och att till exempel förslaget på nytt maskindirektiv, i formen av förordning, kommer omfatta mjukvaran i maskinen, inklusive AI-system, och dess uppdateringar [14]. Om det förslaget också går igenom blir samtliga AI-system som används i maskiners säkerhetskomponenter klassade som hög-risk och därmed reglerade av AI-förordningen. Sammantaget blir uppgiften att granska ett enskilt förslag en komplex uppgift med beroenden till både existerande och föreslagna regler.

Det är därför svårt att se hur förslaget på AI-reglering kommer påverka innovationsklimatet eller vilken effekt det kommer få på forskning och utveckling inom den gemensamma marknaden i sig. Detsamma gäller för kommissionens växande inflytande när det är där definitionerna kommer att hanteras. Den gemensamma marknaden kommer få olika spelregler beroende på om AI inom jordbruket anses vara en hög-risk-aktivitet framöver eller om fördelning av sjukvård och omsorg inkluderas i annex III. Enligt förslaget ska det vara kommissionens fråga att hantera. Om de andra förslagen går i samma riktning kan de resultera i en de facto överflyttning av makt från parlamentet till kommissionen i centrala frågor för den gemensamma marknaden.

Sammanfattningsvis

Förslaget till reglering av AI syftar till att öka medborgarnas tillit till AI som teknologi. Som ansats har vi inga invändningar till syftet. Däremot ser vi en rad risker med förslaget som det ligger. För det första, en otydlighet i vad som regleras, varför det regleras samt hur det påverkar medborgare, företag och offentliga institutioner riskerar att påverka tilliten till regleringen, istället för teknologin. För det andra, regleringen riskerar att påverka förutsättningarna på marknaden olika, dels mellan produktsegment, dels genom att gynna etablerade aktörer på bekostnad av nya initiativ samtidigt som det skapar osäkerhet i relation till investeringar och innovation.

Referenser

[1] 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 COM/2021/206 final

[2] Garske B, Bau A, Ekardt F. Digitalization and AI in European Agriculture: A Strategy for Achieving Climate and Biodiversity Targets? *Sustainability*. 2021; 13(9):4652. https://doi.org/10.3390/su13094652

[3] High-Level Expert Group on Artificial Intelligence, A Definition of AI: Main Capabilities and Disciplines, Apr. 8, 2019

[4] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety

[5] Trafikverket, API, https://api.trafikinfo.trafikverket.se/API/Model

[6] Naturvårdsverket, Avloppsreningsanläggningens utsläppspunkter - utsläppspunkter av avloppsvatten (Urban Waste Water Directive, 91/271/EEG), https://oppnadata.naturvardsverket.se/dataportal-details.html#esc_entry=10563&esc_context=69&esc_-org=http%3A%2F%2Fdataportal.se%2Forganisation%2FSE2021001975

[7] Mohun, J. and A. Roberts (2020), "Cracking the code: Rulemaking for humans and machines", OECD Working Papers on Public Governance, No. 42, OECD Publishing, Paris, https://doi.org/10.1787/3afe6ba5-en.

[8] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) PE/86/2018/REV/1

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

[10] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information PE/28/2019/REV/1

[11] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final.

[12] Proposal for a Regulation on European data governance (Data Governance Act) COM/2020/767

[13] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 final

[14] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

[15] European Commission, Proposal for a Regulation of the European Parliament and of the Council on machinery products, COM(2021)202, 21 April 2021