FOI
Totalförsvarets forskningsinstitut

Vid korrespondens åberopa
FOI beteckning

Datum
2021-07-07

Nr FOI-2021-795:4

Infrastrukturdepartementet

Er referens
I2021/01304

Vår handläggare
Joel Brynielsson

Remissvar gällande Europeiska kommissionens förslag till förordning om harmoniserade regler för artificiell intelligens

Sammanfattning av FOI:s synpunkter

Totalförsvarets forskningsinstitut (FOI) avstyrker förslaget till EU-förordning om harmoniserade regler för artificiell intelligens, särskilt vad avser tillämplighet för nationell säkerhet och brottsbekämpande verksamhet.

Vidare avstyrker FOI reglering utgående från en uppsättning namngivna teknologier och förordar i stället reglering utgående från principen om teknikneutralitet.

FOI menar att det är svårt att avgöra omfattningen av vilka AI-system som ska omfattas av förordningen.

Enligt FOI:s bedömning är det även oklart hur forskning ska hanteras enligt förordningen och i vilken mån FOI:s verksamhet omfattas av regleringen.

Förslaget till AI-förordning behöver också i större omfattning anpassas till befintliga immaterialrättsliga regler och principer samt pågående lagstiftningsarbeten på det immaterialrättsliga området.

FOI lämnar härutöver nedanstående synpunkter och kommentarer på förslaget till förordning.

Förordningens tillämpningsområde

Enligt artikel 4.2 i Fördraget om Europeiska unionen är den nationella säkerheten varje medlemsstats eget ansvar. Frågor om nationell säkerhet utgör följaktligen en angelägenhet för medlemsstaterna själva. Av artikel 2.3 i den föreslagna förordningen framgår att endast ”utveckling och användning av artificiell intelligens för rent militära

Postadress
FOI
164 90 STOCKHOLM

Besöksadress
Gullfossgatan 6, Kista
Leveransadress
Gullfossgatan 12, Kista

Telefon
08-55 50 30 00

Fax

registrator@foi.se

Orgnr: 202100-5182
www.foi.se

ändamål”[1] undantas från förordningens tillämpningsområde, dvs. ett betydligt snävare område än ”nationell säkerhet”. FOI konstaterar därför att Kommissionen väljer att reglera inom ett område som inte omfattas av unionsrätten utan som tillhör medlemsstaternas lagstiftningsområde. Det är enligt FOI:s mening inte lämpligt att EU genom en förordning reglerar ett område som undantas från EU:s lagstiftningsområde i fördraget.

Visserligen kan ett medlemsland utvidga EU-rättens tillämpningsområde till att omfatta även verksamheter som faller utanför EU-rätten i de fall en sådan lösning bedöms vara lämplig. Det måste dock vara upp till varje enskilt medlemsland att bestämma huruvida unionsrättens tillämpning ska utvidgas på sådant sätt.

FOI kan vidare konstatera att utveckling inom området brottsbekämpande verksamhet kan komma att påverkas negativt av förslaget. Brottsbekämpande verksamhet är av sådant slag att den bör särregleras, precis som är fallet med personuppgifter och brottsdatadirektivet.[2] FOI anser därför att utöver nationell säkerhet även brottsbekämpande verksamhet bör undantas från förordningens tillämpningsområde.

Teknikneutralitet

FOI har i uppdrag att bedriva forskning samt metod- och teknikutveckling inom bland annat maskininlärning. FOI har noterat att det skett ett tekniksprång där utvecklingen inom maskininlärningsområdet gjort det möjligt att utveckla nya typer av intelligenta system, och instämmer därför i att behov av reglering föreligger.

FOI menar dock att sådan reglering bör vara teknikneutral. Att som i artikel 3.1 och Annex I definiera AI i termer av ”statistiska metoder, […], sökning och optimering” skulle göra att nästan alla datorprogram definieras som AI-system i enlighet med artikel 3. Om i stället ”statistiska metoder, […], sökning och optimering” tas bort från AI-definitionen så blir definitionen för smal och kan kringgås. En framtida reglering bör därför fokusera på den faktiska informationshanteringen och den utdata som ett system ger upphov till snarare än att lista specifika tekniker.

Ett exempel kan belysa problematiken med att reglera tekniska lösningar i stället för resultatet. Den föreslagna förordningen reglerar bland annat så kallad ”AI-based social scoring”. Social scoring handlar om poängsättning av personer utgående från beteende, och skulle exempelvis kunna användas för att poängsätta medborgare baserat på deras digitala fotspår på sociala medier som grund för att tilldela förmåner. Detta är ett område som behöver regleras, men den föreslagna förordningen lämnar öppet för att utföra ej AI-

[1] Artikel 2.3: ”This regulation shall not apply to AI systems developed or used exclusively for military purposes.”
[2] Direktiv (2016/680) av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

baserad social scoring, dvs. det är social scoring som behöver regleras och detta helt oavsett med vilken teknik som social scoring utförs.

Möjligheten att genom delegation ändra förordningen

Artiklarna innebär en delegation till Kommissionen att under vissa omständigheter komplettera bilagorna Annex I (Tekniker och tillvägagångssätt för artificiell intelligens) och Annex III (AI-system som betecknas som högrisk).

Mot bakgrund av vad som sagts ovan om att EU enligt förslaget till förordning i strid mot Fördraget om Europeiska unionen reglerar på medlemsstaternas lagstiftningsområde när det gäller ”nationell säkerhet”, är det inte rimligt att dessutom ge Kommissionen rätt att självständigt besluta om tillägg till (men inte ta bort) vad som ska anses vara ”AI-system som betecknas som högrisk” enligt Annex III. En sådan befogenhet för Kommissionen skulle innebära att medlemsstaterna helt förlorar kontrollen över området ”nationell säkerhet”, till EU-organ.

Kommissionen kommer för övrigt inte att ha den närhet, kunskap och förståelse som krävs för att i varje läge och vid rätt tidpunkt på ett riskbaserat sätt kunna bedöma vilka åtgärder som behövs för att kunna fatta adekvata beslut i frågan om tillägg till bilagorna. Den föreslagna ordningen verkar dessutom byråkratisk och tungrodd, och sammantaget befarar FOI att processen skulle hämma den snabba utveckling inom AI som Kommissionen samtidigt säger sig vilja gynna.

AI-system som omfattas av förordningen

FOI menar att det är svårt att avgöra omfattningen av vilka AI-system som ska omfattas av förordningen.

Förordningstexten nämner att förordningen ska tillämpas avseende ”leverantörer som släpper ut AI-system på marknaden eller tar sådana i bruk”.[3] Definitionerna i Article 3 (punkterna 8–11) förtydligar begreppen ytterligare.

De åtgärder som krävs för ”AI-system som betecknas som högrisk” är omfattande och kräver stora resurser, och överlag ger förordningstexten intryck av att omfatta stora färdigutvecklade AI-system. Enligt FOI uppvisar inte alla AI-system denna komplexitet och mognad även om de skulle kunna betecknas som ”högrisk”. Många AI-system är betydligt enklare. Ett systems påverkan på enskildas grundläggande rättigheter behöver inte ha med resurser att göra. FOI ser följaktligen svårigheten att tydligt definiera vilka AI-system som är tänkta att omfattas av regleringen.

[3] Artikel 1 a: ”[…] providers placing on the market or putting into service AI systems in the Union […]”.

Kommer förordningen omfatta FOI:s verksamhet?

FOI menar att det är svårt att avgöra om förordningen omfattar FOI:s uppdrag och verksamhet med forskning, metod och teknikutveckling för olika uppdragsgivare.

Som nämnts ovan anges i förordningstexten att förordningen ska tillämpas avseende ”leverantörer som släpper ut AI-system på marknaden eller tar sådana i bruk”. FOI:s uppdrag tycks vid en strikt tolkning inte omfattas av förordningen då FOI utvecklar och testar metoder och teknik för sina i huvudsak offentliga uppdragsgivare. FOI släpper som regel emellertid inte ut produkter på marknader eller tar AI-system i bruk. Däremot har FOI till uppdrag att sprida sin kunskap och möjliggöra för andra att kommersialisera idéer. Utförandet av uppdrag kan också medföra att produkter kan komma att tas i bruk av uppdragsgivaren i ett senare skede (jfr utförandet av ett uppdrag åt polisen). FOI finner följaktligen det oklart i vilken mån förordningen omfattar FOI:s verksamhet.

Om det är så att förordningen ska tillämpas på FOI:s verksamhet verkar det som att förordningen kan komma att begränsa FOI:s möjligheter att utföra uppdrag. Det kan t.ex. gälla uppdrag från brottsutredande myndigheter som verkar kunna omfattas av den förbjudna listan (Annex III). Likaså tycks FOI:s uppdrag kunna omfatta AI-system som finns på listan för ”AI-system som kan betraktas som högrisk”.

Kommissionens lista avseende AI-system som kan betraktas som högrisk (Annex III) förefaller vara alltför snäv och begränsande i ljuset av att samhället rimligen måste få utveckla och använda metoder för att upptäcka och skydda sig mot t.ex. brottslig verksamhet, gränsöverskridande kriminalitet och krafter som har till syfte att kullkasta demokratins fundament. Det bör beaktas att en hög brottslighet i sig också är ett hot mot enskildas fri- och rättigheter.

Forskning

FOI menar att det är oklart hur forskning ska hanteras enligt förordningen. Forskning är till sin natur i framkant och föregår annan användning och kan därför uppfattas som offensiv ur förordningens synvinkel. Samtidigt är forskning i många fall en förutsättning för utveckling. Vidare saknas ofta många av de problem som en reell AI-användning i framkant kan medföra. Exempelvis kan forskning ofta utföras på testdata och i avskilda testmiljöer utan att t.ex. enskildas integritet sätts på spel. Det är därför enligt FOI:s mening av vikt att forskning behandlas fördelaktigt enligt förordningen, om förordningen nu ens ska tillämpas på forskning.

Av skäl 16 till den föreslagna förordningen framgår angående vissa förbjudna AI-system att ”[…] 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.”

Enligt FOI:s mening borde detta viktiga ställningstagande till fördel för forskning tydligt framgå av en artikel i förordningstexten i stället för enbart i skälen till densamma. FOI vill i det sammanhanget också påpeka att det i Sverige redan finns nationella bestämmelser om etikprövning[4] till skydd för människor i forskning, som den föreslagna regleringen kan komma att stå i strid med.

Immateriella rättigheter

Den 17 april 2019 antog EU det nya upphovsrättsdirektivet[5] som inom EU ofta kallas för DSM-direktivet (Digital Single Market). Direktivet ska vara genomfört i medlemsstaterna den 7 juni 2021. Artikel 3 i direktivet har rubriken ”Text- och datautvinning för forskningsändamål”. Enligt artikel 3.1 ska medlemsstaterna föreskriva ett undantag från de rättigheter som fastställs i tidigare direktiv om upphovsrätt för mångfaldigande och utdrag som forskningsorganisationer och kulturarvsinstitutioner genomför för forskningsändamål i syfte att utföra text- och datautvinning av verk eller andra alster som de har laglig tillgång till.

Definitionen av text- och datautvinning återfinns i artikel 2.2: ”automatiserad analysteknik som används för att analysera text och data i digital form för att generera information, inklusive, men inte begränsat till, mönster, trender och samband”.

För ett forskningsinstitut som FOI är undantaget i artikel 3.1 i ovanstående direktiv mycket viktigt. FOI förstår det som att den automatiserade analysteknik som avses innefattar användande av AI. FOI befarar att förslaget till AI-förordning inskränker FOI:s möjlighet att använda sig av forskningsundantaget i DSM-direktivet och därmed av AI i forskningen. FOI vill därför be regeringen att uppmärksamma och värna denna viktiga reglering i samband med utformningen av AI-förordningen.

Regeringen har i december 2020 skickat följande förslag på remiss: Ds 2020:26 Bättre skydd för tekniska företagshemligheter. Förslaget tar bland annat sikte på ändringar i lagen (2018:558) om företagshemligheter, som tillkom som ett led vid genomförandet av ett direktiv med EU-gemensamma regler om skydd för företagshemligheter (Direktiv 2016/943). Skyddet för företagshemligheter har bedömts vara av central betydelse för innovationskraften på såväl EU-nivå som nationell nivå.

Under avsnitt 3.5 (Explanatory memorandum) i förslaget till AI-förordning uppmärksammas att de föreslagna skyldigheterna om transparens kommer att ha påverkan på immateriella rättigheter. Vidare utlovas att ovan nämnda direktiv (2016/943) om skydd för företagshemligheter ska följas och att myndigheter som behöver ta del av konfidentiell information och källkod ska ha skyldigheter rörande konfidentialitet. Den här informationen under avsnitt 3.5 är mycket viktig och borde därför även regleras i en artikel i förordningstexten i förslaget till AI-förordning och inte enbart i Explanatory memorandum.

---

[4] Lagen (2003:460) om etikprövning av forskning som avser människor.
[5] Direktiv 2019/790 om upphovsrätt och närstående rättigheter på den digitala inre marknaden.

Sammanfattningsvis behöver förslaget till AI-förordning i större omfattning anpassas till befintliga immaterialrättsliga regler och principer samt pågående lagstiftningsarbeten på det immaterialrättsliga området.

Allmänt om uppbyggnaden av förordningen, krav på systemadministration, anmälan av AI-system, ansvariga myndigheter, dokumentation osv.

Förordningen föreskriver en mycket omfattande byråkrati kring administration av AI-system, utpekande av och uppbyggnad av övervakande myndigheter på nationell nivå och EU-nivå, när det gäller framför allt ”AI-system som kan betraktas som högrisk”.

FOI konstaterar att Kommissionen valt en annan väg än man gjort med den förhållandevis framgångsrika dataskyddsförordningen (GDPR) där större ansvar ligger på den enskilde (egenansvar och egenkontroll) än på uppbyggnad av och rapportering till register med behandlingar hos separata organ. Det hade varit till fördel om den föreslagna förordningen till större del utformats på liknande sätt som en ramförordning med egenkontroll, vilket hade medfört en smidigare och mer ändamålsenlig tillämpning. Förslaget föreskriver detaljerade åtgärder och ger ett tungrott och byråkratiskt intryck. Av allt att döma kommer förslaget snarare att hämma utveckling och tillväxt än gynna sådan.

En annan hämmande faktor är att regulatoriska krav, kraven på dokumentation och regelkunskap med mera kommer att öka kostnaderna för AI. En överhängande farhåga är att svenska organisationer med begränsade resurser inte kommer att mäkta med att uppfylla alla krav med följden att viktiga uppgifter för samhällets säkerhet och utveckling inte utförs.

FOI
Totalförsvarets forskningsinstitut

Datum
2021-07-07

Nr FOI-2021-795:4

Detta remissvar har beslutats av tjänsteförrättande generaldirektör Maria Lignell Jakobsson efter föredragning av forskningschef Joel Brynielsson. I den slutliga handläggningen har även forskningsledare Fredrik Johansson, jurist Åsa Berglund och särskild rådgivare Mikael Wiklund deltagit.

…….
Maria Lignell Jakobsson

……..
Joel Brynielsson

Sändlista:
Infrastrukturdepartementet

För kännedom
Försvarsdepartementet

Internt FOI
Registrator
GD-sekreterare
Särskild rådgivare
Chefsjurist
AC