

Tjänsteutlåtande

Datum 2021-06-10

Diarienummer SU 2021-02647

Västra Götalandsregionen

Sahlgrenska Universitetssjukhuset

Handläggare: Anders Hyltander

E-post: anders.hyltander@vgregion.se

Till styrelsen för Sahlgrenska Universitetssjukhuset

Svar på remiss av Europeiska kommissionens förslag till förordning om harmoniserade regler för artificiell intelligens

Förslag till beslut

1. Styrelsen för Sahlgrenska Universitetssjukhuset antar tjänsteutlåtandet att utgöra svar på remiss - Europeiska kommissionens förslag till förordning om harmoniserade regler för artificiell intelligens.
2. Paragrafen justeras omedelbart.

Sammanfattning av ärendet

Förslaget från EU kommissionen innehåller nya regler och åtgärder som syftar till att göra EU till ett centrum för utveckling och användning av pålitlig och säker artificiell intelligens (AI). Målsättningen är att definiera den rättsliga ramen för AI som skall gälla för samtliga medlemsstater och branscher. Exempel på branscher där applikationer av AI kommer att kunna utnyttjas är inom industri generellt, inom hälso – och sjukvård, inom transport, energi, jordbruk och turism samt cybersäkerhet. Detta för att garantera säkerhet och grundläggande rättigheter för människor och företag, samtidigt som AI utveckling med åtföljande investeringar och innovation stärks i hela EU.

Ambitionen är även att sätta standarder för att därigenom bana väg för etisk AI utveckling och användande globalt.

Utveckling av AI innebär dock ett antal risker och förslaget från Kommissionen innehåller därför förslag till mycket omfattande och detaljerad reglering framför allt av det som definieras som ”hög-risk” AI, se nedan. Det kan noteras att utveckling av AI för militärt bruk inte berörs i förslaget.

De nya reglerna kommer att tillämpas på likartat sätt i alla medlemsstater baserat på en gemensam definition av AI och de följer en riskbaserad strategi.

Sahlgrenska Universitetssjukhuset (SU) har bland annat följande synpunkter.

Hela detta regelverk ställer omfattande krav på uppföljning och kontroll på såväl nationell – som på EU nivå. Detta innebär för SUs del att i takt med att fler AI-baserade tekniker kommer i allmänt bruk måste resurser och kompetens finnas tillgängliga för kontroll och uppföljning av regelverk och system samt för rapportering till berörd myndighet på nationell nivå.

Eftersom regelverket är omfattande, strikt och komplext är frågan om processtid och kostnader relaterade till granskning, validering och formella godkännanden av framför allt hög risk AI-system central. Det finns en inte helt obefogad oro för att dessa processer kan bli både mycket kostsamma och ta lång tid i anspråk. Vad detta kan komma att betyda för innovationskraft, kreativitet, utveckling och tillgänglighet för marknaden återstår att se. Önskvärt vore att förslaget även innehöll en klausul gällande maximal tid för en dylik process.

Fördjupad beskrivning av ärendet

Oacceptabel risk

AI-system som anses vara ett tydligt hot mot människors säkerhet, försörjning och rättigheter kommer att förbjudas. Detta inkluderar AI-system eller applikationer som manipulerar mänskligt beteende för att kringgå användarnas fria vilja (till exempel leksaker som använder rösthjälp som uppmuntrar farligt beteende hos minderåriga) och system som tillåter regeringar att utnyttja AI för social poängsättning av medborgare.

Högrisk

AI-system som identifierats som högrisk inkluderar AI-teknik som används i:

- Kritisk infrastruktur (till exempel transport) som kan äventyra medborgarnas liv och hälsa.
- Utbildnings- eller yrkesutbildning, som kan avgöra tillgången till utbildning och yrkesmässig kurs i någons liv (till exempel poängsättning);
- Säkerhetskomponenter i produkter (till exempel AI-applikation vid robotassisterad kirurgi);
- Anställning, ledning av arbetstagare och tillgång till egenföretagare (till exempel CV-sorteringsprogramvara för rekryteringsförfaranden);
- Väsentliga privata och offentliga tjänster (till exempel kreditvärdighet som förnekar medborgarnas möjlighet att få ett lån).
- Brottsbekämpning som kan störa människors grundläggande rättigheter (till exempel utvärdering av bevisens tillförlitlighet);
- Hantering av migration, asyl och gränskontroll (till exempel verifiering av resehandlingars äkthet);
- Rättskipning och demokratiska processer (till exempel tillämpa lagen på en konkret uppsättning fakta).

Man föreslår vidare att högrisk AI-system ska omfattas av strikta skyldigheter innebärande omfattande testningar och valideringar innan de kan släppas ut på marknaden. Detta gäller såväl internt utvecklade system som algoritmer skapade av tredje part utanför EU. Exempel på krav är att säkerställa tillgång till följande:

- Lämpliga system för riskbedömning och begränsning.
- Hög kvalitet på de datamängder som matar systemet för att minimera risker och diskriminerande resultat.
- Loggning av aktivitet för att säkerställa spårbarhet av resultat;
- Detaljerad dokumentation som ger all information som behövs om systemet och dess syfte för myndigheterna att bedöma dess efterlevnad.
- Tydlig och adekvat information till användaren;
- Lämpliga mänskliga tillsynsåtgärder för att minimera riskerna.
- Hög robusthet, säkerhet och noggrannhet.
- CE märkning som möjliggör användande bland samtliga EU:s medlemsstater.
- Fysiska personer bör underrättas om att de interagerar med ett AI-system, såvida inte detta är uppenbart av omständigheterna och användningssammanhanget. Dessutom bör fysiska personer meddelas när de utsätts för ett känslomedkännande system eller ett biometriskt kategoriseringssystem. Sådan information och anmälningar bör tillhandahållas i tillgängliga format för personer med funktionsnedsättning.
- Användare, som använder ett AI-system för att generera eller manipulera bild-, ljud- eller videoinnehåll som märkbart liknar befintliga personer, platser eller händelser och som falskt verkar för en person vara äkta, skall avslöja att innehållet har skapats eller manipulerats artificiellt. Enom att märka den artificiella intelligensprodukten i enlighet därmed och avslöja dess artificiella ursprung.

I synnerhet anses alla biometriska identifieringssystem vara höga risker och ska därför underkastas mycket strikta krav. Utnyttjande av dessa i allmänt tillgängliga utrymmen för brottsbekämpning är i princip förbjudet. Undantag från denna generella regel är strikt definierade och reglerade (till exempel där det är strikt nödvändigt för att söka efter saknade barn, för att förhindra ett specifikt och överhängande terroristhot eller för att upptäcka, lokalisera, identifiera eller åtala en gärningsmän eller misstänkt för ett allvarligt brott). Sådan användning är föremål för tillstånd från ett rättsligt eller annat oberoende organ och för lämpliga tidsbegränsningar, geografisk räckvidd och de databaser som söks.

Ännu ett undantag från detta regelverk är att under vissa förhållanden kan snabb tillgång på innovativ teknik vara avgörande för människors hälsa och säkerhet och för samhället som helhet. Det är således lämpligt att av exceptionella skäl för allmän säkerhet eller skydd av naturens liv och hälsa för enskilda personer och

skyddet av industriell och kommersiell egendom, medlemsstaterna skulle kunna tillåta utsläppande på marknaden eller ibruktagande av AI-system som inte har hunnit genomgå en bedömning av överensstämmelse med det föreslagna regelverket.

Begränsad risk, dvs. AI-system med specifika krav på transparens:

När AI-system till exempel som chatbots används, bör användarna vara medvetna om att de interagerar med en maskin så att de kan fatta ett välgrundat beslut om att fortsätta eller gå tillbaka.

Minimal risk: Enligt förslaget tillåter fri användning av applikationer såsom AI-aktiverade videospel eller skräppostfilter. Många AI-system faller således inom denna kategori eftersom dessa system bedöms endast utgöra minimal eller ingen risk för medborgarnas rättigheter eller säkerhet.

När det gäller styrning föreslår kommissionen att nationella behöriga kontrollmyndigheter tillskapas med tillgänglighet dygnet runt som övervakar de nya reglerna och som kan konsulteras i de fall gränsdragningar kan behöva göras snabbt. Förslaget innehåller även inrättandet av ett Europeiskt styrorgan för Artificiell Intelligens, European Artificial Intelligence Board, vars uppgifter bland annat är att övervaka tillämpningar av regelverken, underlätta genomförandet av dessa, driva utvecklingen av standarder för AI inom EU och fatta beslut om risknivåer för AI-system vilket även innefattar förbud om dessa system bedöms innebära en oacceptabel risk enligt definition ovan.

Nästa steg efter att samtliga remissinstanser inkommit med yttranden blir att Europaparlamentet och medlemsstaterna kommer att behöva anta kommissionens slutgiltiga förslag om en europeisk strategi för artificiell intelligens i det ordinarie lagstiftningsförfarandet. När detta antagits kommer förordningarna att vara direkt tillämpliga i hela EU. Parallellt kommer kommissionen att fortsätta att samarbeta med medlemsstaterna för att genomföra de åtgärder som meddelats i den samordnade planen.

Allmänna kommentarer

Eventuell reglering av de stora tech-bolagens algoritmer och AI-system berörs inte alls i förslaget. Man kan dock notera att delar av det som definierats som högrisk AI system finns redan i olika kommersiellt tillämpade produkter från till exempel Google och Facebook och det blir en strategiskt viktig fråga hur dessa system skall kunna regleras.

Förslaget stipulerar att leverantörer och användare av högrisk-AI-system följer reglerna för data och datastyrning. Dokumentation och arkivering; öppenhet och tillhandahållande av information till användare; mänsklig tillsyn; och robusthet, noggrannhet och säkerhet. En viktig nyhet som presenterades i den EU-vitbok om artificiell intelligens som publicerades 2020, är ett krav på förhandsbedömningar

för att fastställa att högrisk AI-system uppfyller dessa krav innan de kan erbjudas på marknaden eller tas i bruk. En ytterligare viktig regel är befogenheter för-och skapande av en struktur för övervakning av marknaden för att upptäcka problem med AI tillämpningar som redan tagits i bruk i syfte att korrigera dessa.

En oklarhet är om och hur gjorda bedömningar vid behov även skall kunna granskas av allmänheten eller nationell tillsynsmyndighet.

Likväl är förslaget en omfattande start på lagstiftningsprocessen i Europa och kan ha potential för en synkronisering av regelverk även med andra marknader och nationer utanför EU.

AI-system som orsakar eller sannolikt kommer att orsaka fysisk eller psykisk skada genom användning av subliminala tekniker eller genom att utnyttja sårbarheter hos en specifik grupp personer på grund av deras ålder, fysiska eller psykiska funktionshinder förbjuds. Förslaget förbjuder även AI-system att tillhandahålla sociala poäng för allmänna ändamål av offentliga myndigheter. Det utesluter också användning av realtids fjärrbiometriska identifieringssystem, såsom ansiktigenkänning, i allmänt tillgängliga utrymmen för brottsbekämpande ändamål. Förbuden är fokuserade på manipulerande eller exploaterande AI-system för att hantera de problem som många grupper och forskare har identifierat, som kan uppstå och syfta till att lura användare att fatta beslut mot sina egna intressen - som att avslöja mer personlig information än vad som behövs till exempel för att få en tjänst. Men en verkställande myndighet måste likväl avgöra när ett system är exploaterande eller manipulerande. Härav följer att effekten av förbudet är beroende av framtida regleringsåtgärder. Det tydliga förbudet mot sociala poäng är en tydlig markering av europeiska värden och normer och avvisar system som de enligt uppgift är under utveckling till exempel i Kina.

En annan aspekt är att efter att ett högrisk AI-system har sålts eller tagits i bruk måste leverantören av detsamma upprätta ett övervakningssystem för eftermarknaden för att samla in data om systemets funktion för att säkerställa att det fortlöpande överensstämmer med förordningen och vidta korrigerande åtgärder vid behov. Sjävlärande system som per definition har möjlighet att fortsätta att lära sig efter att de har tagits i bruk, såväl så kallade machine-som deep learning system, behöver med andra ord en med viss regelbundenhet ny bedömning av överensstämmelse med regelverket och om modifieringarna från inlärningen är betydande. Om ett sådant system ändras i en väsentlig grad, är dock användaren, inte leverantören, ansvarig för att göra den nya bedömningen av överensstämmelse vilket behöver särskilt noteras.

Dessutom föreslås att certifikaten för godkännande av högrisk AI system ska vara giltiga under den period de anger som inte får överstiga fem år. På leverantörens

ansökan kan giltighetstiden för ett certifikat förlängas för ytterligare perioder, dock maximalt ytterligare fem år.

Finansiering och resurskonsekvenser av beslutet

Det finns inte behov av att budgetera för en ny finansiering i nuläget för SUs del baserat på de förslag som presenterats. Däremot behöver en mer långsiktig finansiering säkras för att kunna tillgodose de krav som ställts på tillskapande av en organisation för uppföljning, kontroll och rapportering på såväl lokal som regional och nationell nivå. Som framgår av beskrivningen kommer detta att bli totalt sett betydande enheter med omfattande administrativa uppgifter och härav åtföljande kostnader. Någon möjlighet till mer specifik skattning av dessa kostnader för SU:s del saknas dock för närvarande.

Konsekvenser för hälso-och sjukvård

AI-system som enligt förslaget kommer att definieras som högrisk används och kommer att användas i ökande omfattning till exempel inom prehospitalet vård, det vill säga ambulanssjukvård och triagering, inklusive beslutsfattande. Andra exempel är bedömningar av behov av social service av olika slag. De positiva effekterna för den enskilda individen är påtagliga men man behöver skapa en beredskap för att uppfylla definierat regelverk när klassifikationen som högrisk AI blir en realitet.

En annan aspekt är att AI algoritmer redan används och kommer att användas i ökande omfattning inom hälso-och sjukvård. Exempel på användningsområden är bilddiagnostik, tolkning av text, värdering och tolkning av komplexa data av olika slag. En central fråga i detta sammanhang är om den enskilda patienten vid varje tillfälle måste godkänna att AI baserade algoritmer används i samband med utredning och eventuell behandling eller om vederbörande endast informeras i samband med kontakt med sjukvårdsinrättning om att denna typ av teknik används. Detta kommenteras dock inte i förslaget. Nyttoprincipen väger mycket tungt i detta sammanhang eftersom AI baserad teknik har potential att medföra hög och jämn kvalitet samt att frigöra betydande mänskliga resurser som kan användas för annan typ av patientarbete.

Sahlgrenska Universitetssjukhuset

Ann-Marie Wennberg
Sjukhusdirektör

Bilagor som ingår i beslutsunderlaget

- 1 Proposal for a Regulation on a European approach for Artificial Intelligence
- 2 Annexes to the Proposal

Besluten skickas till

- Regeringskansliet, i.remissvar@regeringskansliet.se, diarienummer I2021/01304
- Regeringskansliet, i.esd.remissor@regeringskansliet.se, för kännedom