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 skadeståndsregler för produkter och 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 450 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.

Förslagens och remissens innehåll

Yttrandet handlar om två föreslagna direktiv, Europaparlamentets och rådets direktiv om skadeståndsansvar för produkter med säkerhetsbrister (Product Liability Directive, PLD) och Europaparlamentets och rådets direktiv om anpassning av reglerna om utomobligatoriskt skadeståndsansvar vad gäller artificiell intelligens, direktivet om skadeståndsansvar gällande AI (AI Liability Directive, AILD).

De föreslagna reglerna är delar i den reglering av området digitalisering som vi ser från EUs sida. Båda föreslagna direktiv handlar om skadeståndsansvar, omfattar AI-system som produkter på den gemensamma marknaden och syftar till att säkerställa rätten till att få anspråk prövade (Stadgan om de grundläggande rättigheterna, SGR, artikel 47). Regleringarna har samtidigt delvis olika omfattning och olika angreppssätt.

Remissyttrandet tar därför, efter en kort introduktion till reglerna, först upp skillnader och likheter mellan de två direktiven och hur skadestånd kan utkrävas för AI-system, för att sedan övergå till hur de föreslagna direktiven är ytterligare exempel på komplexiteten i reglerandet av digitalisering i relation till affärshemligheter och kommersialisering. Den tredje delen av remissyttrandet lyfter disparata frågor och observationer, varpå den fjärde delen sammanfattar våra slutsatser:
- att det nu tydligt framgår att AI-system är att betrakta som produkter på EUs interna marknad, och
- att de föreslagna direktiven för skadestånd kan driva mer ansvarsfull utveckling och användning av produkter men de kan också driva nya försäkringserbjudanden och standardavtal kring ansvarsfördelning.

PLD handlar om att tillverkaren ansvarar för vissa skador som orsakas av en produkt med säkerhetsbrister när den skadelidande är en fysisk person. Ansvaret kan inte begränsas genom avtal eller nationell reglering. Det gäller för personskada, för skada på annan egendom än själva

produkten om egendomen inte endast används för yrkesmässiga ändamål samt för förlust eller förvanskning av data som inte endast används för yrkesmässiga ändamål.

AILD rör bevisbördan i fall där medlemsstaten har regler om utomobligatoriskt skadeståndsansvar (dvs. när det inte finns ett avtal mellan den som söker ersättning, den skadelidande, och den som krävs på ersättning) vid vållande. Förslaget ger att skadeståndsansvar som kan göras gällande vid en persons vållande också i vissa fall kan hävdas på grund av en produkts utdata. Till skillnad från PLD kan den skadelidande enligt AILD också vara ett företag.

AI och skadestånd

Det finns här två grunder för skadeståndsanspråk:

1) En tillhandahållare av en produkt kan bli ersättningsskyldig om produkten har en brist och orsakar skada. Då är vållande inte viktigt utan det är kopplingen mellan bristen i produkten och skadan som uppstått som är centralt, att bristen orsakat skadan.
2) En person kan bli ansvarig för sina handlingar och därmed ersättningsskyldig om handlandet orsakar skada för någon annan och det finns ett samband mellan handlingen och skadan. Här är vållandet (*culpa*) centralt.

Det som utmärker och skiljer det första ansvaret från det andra är att en produkttillverkare kan ha haft alla möjliga goda syften men ändå finns det en brist i en produkt och då är tillverkaren ansvarig för skador som produkten orsakar. I det andra fallet är det bristen på aktsamhet som utgör grunden för ansvaret. Här kan även det faktum att den ansvarige inte agerat väga in om en handling hade kunnat reducera effekten av skadan eller kunnat hindra att den inträffade.

De föreslagna skadeståndsreglerna samspelar med den föreslagna AI-förordningen (AIA). Där är fokus på två tillämpningar av AI som anses utgöra hög risk för medborgare

1) när ett AI-system är en produkt i sig självt enligt EUs produktreglering, eller om AI-systemet ingår som säkerhetskomponent i en sådan produkt (Annex II), eller
2) när AI-systemet är ett självständigt system med syfte att automatisera verksamhet som traditionellt utförts av människor (Annex III).

De två tillämpningarna av AI rimmar med varsitt skadeståndsanspråk - produktansvaret i allmänhet som också omfattar AI som produkt eller komponent i produkten, och vållandet genom oaktsamhet som korrelerar med automatisering av mänskligt utförd verksamhet. En komplicerande faktor i relation till vållande (*culpa*) är att ett AI-system inte kan anses vålla skada, då de inte kan ha subjektiv täckning för en handling.

Därför fokuserar AILD på leverantörens ansvar för felaktig produkt (artikel 4.2) eller användarens ansvar för felaktigt handhavande av produkt (artikel 4.3), vilka båda antas resultera i felaktig eller utebliven utdata (artikel 4.1). Därmed begränsas också de skador som man kan kräva ersättning för till de som är en direkt effekt av utdata.

AI är ingen vanlig produkt

PLD slår fast att AI-system är att betrakta som produkter (se Bakgrund till förslaget samt skäl 12). PLD tar också upp att AI-system kan vara så pass komplexa produkter att det är svårt för den som söker ersättning att bevisa kausaliteten mellan systemets konstruktion och den skada en säkerhetsbrist i produkten medfört (skäl 34). Därför lättar artikel 9.4 i PLD på bevisbördan för den sökande om ett AI-system orsakat skadan. Ändå finns en specifik reglering av skadeståndsansvaret för AI-system (AILD) som både är mer detaljerad och tillämpbar i fler fall än motsvarande artikel i PLD:

Parter: Enligt PLD kan en skadelidande bara vara en fysisk person. Enligt AILD kan en sökande vara en fysisk eller en juridisk person. PLD kallar den produktansvarige för ekonomisk aktör och AILD använder begreppet motpart för den som ansvarar för AI-systemet i den givna kontexten.

Relation: PLD gäller alltid mellan skadelidande och produktansvarige, skadeståndsansvaret för produkten går inte att förhandla bort. AILD gäller när det inte redan finns en annan relation mellan parterna, AILD är inte applicerbar om det finns en etablerad relation mellan parterna, t.ex. ett avtal.

PLD lägger ansvaret för skada hos den ekonomiske aktör som sätter produkten på marknaden. Det är endast enligt AILD som användaren av ett AI-system kan bli skadeståndsansvarig.

Skada: PLD gäller inte för skada på egendom som endast används för yrkesmässiga ändamål (artikel 4) medan AILD kan gälla även vid kommersiell användning av AI-system (artikel 2). PLD definierar begreppet skada och är endast tillämplig när skadan uppfyller den definitionen (artikel 4). AILD definierar inte vad skada är utan hänvisar till nationell lag, där bland annat AILD kommer ingå när direktivet implementerats (se Rättslig grund i AILD).

Sammantaget ger förslagen i princip två sätt att kräva ersättning för skador orsakade av AI-system:

PLD: När den skadelidande är en fysisk person som lidit fysisk eller psykisk skada samt om systemet förvanskat eller förlorat data, eller

AILD: När den klagande är en fysisk eller juridisk person som orsakats skada på grund av att en brist i AI-systemet, eller i användandet av AI-systemet, resulterat i fel eller utebliven utdata.

Det är i sammanhanget värt att poängtera att annan lagstiftning eller överenskommelser mellan juridiska personer kommer behövas för att reglera ersättningen då användandet av ett AI-system leder till skador som inte är förlust eller förvanskning av data, såsom informationsläckage till tredje part.

Slutligen, andra nya regleringar som Dataakten (Data Act, DA) använder också konceptet *produkt* men ger det andra definitioner (se DA artikel 2). Definitionen av produkt i PLD kan anses omfatta även definitionen av produkt i DA, då produkter enligt DA är en strikt delmängd av produkterna enligt PLD. Det omvända gäller alltså inte, det finns produkter enligt PLD som inte är produkter enligt DA. Vissa produkter kan falla inom definitionerna i DA och AILD, vissa uppfyller bara den ena definitionen. Eller ingen. Även Cyber-resiliens förordningen (Cyber Resilience Act, CRA) använder sig av begreppet produkt med en fjärde definition. Här gäller det alltså att veta vilken definition man använder sig av när konceptet produkt diskuteras. Det förstärker också intrycket att de regulatoriska initiativen inom det digitala årtiondet skapar ett nytt landskap av regleringar.

Ansvar, insyn och affärshemligheter

I och med bevisbördan för att ett AI-system orsakat skada ligger hos den sökande ser vi två sannolika scenarion framöver. För det första kommer fler avtal att skrivas för att reglera vem som ansvarar för vad och vilken ersättning som utgår om en part brister i sina åtaganden. För det andra ser vi att användaren av AI-system kommer vilja ha mer insyn i hur ett AI-system är konstruerat för att ha en rimligare bild av hur man håller sig fri från framtida skadeståndskrav.

Påståendet är inte nytt. Redan i vårt remissyttrande (RAI, 2021) om den föreslagna AI-förordningen påpekar vi att regleringen av AI kommer driva privata och offentliga aktörer till att se över sina kontrakt och relationer till underleverantörer och kunder. Dels för att säkerställa att deras leverans är förenlig med att AI-systemet går att certifiera, dels för att säkerställa att det används på rätt sätt. Man kan inte nöja sig med att säkerställa att AI-systemen överensstämmer med kraven på certifiering och är vederbörligt CE-märkta. Med reglerna om bevisbördan kommer nu också frågan om hur systemet är konstruerat för att kunna bedöma risken för framtida skadeståndskrav.

Det kan innebära att man vill veta vilken data som använts vid träning och testning eller vilka strategier och tekniker som implementerats för att garantera systemets robusthet och säkerhet. Att den informationen är känslig i relation till leverantörens affär var något som vi lyfte redan 2021 i relation till användarens skyldigheter för hög-risk AI (artikel 29). Det som är nytt genom de nu föreslagna direktiven är att samma diskussioner nu kommer föras också för övriga AI-system.

Sen dess har diskussionen om affärshemligheter fått ett genomslag i andra rättsakter lanserade inom det digitala årtiondet. I Dataakten (Data Act, DA) och Dataförvaltningsförordningen (Data Governance Act, DGA) balanseras skyldigheterna och möjligheterna för datadelning med vikten av att inte röja konfidentialitet och affärshemligheter.

En skillnad mellan de akterna och de kommande direktiven för skadeståndsanspråk är att de senare har sanktioner som går att mitigera genom förhandling, antingen med motparten eller med en tredje

part. Både PLD och AILD öppnar för att täcka sina skadeståndskostnader med försäkringar, vilket skulle ge upphov till en ny affär hos försäkringsgivare. AILD gäller dessutom bara när det inte finns en etablerad relation mellan den sökande och motparten.

Det är också ett affärsmässigt val som går att göra i sin näringsverksamhet om det är motiverat att hellre ta risken för skadeståndsansvar, dvs. värdera det som billigare att betala en ersättning än eventuella kostnader som uppstår om affärshemligheterna hamnar utanför ens kontroll eller till en sökande genom att relevant information lämnas ut i en domstolsprocess. Det finns alltså scenarion där den tänkta effekten av regleringen inte når sitt mål med ansvarsfull produktutveckling i ett digitaliserat samhälle.

Övriga kommentarer

Artikel 4 i PLD definierar de flesta begreppen men två begrepp definieras i andra artiklar. Det är *skadelidande* som definieras i artikel 5 och *klagande* som definieras i artikel 8. Vi föreslår att samtliga definitioner introduceras i samma artikel. Jämför AILD där definitioner finns i artikel 2.

Genomgående i AILD skriver man ”AI-baserade produkter och tjänster” medan i skäl 7 används formuleringen ”den digitala karaktären hos de produkter och tjänster som omfattas av detta direktiv”. Det kan vara bra att tydliggöra hur det kommer sig att en annan formulering används.

I AILD artikel 4.5 hänvisar man till orsakssambandet som tas upp i artikel 4.1, vilken i sin tur hänvisar till att följande villkor ska vara uppfyllda för att orsakssambandet mellan en motparts culpa och ett AI-systems felaktiga eller uteblivna utdata ska anses hålla:

a) Bristande efterlevnad av ett aktsamhetskrav som direkt syftar till att skydda mot den uppkomna skadan
b) Det är rimligt att anta att bristen på efterlevnad har påverkat ett AI-systems utdata eller att utdata uteblev
c) Det är (den uteblivna) utdatan som orsakat skadan.

Det är alltså två orsakssamband som ingår i resonemanget: (1) bristande efterlevnad har påverkat att utdatan är felaktig eller uteblev och (2) felaktig eller utebliven utdata har orsakat skadan. Syftar artikel 4.5 på det första, det andra eller båda orsakssambanden?

Det är intressant att skadeståndsanspråk inte kan göras beroende på den ansvariga organisationens storlek (PLD memorandum), men däremot ska kraven på säkerhetsarbetet vara proportionellt med storleken på organisationen (AIA, artikel 17.2). I båda fallen hänvisas till att inte snedvrida konkurrensen på marknaden.

Det saknas en motivering till varför transportsystemet är undantaget från AILD. Samtidigt är det inte tydligt om det exkluderar ”AI-system som är avsedda att användas som säkerhetskomponenter i samband med förvaltning och drift av vägtrafik” (se Annex III i AIA) från AILD. Är sådana AI-system en del av transportsystemet? Till saken hör att det kommer regleringar om ansvar för fordon men de regleringarna täcker inte hela transportsystemet och inte heller AI-system för hanteringen av vägtrafik. Här hade tydligare definitioner och motiveringar varit behjälpliga för både kommersiella och offentliga aktörer för att förbereda sig inför att de nya direktiven implementeras.

De föreslagna reglerna påverkar inte möjligheten till utlåtande, utan vem som ska bevisa vad och med vilken säkerhet. Därmed kvarstår möjligheten att använda sig av anmälda organ och andra ackrediterade organisationer för att bedöma sannolikheten att en produkt eller utdata orsakat en viss skada. Det gäller även för bedömningen av brister i konstruktionen eller handhavandet av ett AI-system. Även här kan man tänka sig att det kommer finnas en framtida marknad för att bistå i fastläggandet av ansvar när komplexa produkter står i centrum för skadeståndskrav.

Ansvarsfull utveckling

Mjukvarusystem i allmänhet och AI-system i synnerhet är nu produkter enligt EUs regelverk. På så sätt bidrar de föreslagna direktiven till att klargöra att mjukvarusystem ska uppfylla harmoniserade produktregler och kan köpas och säljas på den interna marknaden. Direktiven klargör också vilka

skador som man kan få ersättning för när orsaken kan anses bero på komplex funktionalitet i mjukvara. Hur direktiven kommer påverka i relation till användande av AI får framtiden visa.

De föreslagna direktiven kan driva mer ansvarsfull utveckling och användning av produkter, de kan också driva nya försäkringserbjudande och standardavtal kring ansvarsfördelning. Båda direktiven relaterar till social hållbarhet och enskildas rätt till effektiva rättsmedel. PLD kompletteras dessutom med regleringar för miljömässig hållbarhet för bland annat ansvar för miljöpåverkan och energikonsumtion, medan AILD än så länge saknar motsvarande krav på hållbarhet. Incitament till innovation för energieffektivare AI-utveckling och för reducering av beroendet av kritiska mineraler och andra ändliga naturresurser i relation till digitaliseringen kan komplettera regleringarna på sikt.

Referenser

AIA. (2021). 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 april 2021.

AILD. (2022). Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV Om anpassning av reglerna om utomobligatoriskt skadeståndsansvar vad gäller artificiell intelligens (direktivet om skadeståndsansvar gällande AI), COM/2022/496 final. Bryssel, Belgien, 28 september 2022.

CRA. (2022). Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020, COM/2022/454 final. Bryssel, Belgien, 15 september 2022.

DA. (2022). Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om harmoniserade regler för skälig åtkomst till och användning av data (dataakten), COM/2022/68 final. Bryssel, Belgien, 23 februari 2022.

DGA. (2022). EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten). Bryssel, Belgien.

PLD. (2022). Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om skadeståndsansvar för produkter med säkerhetsbrister, COM/2022/495 final. Bryssel, Belgien, 28 september 2022.

RAI. (2021) Remissyttrande från RISE avseende kommissionens förslag till förordning om regler för AI-system. 24 juni 2021.

SGR. (2012). EUROPEISKA UNIONENS STADGA OM DE GRUNDLÄGGANDE RÄTTIGHETERNA, 2012/C 326/02. 26 oktober 2012.

RISE Research Institutes of Sweden

Digitala Divisionen – AI Policy Impact

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