Webbinar om AI

Malin Johansson, jurist
Ledningskansliet

AI – ett värdefullt verktyg men inte felfritt och kommer med risker

The New York Times

The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work

Millions of articles from The New York Times were used to train chatbots that now compete with it, the lawsuit said.

Share full article 1.3K

Sverige / Region Kronoberg

Läkarnas förvåning: ”Buk” byttes till ”kuk”

Publicerad 1 maj 2024 kl 15.37

I region Kronoberg satsas det på AI, artificiell intelligens, för att skriva läkarnas journaler.

Men AI:n ersätter ibland medicinska diagnoser med namn på grönsaker och kan byta ut ord som ”buk” mot ”kuk”.

– Naivitet är nog ett ganska bra ord för att beskriva vad som präglat det här införandet, säger urolog och överläkare till SR.

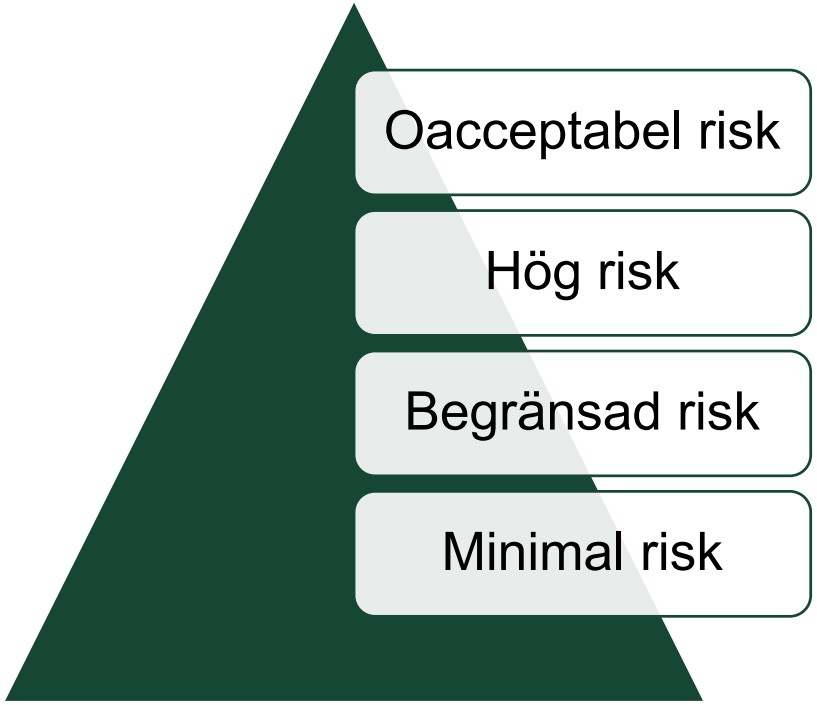
”EU vill bli världsledande inom säker AI. Genom att ta fram ett starkt regelverk som utgår från mänskliga rättigheter och grundläggande värden kan EU utveckla ett AI-ekosystem som gynnar alla.”
– EU kommissionen

AI-förordningen

- Världens första lagstiftning om AI
- Består av 113 artiklar
- Svensk lag sedan 1 augusti 2024
- Stegvis tillämpning – i princip full tillämpning till den 2 augusti 2026
- Art 1-5 börjar tillämpas 2 februari 2025
  - Art 4 krav på att personal som arbetar med drift och användning av AI-system har tillräcklig AI-kunnighet.

+ om vi börjar tänka utifrån lagstiftningen redan nu blir det en mindre omställning när den tillämpas i sin helhet

Riskbaserat förhållningssätt



- AI-system med oacceptabel risk (förbjuden)
- AI-system med hög risk (flertalet krav)
- AI-system med begränsad risk (krav på öppenhet)
- AI-system med minimal risk (AI-förordningen ställer inga krav)

Riskbedömningen är baserad på det avsedda användningsområdet.

Vad är ett AI-system?

Ett maskinbaserat system som är utformat för att fungera med varierande grad av autonomi och som kan uppvisa anpassningsförmåga efter införande och som, för uttryckliga eller underförstådda mål, drar slutsatser härledda från den indata det tar emot, om hur utdata såsom förutsägelser, innehåll, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer ska genereras.

AI-system med oacceptabel risk

- AI-system som är förbjudna

- Finns några få undantag, t.ex. för polis vad gäller biometrisk fjärridentifiering i realtid

AI-system med hög risk

Det finns två kategorier av AI-system med hög risk.

Kategori 1

AI-system som är tänkt att användas som en säkerhetskomponent i en produkt, eller AI-systemet i sig är en produkt, som omfattas av en rättsakt i bilaga 1

OCH

denna produkt måste genomgå en tredjepartsbedömning för att få släppas ut på marknaden eller tas i bruk.

Kategori 2

AI-system som omfattas av bilaga 2 i förordningen.

- Utbildning och yrkesutbildning
- Anställning, arbetsledning och tillgång till egenföretagande

T.ex. AI-system som används för rekrytering och utvärdering av anställda eller för att utvärdera läranderesultat eller fastställa antagning till utbildning.

AI-system med hög risk

Skyldigheter åläggs både **leverantör** och tillhandahållare.

- Riskhanteringssystem
- Data och dataförvaltning
- Teknisk dokumentation
- Loggning
- Transparens och tillhandahållande av information
- Mänsklig kontroll
- Riktighet, robusthet och cybersäkerhet
- Kvalitetsstyrningssystem
- Övervakning efter utsläppande på marknaden

AI-system med hög risk

Leverantören behöver visa att AI-systemet överensstämmer med AI-förordningen innan det släpps ut på marknaden eller tas i bruk.

I princip behöver de säkerställa att kraven på förgående sida uppfylls.

Kan även innebära en tredjepartsbedömning.

Leverantören ska:

- Upprätta en EU-deklaration om överenstämmelse
- Registrera systemet i EU:s databas för högrisk-AI-system
- CE-märka AI-systemet

AI-system med hög risk

Skyldigheter åläggs både leverantör och **tillhandahållare**.

- Följa bruksanvisningen för AI-systemet
- Säkerställa AI-kompetens (utbilda personal)
- Informera leverantören och behörig myndighet om risker
- Spara loggar
- Informera berörda arbetstagare och fackförbund
- I vissa fall genomföra en **konsekvensbedömning avseende grundläggande rättigheter**

OBS! bedömningen ska göras **innan** systemet börjar användas.

AI-system med begränsad risk

AI-system som interagerar med människor.

Transparenskrav som innebär att användaren ska förstå att hen interagerar med ett AI-verktyg.

T.ex. chatbot.

AI-system som genererar texter, bilder med mera.

Transparenskrav som innebär att man ska förstå att materialet är AI-genererat.

T.ex. deepfakes.

AI-system med minimal risk

- AI-förordningen ställer inga krav
- Verksamheter kan på frivillig basis förbinda sig till uppförandekoder för AI-system
- Annan lagstiftning gäller fortfarande, t.ex. GDPR

Art 2.6 AI förordningen
Denna förordning är inte tillämplig på AI-system eller AI-modeller, inbegripets, dess utdata, som specifikt utvecklas och tas i bruk enbart i vetenskapligt forsknings- och utvecklingsarbete.

Undantag för forskning

- AI-förordningen ska inte underminera forsknings- och utvecklingsverksamhet.

- Innebär att AI-förordningen inte behöver tas hänsyn till under processen att ta fram ett AI-system. OBS! AI kan ändå inte tränas på vilken data som helst, regleras av annan lagstiftning.

- Påverkar inte skyldigheten att följa förordningen om ett AI-system som omfattas ska släppas ut på marknaden.

AI-förordningen och GDPR

- GDPR gäller parallellt med AI-förordning
- Innebär att oavsett risknivå på AI-systemet om det behandlar personuppgifter ska GDPR tas hänsyn till
  - Behöver finnas ett syfte/ändamål med behandling, ”cool/rolig” leksak/häftig ny teknik inte tillräckliga syften
  - Grundläggande principerna behöver följas.
  - Tredjeland behöver tas hänsyn till
  - Personuppgiftsbiträdesavtal ska finnas
- IMY har tagit fram vägledning om GDPR och AI

Att tänka på vid användning

- Transparens: om text eller bild är skapad eller bearbetad med AI behöver det framgå.
- Använder du AI för att t.ex. översätta en text bör du kontrollera den innan du publicerar texten. Du har ansvaret även om en AI gjort jobbet.
- Om du avser att behandla någons personuppgifter i en AI behöver du informera personen om det **först**.
- SLU som myndigheter behöver kunna motivera sina beslut.

Att tänka på vid användning

- Tänk på vad du delar med en AI, många AI (framförallt gratis versioner) använder den data de får för att lära sig. Medför spridning av den data AI:n matas med. Dela inte:
  - sekretessuppgifter
  - känsliga personuppgifter
  - uppgifter som inte kan delas med vem som helst, t.ex. källkod, lösenord

- Vanliga IT-systems regler gäller även för AI.
  - bedömning enligt 10 kap 2a§ OSL före att sekretessuppgifter delas med betrodd AI
  - cybersäkerhetslagen ska tillämpas

Medskick från detta webbinar

- AI kan vara ett bra arbetsverktyg för din roll vid SLU men användningen behöver ske på ett **säkert** och **ändamålsenligt** sätt
- Innan ett AI-system införskaffas fundera på vilken risknivå det har och se över vilket arbete du behöver göra **innan** du skaffar systemet
- AI-kunnighetskravet gör att ursäkter som ”*jag visste inte att jag behövde vara transparent*” inte godtas
- Tänk på att andra lagar/regler även gäller för AI-system, t.ex. GDPR

Tack för uppmärksamheten!

KONTAKTUPPGIFTER

Malin Johansson, jurist/legal counsel
018-67 28 48, malin.a.johansson@slu.se

Om du har frågor eller feedback kring dagens webbinar kontakta oss gärna på e-post dataskydd@slu.se

På medarbetarwebben kan du hitta råd för att använda AI-tjänster.


SLU
SCIENCE AND EDUCATION FOR SUSTAINABLE LIFE