Ingen kan ha missat den snabba utvecklingen av AI-verktyg, vilka blivit mer och mer avancerade inom en mycket kortare tidsperiod än någon hade kunnat förvänta sig. Men vad är egentligen integritetskonsekvenserna av detta? Setterwalls biträdande jurister **Jonatan Blomqvist** och **Karolina Jivebäck Pap** utvecklar vad detta innebär för företag som behandlar stora mängder känsliga personuppgifter, såsom läkemedelsföretag.

AI vs

– integritetskonsekvenserna av att använda AI-verktyg för läkemedelsföretag

Under våren har olika AI-verktyg utvecklats till något mycket mer avancerat inom en mycket kortare tidsperiod än vad någon hade kunnat förvänta sig. Det mest ”hypade” AI-verktyget heter ChatGPT – ett AI-verktyg utvecklat av företaget OpenAI. På deras hemsida beskrivs verktyget på följande sätt:

”We’ve trained a model called ChatGPT which interacts in a conversational way. The dialogue format makes it possible for ChatGPT to answer follow-up questions, admit its mistakes, challenge incorrect premises, and reject inappropriate requests”.[1]

I grund och botten har de således utvecklat en AI som kan svara på en mängd olika frågor och följdfrågor. Men hur kan verktyget göra detta? ChatGPT är nämligen en så kallad ”Generativ AI”, vilket innebär att den kan generera svar på nästan vilken fråga som helst. AI:n har använt människor för att ge så kallade exempelsvar och använt människor för belöning av modellfunktion (på engelska kallad ”Reinforcement Learning from Human Feedback” [RLHF]) under sin upplärning. Denna träning gick i princip ut på att skrapa internet efter all slags information, inklusive personuppgifter, för att AI:n skulle kunna utvecklas till vad det är i dag.

Dessutom bör man ha i åtanke att allt som används som indata, det vill säga all information du förser AI:n med när du ställer en fråga, kan potentiellt komma att användas som utdata, det vill säga AI-verktygen kan eventuellt använda den information som den har fått av sina användare för sin egen utveckling och lärande. Detta gör AI:n smartare och möjliggör att den exempelvis kan svara på liknande frågor i framtiden.

De nya AI-verktygen har möjlighet att hjälpa alla typer av företag att öka effektiviteten genom att slutföra vissa uppgifter eller svara på vissa frågor mycket snabbare än någon anställd skulle kunna göra.

De nya AI-verktygen har möjlighet att hjälpa alla typer av företag att öka effektiviteten genom att slutföra vissa uppgifter eller svara på vissa frågor mycket snabbare än någon anställd skulle kunna göra. Därför är det inte förvånande att de är i ropet och redan används i stor utsträckning över hela världen. Men även om de uppskattas medför de vissa konsekvenser, där integritetskonsekvenserna inte är de enda


GDPR
AI Chatbot
Hello! I am chatbot_

I förhållande till ovanstående är det därför av yttersta vikt för läkemedelsföretagen att se till att deras IT- och integritetspolicyer uppdateras för att inkludera eventuella begränsningar avseende tillåten användning av AI-verktyg såsom ChatGPT.

– det finns nämligen alltid en risk att få partisk eller till och med helt felaktig information. Ett exempel på en sådan partisk AI är den som United Health använde för att utvärdera patienters vårdbehov. AI:n var neutral vad gällde patienternas hudfärg och var därmed inte avsiktligt diskriminerande eller partisk. Problemet var istället att algoritmen baserades på vårdkostnaden för patienterna – inte själva sjukdomen – och på grund av det amerikanska sjukvårdssystemet med försäkringar och höga kostnader söker ljushyade patienter vård i större utsträckning och har därmed en högre vårdkostnad. Eftersom mindre pengar spenderas på mörkhyade patienter med samma behovsnivå, drog AI:n således den felaktiga slutsatsen att mörkhyade patienter var friskare än lika sjuka ljushyade patienter.[2]

Vidare finns det en risk för att företagshemligheter exponeras vid användning av allmänt tillgänglig AI på samma sätt som personuppgifter kan komma att göra. Kort sagt: Precis som företag inte ska dela personuppgifter med AI:n, och särskilt inte känsliga personuppgifter, bör de se till att inte dela företagshemligheter med den. I det följande kommer vi dock att fokusera på konsekvenserna för integriteten.

Några av konsekvenserna för integriteten

GDPR bygger på flera rättsliga principer och uppgiftsminimering är en av dem. Denna princip anger att endast de kategorier av personuppgifter som är nödvändiga för det ändamål du samlar in dem, ska samlas in. Således är det inte tillåtet att samla in några extra kategorier av personuppgifter ”för säkerhets skull”. Naturligtvis är AI-verktyg som ChatGPT som skrapar internet för information om allt och vem som helst inte i överensstämmelse med denna dataminimeringsprincip. Detta är en grundläggande motsägelse som sannolikt kommer att fortsätta att vara ett problem när man fortsätter utveckla AI.

En annan viktig aspekt som bör nämnas är vissa AI-verktygs brist på integritetsinformation till sina användare. ChatGPT kan återigen användas som exempel. I OpenAI:s integritetspolicy är det inte helt klart på vilken grund de samlar in personuppgifter för att träna AI:n. I policyn anges endast att de kan basera behandlingen av användargenererat innehåll (det vill säga all slags information som användaren lägger in i verktyget) på deras legitima intresse för att utveckla, förbättra eller marknadsföra sina tjänster.

Således är bristen på transparens ett annat problem i förhållande till ovan – det är inte klart för användarna vilka data som verkligen används för träning av AI:n. Det är också oklart hur länge OpenAI kommer att lagra personuppgifterna, särskilt de personuppgifter som kan ha samlats in när AI:n under sin träning skrapade internet. Detta strider mot principen om lagringsminimering som anges i GDPR.

Känsliga personuppgifter och AI

Särskilda kategorier av personuppgifter, såsom hälsouppgifter, får inte behandlas om inte ett undantag enligt GDPR föreligger, se artikel 9. Därför bör läkemedelsföretag och andra företag inom life science-industrin, till exempel MedTech-företag som behandlar stora mängder hälsouppgifter, vara extra försiktiga med hur de behandlar personuppgifterna och med vem de delar dem.

När det gäller behandling av personuppgifter är det först och främst viktigt att alla anställda förstår vad de får och inte får göra, särskilt när suget efter att prova de nya och intressanta tekniska lösningarna som AI-verktygen innebär. Även om AI:n är intressant ur ett effektivitetsperspektiv, finns det ingen transparens i förhållande till vad uppgifterna kan komma att användas till. Om en anställd på ett läkemedelsföretag förser ett AI-verktyg med personuppgifter i form av hälsouppgifter finns det alltså en risk att uppgifterna används för att träna AI:n. Därefter finns det inget sätt att säkerställa att hälsouppgifter inte kommer att användas som utdata när andra användare ställer motsvarande frågor.

I förhållande till ovanstående är det därför av yttersta vikt för läkemedelsföretagen att se till att deras IT- och integritetspolicyer uppdateras för att inkludera eventuella begränsningar avseende tillåten användning av AI-verktyg såsom ChatGPT. Det är dessutom viktigt att ha regelbundna utbildningar för de anställda. Företagen kan kanske till och med se utvecklingen av AI som en möjlighet att uppdatera de generella GDPR-utbildningarna.

Slutligen bör det nämnas att EU:s AI-förordning för närvarande är under utveckling. Några av dess grundläggande principer är transparens och ansvarsskyldighet. Förordningen har alldeles nyligen varit föremål för vissa sista minutenändringar i Europaparlamentet på grund av den snabba utvecklingen av generativ AI, såsom ChatGPT. Till exempel tillades att generativ AI kommer att behöva informera om allt upphovsrättsskyddat material som används för att utveckla dess system. Det ska bli intressant att se den slutliga versionen av förordningen och hur den kommer att tillämpas i förhållande till generativ AI. Vi på Setterwalls Advokatbyrå följer detta noga.

Referenser

1. https://openai.com/blog/chatgpt.

2. New York insurance regulator to probe Optum algorithm for racial bias | Fierce Healthcare.

KAROLINA JIVEBÄCK PAP
Associate,
Setterwalls Advokatbyrå

JONATAN BLOMQVIST
Associate,
Setterwalls Advokatbyrå