






Wie is er een betere jurist? Jij of AI?

Volgende slide

Tja, wie is er dan die betere jurist, jij of AI?

The screenshot shows a web browser window with the URL <https://news.bloomberglaw.com/business-and-practice/legal-errors-by-top-ai-models-a...>. The article title is "Popular AI Chatbots Found to Give Error-Ridden Legal Answers". The authors are Isabel Gottlieb, Correspondent, and Isaiah Poritz, Legal Reporter. The article includes a list of bullet points, a paragraph about AI chatbots from OpenAI, Google, and Meta, a paragraph about large language models hallucinating, and a paragraph about generative AI helping provide legal services. On the right side, there are search filters for "Search by Topic" and "Search by Company".

► Listen     

- Researchers measured AI responses to 200,000 legal questions
- Frequent 'hallucinations' could hurt self-represented litigants

Popular AI chatbots from OpenAI Inc., Google LLC, and Meta Platforms Inc. are prone to "hallucinations" when answering legal questions, posing special risks for people using the technology because they can't afford a human lawyer, new research from Stanford University said.

Large language models hallucinate at least 75% of the time when answering questions about a court's core ruling, [the researchers found](#). They tested more than 200,000 legal questions on OpenAI's ChatGPT 3.5, Google's PaLM 2, and Meta's Llama 2—all general-purpose models not built for specific legal use.

Generative artificial intelligence has raised hopes that the powerful technology can help provide legal services to people who can't afford a lawyer. According to the nonprofit Legal Services Corporation, low-income people in the US received

Search by Topic

- [Pro Se Representation](#)
- [Large Language Models](#)
- [Access To Justice](#)
- [Same-Sex Marriage](#)

Search by Company

- [Alphabet Inc](#)
- [Meta Platforms Inc](#)

Tja, wie is er dan die betere jurist..... (2)

Nieuws • Artificial Intelligence +

23 juni 2023 ⌚ leestijd 2 minuten 💬 0 reacties

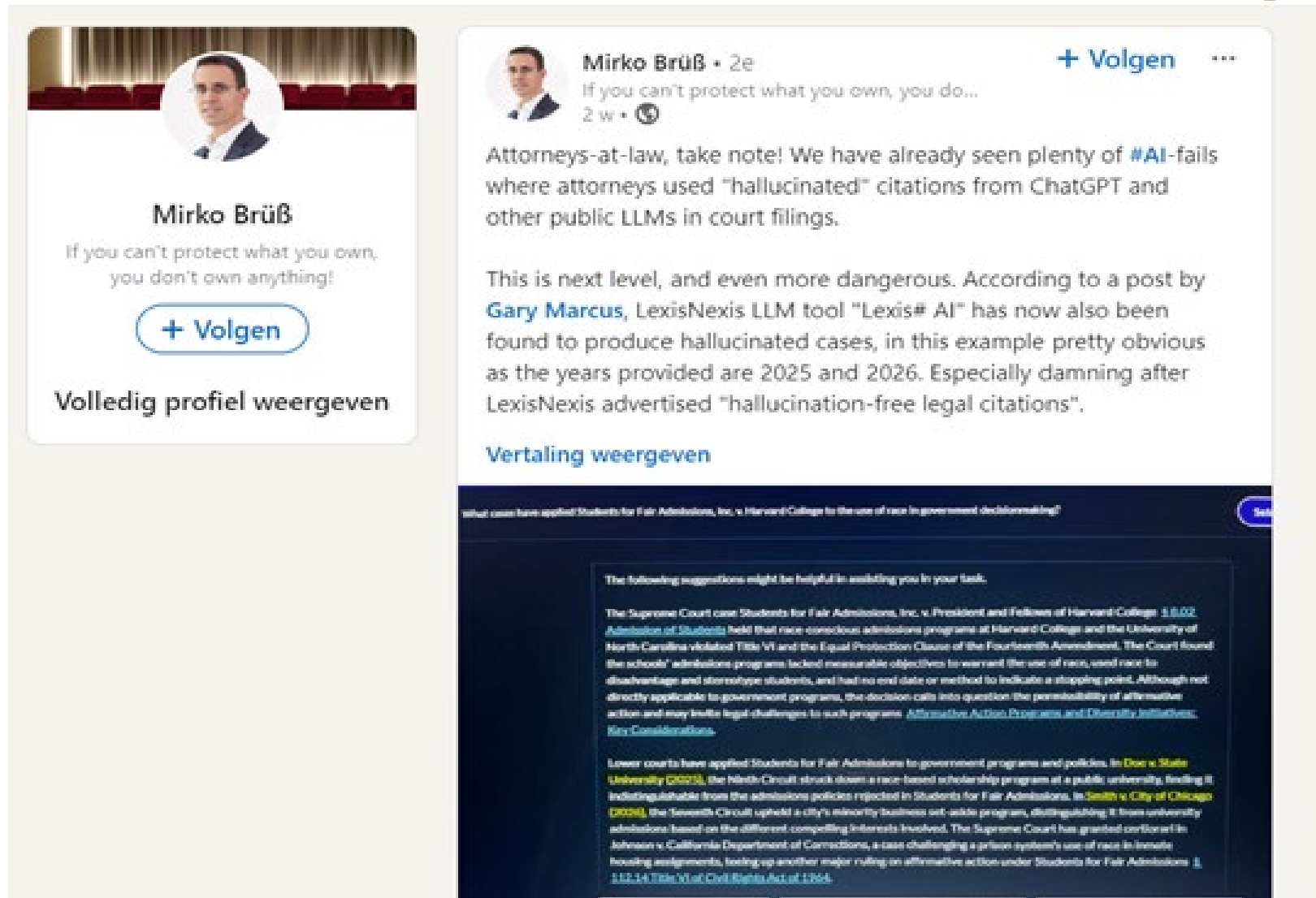
Boete voor advocaat die niet-bestaande ChatGPT-gegenereerde zaken gebruikte

De Amerikaanse advocaat die ChatGPT gebruikte voor het aandragen van jurisprudentie moet een boete betalen van de rechter. De zaken die ChatGPT voor hem aandroeg, bleken helemaal niet te bestaan. Volgens de rechter heeft zowel de advocaat als het bedrijf waarvoor hij werkt "zijn verantwoordelijkheden laten varen".



Museum toont
AI-gegenereerd
Meisje met de
Parel

Tja, wie is er dan die betere jurist..... (3)



The image shows a LinkedIn profile for Mirko Brüb and a tweet from him. The profile includes a circular profile picture, the name 'Mirko Brüb', a bio 'If you can't protect what you own, you don't own anything!', a '+ Volgen' button, and the text 'Volledig profiel weergeven'. The tweet, posted 2 weeks ago, discusses AI failures in legal citations and mentions LexisNexis LLM tool 'Lexis# AI'.

Mirko Brüb
If you can't protect what you own,
you don't own anything!
[+ Volgen](#)
Volledig profiel weergeven

Mirko Brüb • 2e
If you can't protect what you own, you do...
2 w • 🌐

Attorneys-at-law, take note! We have already seen plenty of #AI-fails where attorneys used "hallucinated" citations from ChatGPT and other public LLMs in court filings.

This is next level, and even more dangerous. According to a post by [Gary Marcus](#), LexisNexis LLM tool "Lexis# AI" has now also been found to produce hallucinated cases, in this example pretty obvious as the years provided are 2025 and 2026. Especially damning after LexisNexis advertised "hallucination-free legal citations".

[Vertaling weergeven](#)

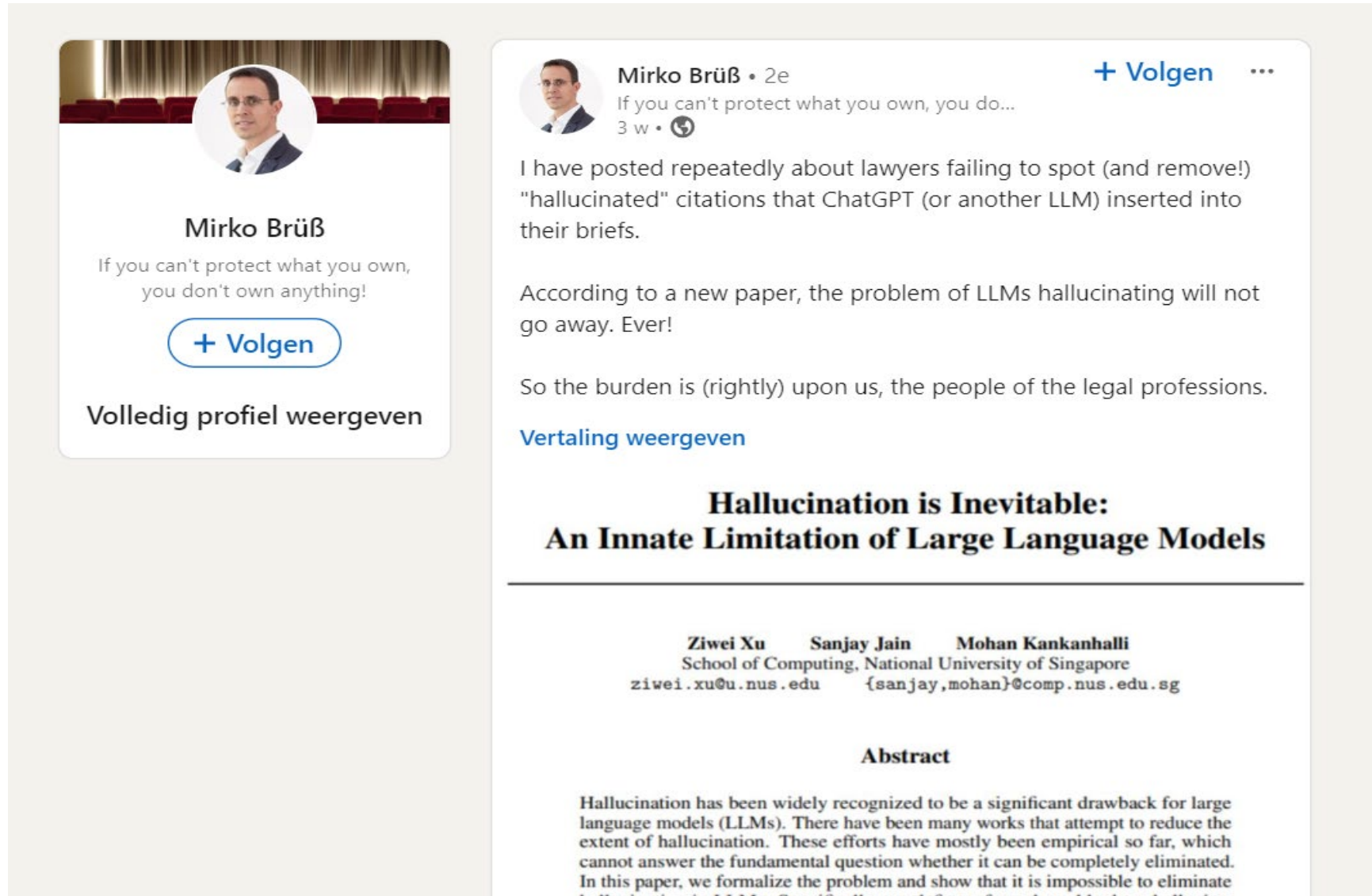
What cases have applied *Students for Fair Admissions, Inc. v. Harvard College* to the use of race in government decisionmaking?

The following suggestions might be helpful in assisting you in your task.

The Supreme Court case *Students for Fair Admissions, Inc. v. President and Fellows of Harvard College*, 18-002, [Admission of Students](#) held that race-conscious admissions programs at Harvard College and the University of North Carolina violated Title VI and the Equal Protection Clause of the Fourteenth Amendment. The Court found the schools' admissions programs lacked measurable objectives to warrant the use of race, used race to disadvantage and stereotype students, and had no end date or method to indicate a stopping point. Although not directly applicable to government programs, the decision calls into question the permissibility of affirmative action and may invite legal challenges to such programs. [Affirmative Action Programs and Diversity Initiatives: Key Considerations](#).

Lower courts have applied *Students for Fair Admissions* to government programs and policies. In [Doe v. State University](#), 2023, the Ninth Circuit struck down a race-based scholarship program at a public university, finding it indistinguishable from the admissions policies rejected in *Students for Fair Admissions*. In [Smith v. City of Chicago](#), 2024, the Seventh Circuit upheld a city's minority business set-aside program, distinguishing it from university admissions based on the different compelling interests involved. The Supreme Court has granted certiorari in *Johnson v. California Department of Corrections*, a case challenging a prison system's use of race in inmate housing assignments, looking up another major ruling on affirmative action under *Students for Fair Admissions*. [18-14 Title VI of Civil Rights Act of 1964](#).

Kortom: “Hallucinating AI is here to stay!”



The image shows a LinkedIn profile and a post. The profile is for Mirko Brüb, with a bio that reads "If you can't protect what you own, you don't own anything!". The post is from 2 weeks ago and contains the following text:

I have posted repeatedly about lawyers failing to spot (and remove!) "hallucinated" citations that ChatGPT (or another LLM) inserted into their briefs.

According to a new paper, the problem of LLMs hallucinating will not go away. Ever!

So the burden is (rightly) upon us, the people of the legal professions.

[Vertaling weergeven](#)

**Hallucination is Inevitable:
An Innate Limitation of Large Language Models**

Ziwei Xu Sanjay Jain Mohan Kankanhalli
School of Computing, National University of Singapore
ziwei.xu@u.nus.edu {sanjay,mohan}@comp.nus.edu.sg

Abstract

Hallucination has been widely recognized to be a significant drawback for large language models (LLMs). There have been many works that attempt to reduce the extent of hallucination. These efforts have mostly been empirical so far, which cannot answer the fundamental question whether it can be completely eliminated. In this paper, we formalize the problem and show that it is impossible to eliminate hallucination in LLMs. Specifically, we define a formal model where hallucination

Hoe vaak een LLM hallucineert bij het samenvatten van een document (jan 24)

Model	Hallucination Rate	Factual Consistency Rate	Answer Rate	Average Summary Length (Words)
GPT 4	3.0 %	97.0 %	100.0 %	81.1
GPT 4 Turbo	3.0 %	97.0 %	100.0 %	94.3
GPT 3.5 Turbo	3.5 %	96.5 %	99.6 %	84.1
Google Gemini Pro	4.8 %	95.2 %	98.4 %	89.5
Llama 2 70B	5.1 %	94.9 %	99.9 %	84.9
Llama 2 7B	5.6 %	94.4 %	99.6 %	119.9
Llama 2 13B	5.9 %	94.1 %	99.8 %	82.1
Cohere-Chat	7.5 %	92.5 %	98.0 %	74.4
Cohere	8.5 %	91.5 %	99.8 %	59.8
Anthropic Claude 2	8.5 %	91.5 %	99.3 %	87.5
Microsoft Phi 2	8.5 %	91.5 %	91.5 %	80.8
Google Palm 2 (beta)	8.6 %	91.4 %	99.8 %	86.6
Mixtral 8x7B	9.3 %	90.7 %	99.9 %	90.7
Amazon Titan Express	9.4 %	90.6 %	99.5 %	98.4
Mistral 7B	9.4 %	90.6 %	98.7 %	96.1
Google Palm 2 Chat (beta)	10.0 %	90.0 %	100.0 %	66.2
Google Palm 2	12.1 %	87.9 %	92.4 %	36.2
Google Palm 2 Chat	27.2 %	72.8 %	88.8 %	221.1

Wie is Menno Weij trouwens?



Menno Weij

Partner Tech & Privacy Law

Menno.Weij@bdo.nl

+31 6 109 190 24

Menno Weij heeft aan de Universiteit Leiden Nederlands Recht (civiel- en strafrecht) gestudeerd. Vervolgens is hij ruim 20 jaar werkzaam geweest als ‘tech advocaat’. Sinds december 2018 werkt Menno bij BDO Legal, binnen het team “Tech & Privacy Law”. In 2001 heeft Menno met goed gevolg de postdoctorale opleiding ICT-recht aan de Grotius Academie afgerond. Naast BDO, is Menno bestuurslid van de NVVIR en redacteur bij het Tijdschrift voor Internetrecht. Menno is voorts co-founder van IncPlus, en van VraagHugo & DocBldr. Menno is commissaris bij het Security of Things Fund en lid van de RvT bij SOMI. Tenslotte is Menno een officiële “vriend” van BNR.

De belangrijkste AI-gebeurtenissen van 2023

🚀 De 8 Belangrijkste AI-Gebeurtenissen van 2023: Een Terugblik 🚀

👉 Er is natuurlijk veel te veel gebeurd het afgelopen jaar om samen te vatten, maar dit zijn [Job van den Berg](#) en mij vanuit [ai.nl - The AI Group](#) en [The Automation Group](#) zijn opgevallen.

1 De slag om OpenAI.

Game of Thrones in Silicon Valley - het ontslag en terugkeer van Sam Altman en Greg Brockman bij OpenAI, de invloed van Satya Nadella en het (bijna) voltallige bestuur dat moest vertrekken. Zonder twijfel komt hier een Netflix-serie over.

2 Talloze nieuwe taalmodellen

Falcon180b, Llama2, Gemini, Claude2, Palm2, er kwamen talloze foundational models bij. Toch bleef GPT4 de ongekroonde koning van de taalmodellen qua bekendheid en adoptie. Bovendien werden ze "multimodal".

3 Europa doet weer (een beetje) mee

Met de investering van 500 miljoen in het Duitse AI-bedrijf Aleph Alpha, 385 voor het Franse Mistral en 235 voor het eveneens Franse Hugging Face (en 13.5 miljoen voor GPT-NL ;-)) kan Europa een klein beetje meekomen in de LLM-race.

4 Self driving in mineur

Waar Musk al jaren roept dat Full Self Driving echt om de hoek staat, is er in 2023 zeker in Europa nog weinig van te merken. In de VS kwam er wetgeving die meer vrijheid gaf aan zelfrijdende taxi-diensten als Waymo, maar tegelijkertijd vielen er flinke klappen bij concurrent Cruise die de licentie verloor na verschillende

5 Nvidia door het dak

Het aandeel van Nvidia ging met 234% de lucht in en hoewel er meer concurrentie komt van Google, Microsoft, AMD en Intel op specifieke chipsets voor AI-applicaties, is het bedrijf zowel qua technologie als software stack (sterk ondergewaardeerde asset) de nummer 1 positie nog lang niet kwijt.

6 De discussie rondom AGI barste los

Elon Musk, Geoff Hinton, Ilya Sutskever en anderen denken allemaal dat Artificial General Intelligence voor de deur staat en dat de impact op werk en samenleving gigantisch zal zijn. Yann LeCun van Meta is de (m.i. prettige) realist van de groep die zegt dat de impact groot is, maar dat we inventief genoeg zijn om technologie verantwoordelijk te ontwikkelen.

7 Regulering met de AI Act en Biden's Executive Order

Na jaren van overleg is er zowel in de VS als de EU - duidelijkheid waar de regulering van AI naartoe zal gaan. En hoewel de technische uitwerking nog moet komen, weten bedrijven globaal waar ze aan toe zijn en zal dit zorgen voor een meer evenredig speelveld. Tegelijkertijd zal moeten blijken hoe China en AI-samenwerkingspartner Rusland hier mee om zullen gaan.

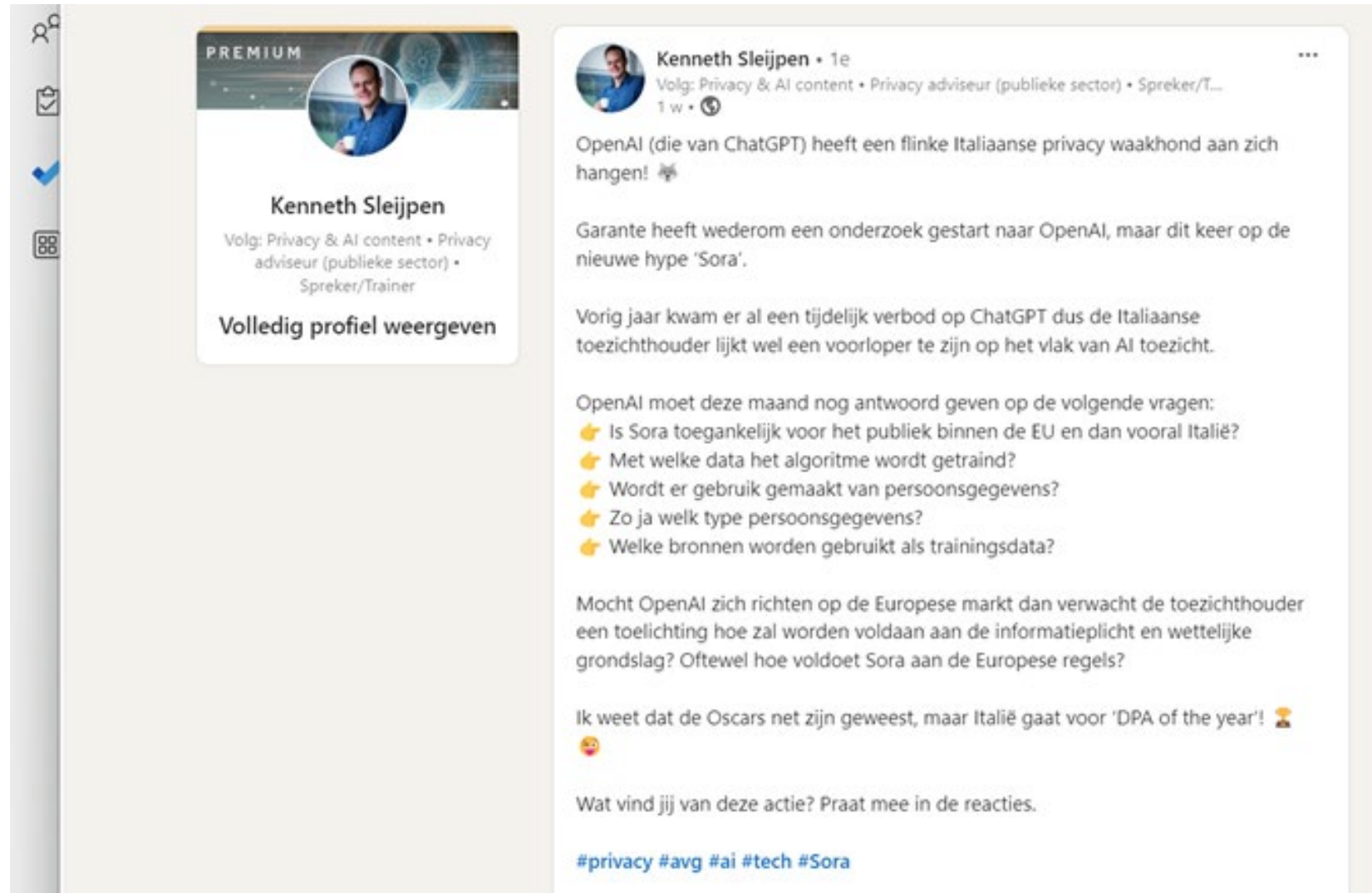
8 (Humanoid) Robots are coming

2023 is het jaar dat grote doorbraken bracht op het vlak van humanoid robots: robots die gelijkenissen hebben met mensen. Figure AI en Tesla Optimus Gen 2 die deze week werd gepresenteerd maken duidelijk dat binnen een paar jaar we meer en meer van deze robots zullen zien.

Een AI nieuwszender



Maar nu is er ook Sora: text to video - met meteen een probleem



Kenneth Sleijpen
Volg: Privacy & AI content • Privacy adviseur (publieke sector) • Spreker/Trainer
Volledig profiel weergeven

Kenneth Sleijpen • 1e
Volg: Privacy & AI content • Privacy adviseur (publieke sector) • Spreker/T...
1 w • 🌐

OpenAI (die van ChatGPT) heeft een flinke Italiaanse privacy waakhond aan zich hangen! 🐾

Garante heeft wederom een onderzoek gestart naar OpenAI, maar dit keer op de nieuwe hype 'Sora'.

Vorig jaar kwam er al een tijdelijk verbod op ChatGPT dus de Italiaanse toezichthouder lijkt wel een voorloper te zijn op het vlak van AI toezicht.

OpenAI moet deze maand nog antwoord geven op de volgende vragen:

- 👉 Is Sora toegankelijk voor het publiek binnen de EU en dan vooral Italië?
- 👉 Met welke data het algoritme wordt getraind?
- 👉 Wordt er gebruik gemaakt van persoonsgegevens?
- 👉 Zo ja welk type persoonsgegevens?
- 👉 Welke bronnen worden gebruikt als trainingsdata?

Mocht OpenAI zich richten op de Europese markt dan verwacht de toezichthouder een toelichting hoe zal worden voldaan aan de informatieplicht en wettelijke grondslag? Oftewel hoe voldoet Sora aan de Europese regels?

Ik weet dat de Oscars net zijn geweest, maar Italië gaat voor 'DPA of the year'! 🏆
😬

Wat vind jij van deze actie? Praat mee in de reacties.

#privacy #avg #ai #tech #Sora

Google drukte ondertussen even op “pauze”

Google pauzeert AI-afbeeldinggenerator na 'problemen'

Google stopt voorlopig met de mogelijkheid om afbeeldingen van mensen te genereren met AI-technologie Gemini. Het besluit volgt op kritiek van gebruikers dat de dienst inaccurate resultaten opleverde.

Met Gemini kunnen onder meer kunstmatige afbeeldingen gegenereerd worden op basis van tekstuele omschrijvingen van gebruikers. Daarmee lijkt het op eerder uitgebrachte technologieën van concurrenten, zoals afbeeldinggenerator DALL-E.

Uit onderzoek van onder meer [The Washington Post](#) bleek eerder dat deze technologieën stereotyperingen in de hand kunnen werken. Als een gebruiker bijvoorbeeld om een afbeelding van een 'leider' vraagt, wordt relatief vaak een man getoond, terwijl 'gevangenen' in meerderheid afbeeldingen van zwarte mensen oplevert.

Overheidsverbod ChatGPT?

ChatGPT voor ambtenaren verboden: 'Maar experimenteren met AI blijft mogelijk'

🕒 12 december - 15:45 Laatste update: 19:53



Erwin Vogelaar
Redacteur



Binnen de [overheid](#) zijn [ChatGPT](#) en Bard verboden, maar het moet wel mogelijk blijven om te experimenteren met de technologie. Dat schrijft staatssecretaris Alexandra van Huffelen in een [brief](#) aan de Tweede Kamer.

Overheid terughoudend met gebruik 'publieke' Gen AI


Generatieve AI biedt veelbelovende mogelijkheden om efficiënter te werken en effectiever publieke doelen te behalen, maar er zitten volgens demissionair staatssecretaris Van Huffelen te veel risico's aan het gebruik ervan. In beginsel wordt het gebruik daarom niet toegestaan, 'tenzij de aanbieder en de gebruiker aantoonbaar voldoen aan de geldende wet- en regelgeving.'

In een [Kamerbrief](#) zet de staatssecretaris het voorlopige standpunt over generatieve AI door rijksorganisaties uiteen. Hiervoor won ze onder meer advies in bij de Landsadvocaat en de Autoriteit Persoonsgegevens (AP). In het eerst kwartaal van 2024 zal ze een overheidsbrede visie op generatieve AI naar de Kamer sturen.t.

Voorlopig standpunt

- Alle (experimenten met) generatieve AI-toepassingen moeten voldoen aan geldende wet- en regelgeving
- Voorafgaand aan gebruik van generatieve AI moet voor iedere casus een risicoanalyse worden uitgevoerd. Dit zijn een (pre-scan) Data Protection Impact Assessment (DPIA4) en een algoritme impact assessment (zoals een Impact Assessment Mensenrechten en Algoritmes (IAMA5))
- De uitkomsten hiervan moeten voorgelegd worden aan de (departementale) Chief Information Officer en de Functionaris Gegevensbescherming.
- Gebruik van niet-gecontracteerde generatieve AI-toepassingen, zoals ChatGPT, Bard en Midjourney, zijn in beginsel niet toegestaan binnen de overheid. Die voldoen over het algemeen niet aantoonbaar aan de geldende privacy- en auteursrechtelijke wetgeving.



Beperkingen toegang ivm trainen AI



Martijn Kleppe
Directieteamlid Koninklijke Bibliotheek, portefeuille Onderzoeken&Ontdekken


[+ Volgen](#)

Volledig profiel weergeven

 **Martijn Kleppe** • 2e
Directieteamlid Koninklijke Bibliotheek, portefeuille Onder...
1 w • Bewerkt • 

Vandaag hebben we vanuit de [Koninklijke Bibliotheek \(KB\)](#), [nationale bibliotheek](#) een belangrijk bericht online gezet over AI & datacollecties.

- ▶ Samenvatting: KB beperkt toegang collecties voor trainen commerciële AI.
- ▶ Lange versie: Als KB zijn we enthousiast over de mogelijkheden van AI. Maar ook vinden we het belangrijk dat AI-bedrijven op een ethisch verantwoorde wijze werken. Daarom willen we niet dat commerciële bedrijven zonder toestemming digitale bronnen gebruiken voor het trainen van AI. En dus hebben we maatregelen genomen. Nieuwsbericht: https://lnkd.in/e_yfwkzj Uitgebreider statement: <https://lnkd.in/e7SDAdr>

 Nieuws 09 januari 2024

KB beperkt toegang collecties voor trainen commerciële AI

De KB neemt maatregelen om het crawlen van digitale bronnen voor het trainen van generatieve AI tegen te gaan. Lees hier wat dit betekent.

En nu snap je wellicht waarom ;)



Image Source: Getty complaint



Chris in 't Veld • 2e

Owner/Lawyer at PS2C <press start 2 continue>
3 mnd •

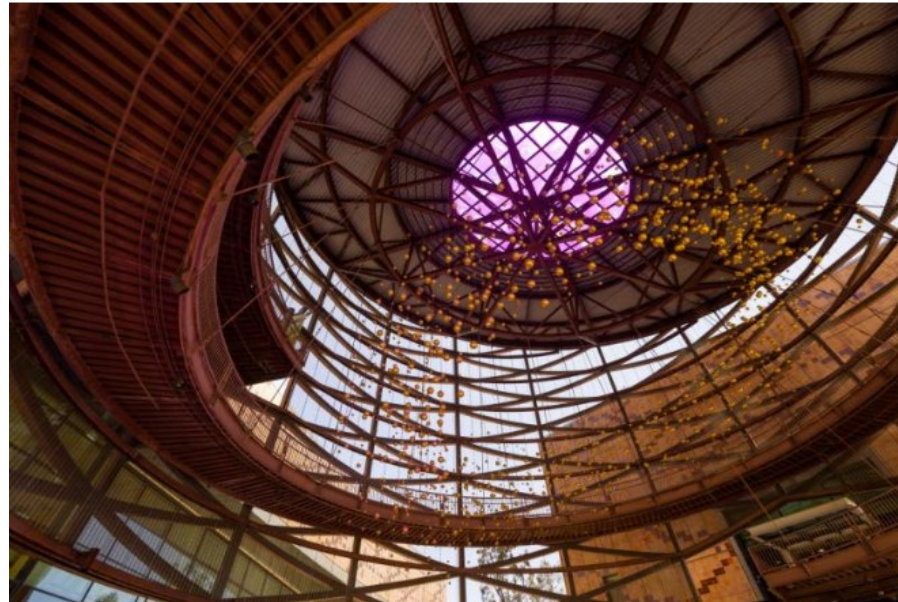
+ Volgen ...

Microsoft expanding its IPR indemnity clause to cover AI output. Sure - you need to use the protection Microsoft build into its products, but this seems like a big step forward. Let's see if the other big AI players will follow.

Especially like this quote from Microsoft: "We are charging our commercial customers for our Copilots, and if their use creates legal issues, we should make this our problem rather than our customers' problem."

Thanks [Daan Debie](#) for sharing this.

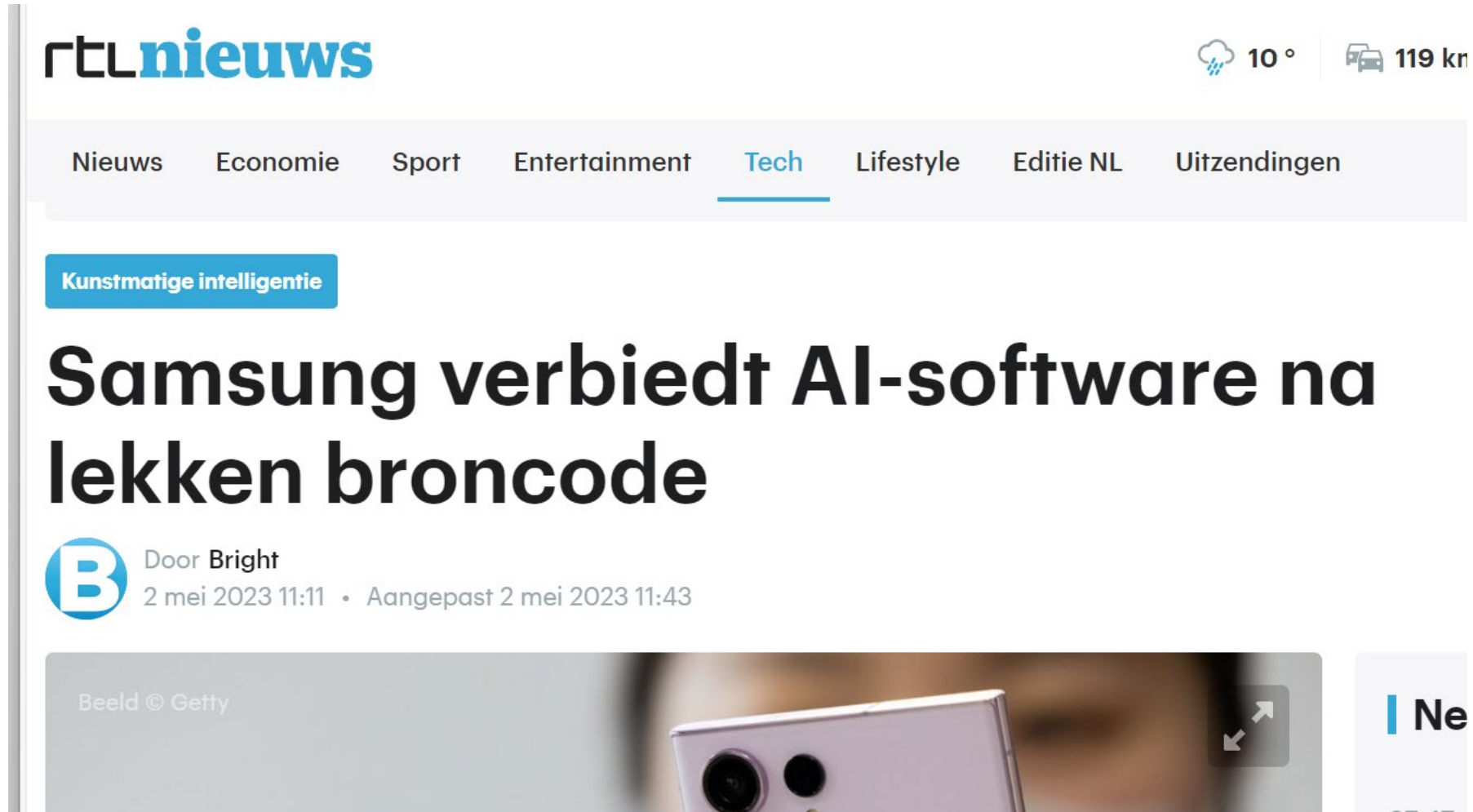
[Vertaling weergeven](#)



Microsoft announces new Copilot Copyright Commitment for customers -
Microsoft On the Issues

blogs.microsoft.com • Leestijd: 3 min.

Daar gaat je bedrijfsgeheim!



The screenshot shows the RTL Nieuws website interface. At the top left is the logo 'rtl nieuws'. On the right, there is a weather icon with '10 °' and a carpooling icon with '119 kr'. Below the logo is a navigation menu with items: 'Nieuws', 'Economie', 'Sport', 'Entertainment', 'Tech' (which is underlined), 'Lifestyle', 'Editie NL', and 'Uitzendingen'. A blue tag labeled 'Kunstmatige intelligentie' is positioned above the main headline. The headline itself reads 'Samsung verbiedt AI-software na lekken broncode'. Below the headline, it says 'Door Bright' and '2 mei 2023 11:11 • Aangepast 2 mei 2023 11:43'. At the bottom of the article preview, there is a photo of a smartphone with the text 'Beeld © Getty' and a share icon.

rtl nieuws

10 ° 119 kr

Nieuws Economie Sport Entertainment Tech Lifestyle Editie NL Uitzendingen

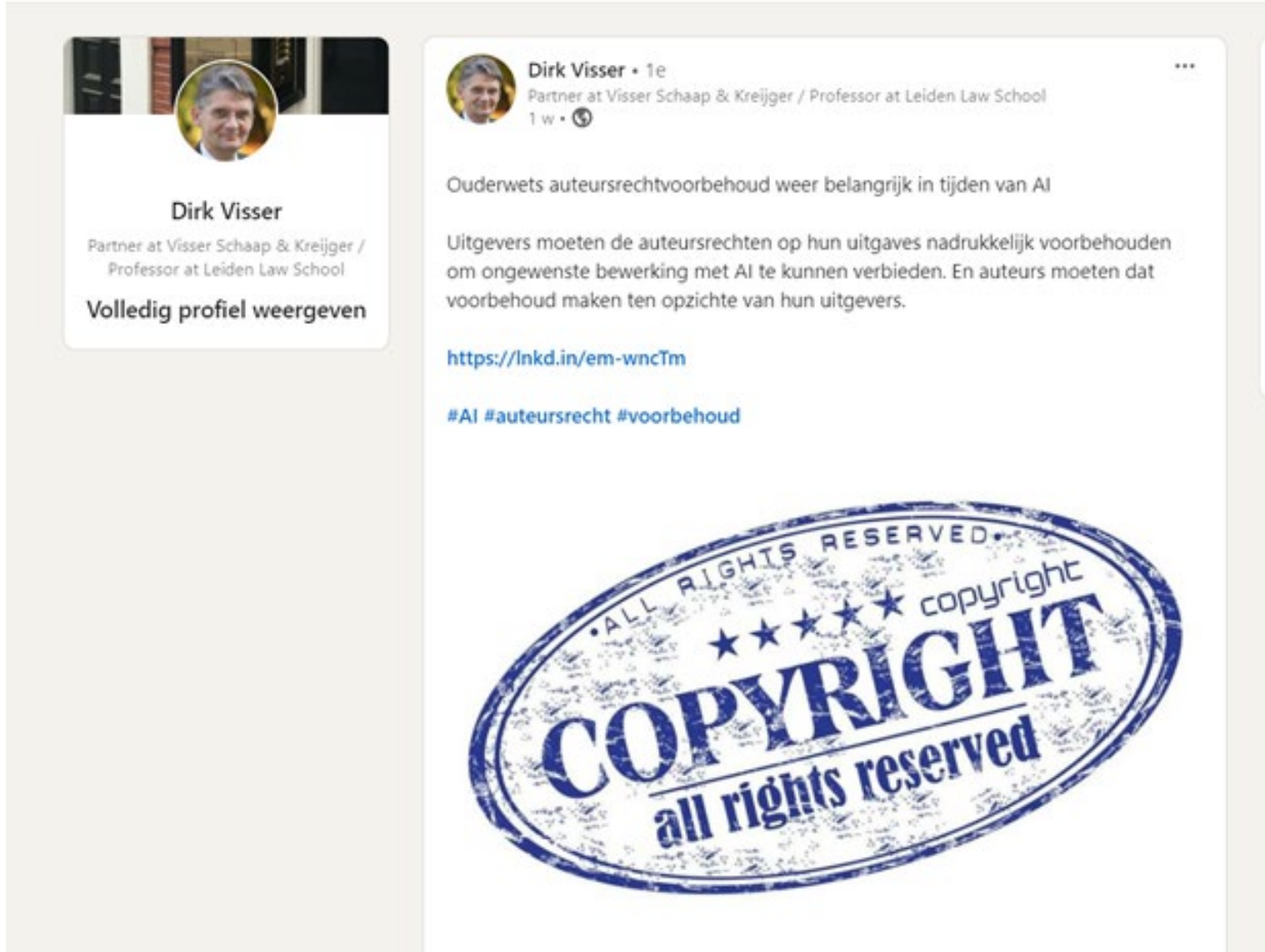
Kunstmatige intelligentie

Samsung verbiedt AI-software na lekken broncode

Door Bright
2 mei 2023 11:11 • Aangepast 2 mei 2023 11:43

Beeld © Getty

AI raakt ook uitgevers en auteurs



Dirk Visser
Partner at Visser Schaap & Kreijger / Professor at Leiden Law School
Volledig profiel weergeven


Dirk Visser • 1e
Partner at Visser Schaap & Kreijger / Professor at Leiden Law School
1 w •

Ouderwets auteursrechtvoorbehoud weer belangrijk in tijden van AI

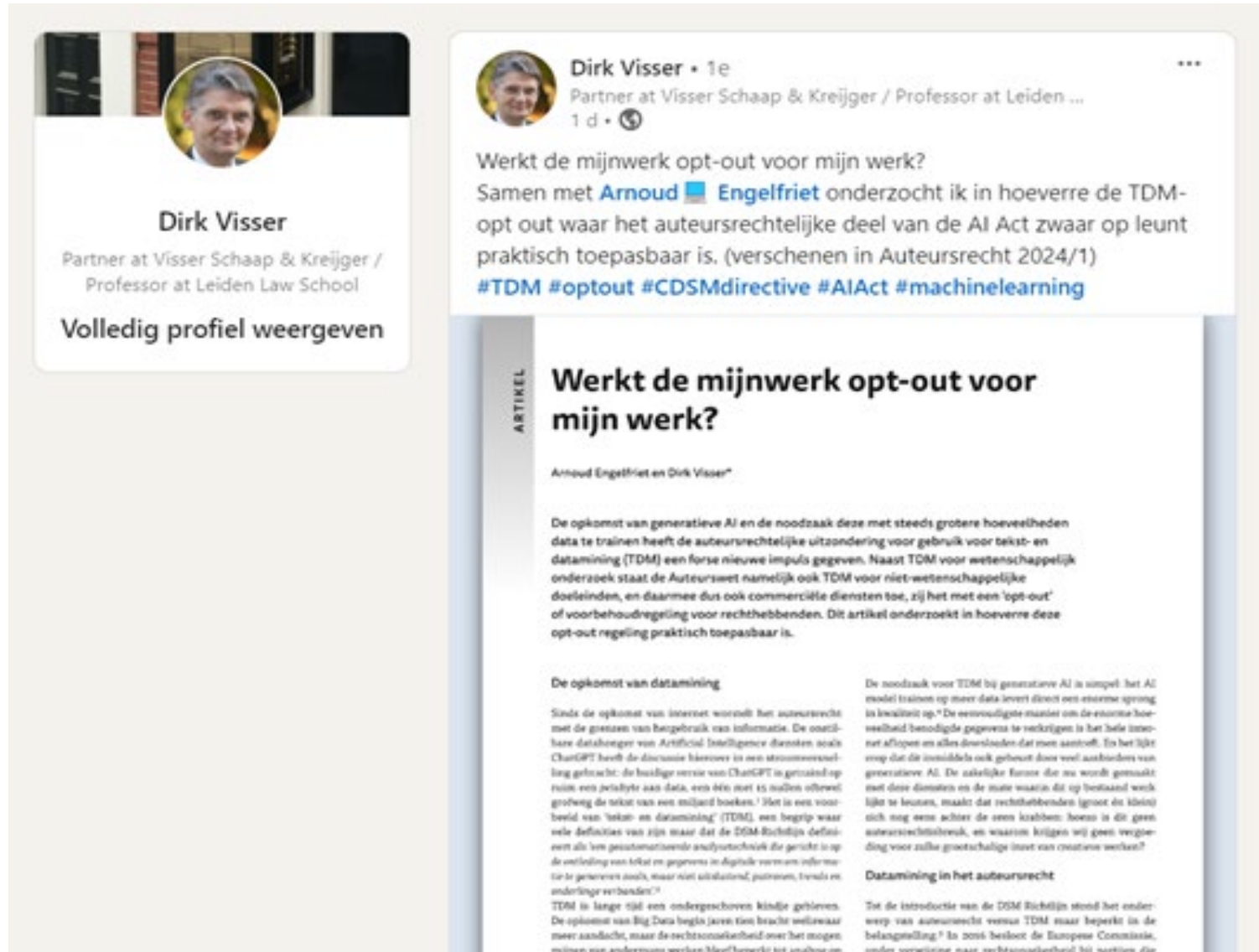
Uitgevers moeten de auteursrechten op hun uitgaves nadrukkelijk voorbehouden om ongewenste bewerking met AI te kunnen verbieden. En auteurs moeten dat voorbehoud maken ten opzichte van hun uitgevers.

<https://lnkd.in/em-wncTm>

#AI #auteursrecht #voorbehoud



Deze gaat wel dieper in op Auteursrecht en AI, maar toch



Dirk Visser
Partner at Visser Schaap & Kreijger / Professor at Leiden Law School
Volledig profiel weergeven

Dirk Visser • 1e
Partner at Visser Schaap & Kreijger / Professor at Leiden ...
1 d • 🌐

Werkt de mijnwerk opt-out voor mijn werk?
Samen met [Arnoud Engelfriet](#) onderzocht ik in hoeverre de TDM-opt out waar het auteursrechtelijke deel van de AI Act zwaar op leunt praktisch toepasbaar is. (verschenen in Auteursrecht 2024/1)
[#TDM](#) [#optout](#) [#CDSMDirective](#) [#AIAct](#) [#machinelearning](#)

ARTIKEL
Werkt de mijnwerk opt-out voor mijn werk?
Arnoud Engelfriet en Dirk Visser*

De opkomst van generatieve AI en de noodzaak deze met steeds grotere hoeveelheden data te trainen heeft de auteursrechtelijke uitzondering voor gebruik voor tekst- en datamining (TDM) een forse nieuwe impuls gegeven. Naast TDM voor wetenschappelijk onderzoek staat de Auteurswet namelijk ook TDM voor niet-wetenschappelijke doeleinden, en daarmee dus ook commerciële diensten toe, zij het met een 'opt-out' of voorbehoudsregeling voor rechthebbenden. Dit artikel onderzoekt in hoeverre deze opt-out regeling praktisch toepasbaar is.

De opkomst van datamining

Sinds de opkomst van internet wereldwijd het auteursrecht met de grenzen van het gebruik van informatie. De oorspronkelijke databeheer van Artificial Intelligence diensten, zoals ChatGPT heeft de discussie hierover in een stroomversnelling gebracht: de huidige versie van ChatGPT is getraind op ruim een petabyte aan data, een één met 15 nullen oftewel grofweg de tekst van een miljard boeken.¹ Het is een voorbeeld van 'tekst- en datamining' (TDM), een begrip waar vele definities van zijn maar dat de DSM Richtlijn definieert als 'een geautomatiseerde analysetechniek die gericht is op de ontdekking van teksten en gegevens in digitale vormen van informatie te genereren zoals, maar niet uitlokkend, patronen, trends en onderlinge verbanden'.²

TDM is lange tijd een ondergeschoven kindje gebleven. De opkomst van Big Data heeft jaren tien bracht weliswaar meer aandacht, maar de rechtszekerheid over het mogen minen van anderen werken bleef beperkt tot analyse op

De noodzaak voor TDM bij generatieve AI is simpel: het AI model traint op meer data levert direct een enorme sprong in kwaliteit op.³ De eenvoudigste manier om de enorme hoeveelheid benodigde gegevens te verkrijgen is het hele internet aflopen en alles downloaden dat men aantreft. In het licht erop dat dit inmiddels ook gebeurt door veel aanbieders van generatieve AI. De zakelijke formaten die nu wordt gemaakt met deze diensten en de mate waarin dit op bestaand werk lijkt te leunen, maakt dat rechthebbenden (groot en klein) zich nog eens achter de vingers krabben: hoest is dit geen auteursrechtsoverbreuk, en waarom krijgen wij geen vergoeding voor zulke grootschalige inzet van creatieve werken?

Datamining in het auteursrecht

Zet de introductie van de DSM Richtlijn stond het onderzoek van auteursrecht versus TDM maar beperkt in de belangstelling.⁴ In 2006 besloot de Europese Commissie, onder verwijzing naar rechtszekerheid bij partijen die

AI & desinformatie



AI-chatbots zijn politiek gekleurd: ChatGPT is links, Meta is rechts
© Aangeboden door Bright.nl

Onderzoekers hebben gekeken naar de ingebakken politieke voorkeur van AI-taalmodellen. Die blijkt per model flink te verschillen. Zo blijkt het model van Meta het meest rechts en autoritair en die van OpenAI het meest links.

INNOVATIONS

ChatGPT invented a sexual harassment scandal and named a real law prof as the accused

The AI chatbot can misrepresent key facts with great flourish, even citing a fake Washington Post article as evidence

By [Pranshu Verma](#) and [Will Oremus](#)

April 5, 2023 at 2:07 p.m. EDT

AI & desinformatie



Nepfoto van explosie bij Pentagon zorgt voor korte dip op Amerikaanse beurs

Door onze nieuwsredactie

23 mei 2023 om 01:02

Update: 8 maanden geleden

 94 reacties

 Delen

Een nepfoto van een explosie in de buurt van het Pentagon heeft maandag tot verwarring en een korte dip op de Amerikaanse beurs geleid. De afbeelding is hoogstwaarschijnlijk met kunstmatige intelligentie (AI) gemaakt.

“Foutje, bedankt”

Hoe een AI-gegenereerde foto in het NOS Journaal terecht kwam



Het is je misschien helemaal niet opgevallen, maar dat is precies het punt. In het NOS Journaal van 18.00 op donderdag 24 augustus zat een achtergrondfoto die niet echt was. De ‘schermfoto’ van koningspinguïns op Antarctica was geen echt archiefbeeld van die dieren, het was een door AI gegenereerde manipulatie.


Nieuwsbeeld dat op de redactie van NOS Nieuws binnenkomt wordt altijd nauwgezet gecontroleerd. Wat is de bron? Hoe zeker zijn we van tijdsbepaling en locatie? Kunnen we manipulatie uitsluiten? Bij twijfel gaan onze specialisten aan het werk, en proberen we – vaak met hulp van open source-technieken – nader onderzoek te doen voor we foto's of videobeeld publiceren.

Dat is nodig, want zeker nu artificiële intelligentie (AI) zo'n grote vlucht neemt, worden beeldmanipulaties steeds makkelijker te maken en steeds minder goed te herkennen.

In het NOS Journaal zie je niet alléén nieuwsbeelden, in de schermen achter en naast de presentator staat bij sommige onderwerpen ook stockmateriaal. Dat zijn tijdloze foto's die ter illustratie worden gebruikt. En met zo'n foto ging het donderdag fout.

New York Times vs. OpenAI ivm auteursrechtschending



Barry Scannell  • 2e

Leading AI Law Expert | Senior Lawyer in top ranked Irish l...

Mijn website bezoeken

3 w • 

+ Volgen ...

BIG AI LEGAL UPDATE!!! The New York Times has just filed a lawsuit against OpenAI and Microsoft, claiming copyright infringement, for “billions of dollars”.

The claim alleges the use millions of NYT articles without permission to train sophisticated large language models (LLMs), like GPT. This lawsuit, positioned at the intersection of AI and intellectual property rights, raises pivotal questions about the permissible limits of AI in the context of copyright.

The crux of the NYT's allegation is that OpenAI systematically replicated extensive volumes of its content during the development of AI models. This process, the lawsuit claims, involved not only unauthorised copying but also potentially undermined the NYT's business model by diverting readers and revenue away from its journalism.

Central to this case is the understanding that LLMs are fundamental to generative AI products. These models, trained on potentially billions of examples, predict text sequences, forming the backbone of AI-driven content generation. The training process of these models is intricate, involving setting model parameters by repetitively processing encoded copies of training materials, including, as alleged, content from the NYT.

US: massaschade claim OpenAi ivm privacy schendingen



Luiza Jarovsky • 2e

CEO at Implement Privacy, Author of The Privacy Whispere...

2 mnd •

+ Volgen ...

🔥 BREAKING: New class action against OpenAI over privacy violations. Below are some important quotes from the lawsuit:

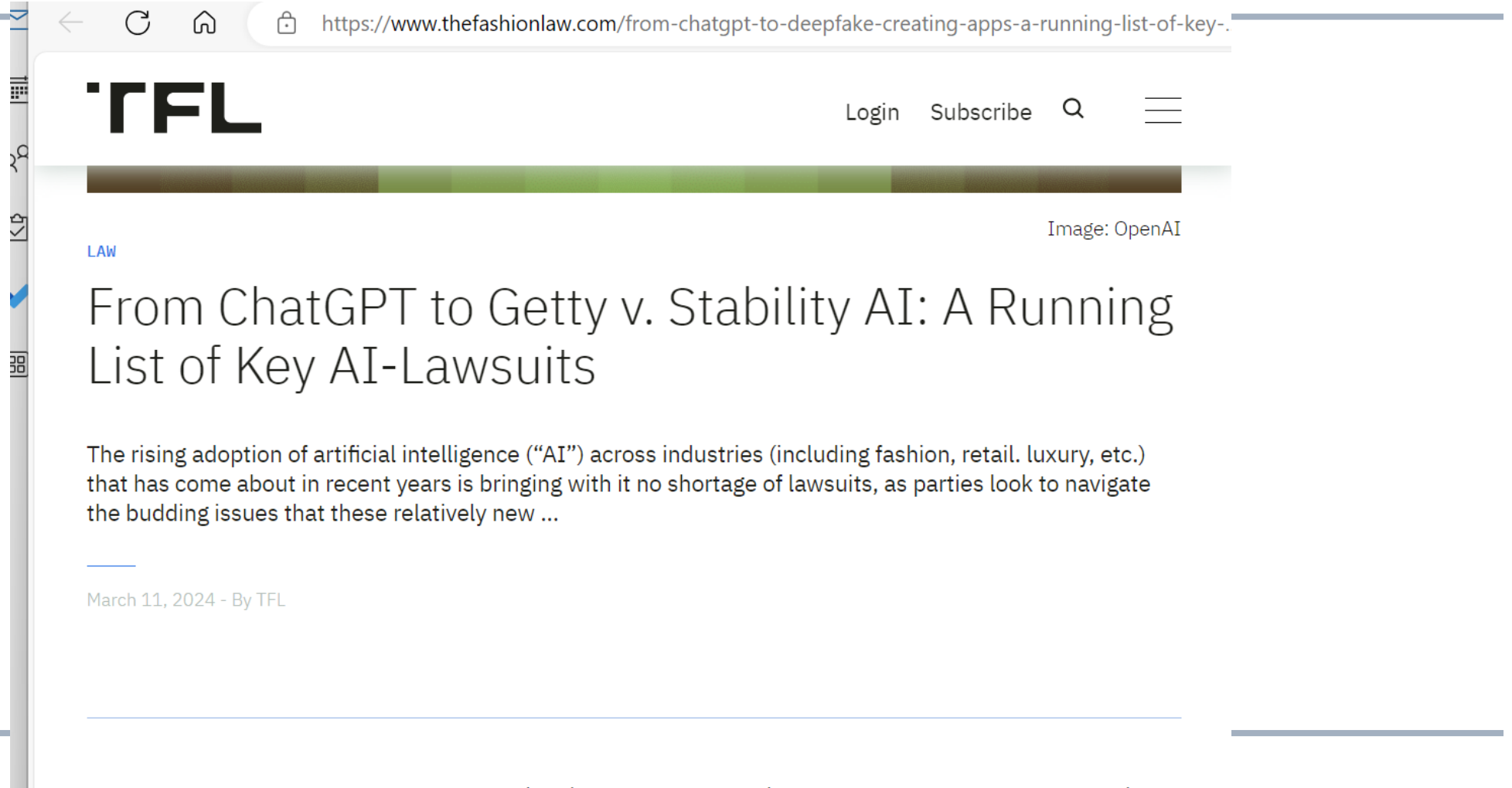
"The massive, unparalleled collection and tracking of users' personal information by Defendants endangers individuals' privacy and security to an incalculable degree. This information can be exploited and used to perpetrate identity theft, financial fraud, extortion, and other malicious purposes. It can also be employed to target vulnerable individuals with predatory advertising, algorithmic discrimination, and other unethical and harmful acts." (page 47)

-

"Given ChatGPT's ability to generate human-like understanding and responses, there is a high likelihood that users might share (and already are sharing) their private health information while interacting with the model, by asking health-related questions or discussing their medical history, symptoms, or conditions. Moreover, this information can be logged and reviewed as part of ongoing efforts to "train," improve and monitor each model's performance." (page 49)

-

The Fashion Law: overzicht belangrijke AI rechtzaken (US)



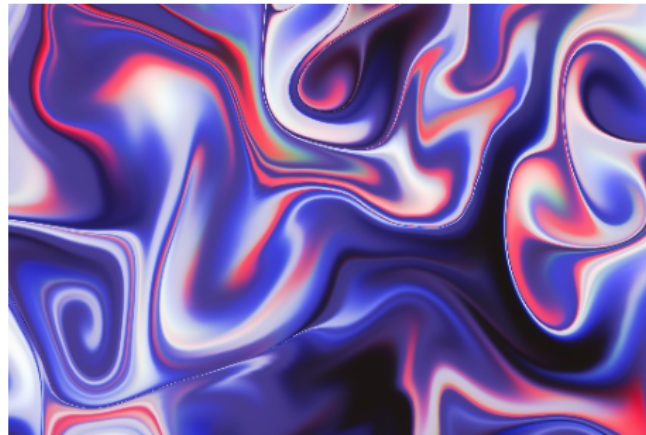
Voorbeelden massaschade (zie mn Github, open source)

Massaclaims tegen AI bedrijven

Amerika loopt op veel fronten voorop, zo ook wat betreft massa-claims die in verband met de opmars van AI zijn ingesteld. De basis van deze rechtszaken is steeds de ontwikkeling van de verschillende AI-modules die, kort gezegd, via bronnen op het internet zijn getraind. Daarmee zou vervolgens inbreuk worden gemaakt op verschillende rechten, waaronder auteursrecht (copyright) van de makers en privacy van de gebruikers van het internet.

2 oktober 2023

Blog ai auteursrecht massaclaim



Een kleine greep uit de ingestelde acties laat zien hoe divers deze klachten zijn die vrijwel vanaf het razendsnelle begin van ChatGPT zijn ingediend en steeds maar toenemen:


- AI in januari van dit jaar werd een procedure gestart tegen GitHub, Microsoft en OpenAI (de maker van ChatGPT). De klacht ziet op de manier waarop het AI-systeem zijn kennis vergaart, en de vraag hoe zich dit verhoudt tot open-source software dan wel fair use ervan.
- Kort daarna volgde de eerste zaak in verband met foto's. Zo begon GettyImages een zaak tegen Stability AI, die daarnaast werd betrokken bij een class action van kunstenaars in

Californië die hun pijlen ook hebben gericht op Midjourney en Deviant Art.


- In juli werd Google aangesproken op het scrapen van het internet en aansprakelijk gehouden voor een bedrag van USD 5 miljard, in september kwam er weer een zaak tegen OpenAI bij.

Duitse privacywaakhond start discussie over persoonsgegevens & AI

PREMIUM


Stefan Eder
do ut des
[+ Volgen](#)

Volledig profiel weergeven

Stefan Eder • 2e
do ut des
1 w • Bewerkt • 

[+ Volgen](#) ...

!!MUST READ!!GERMAN DATA PROTECTION REGULATOR ON PERSONAL DATA AND AI ▶ READ BEFORE YOU RUN YOUR AI APPLICATIONS ON REAL DATA


👉 Legal bases in data protection for the use of artificial intelligence 👉
a discussion paper by the [Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg](#)

👉 Read when and how may personal data be processed for the training and application of artificial intelligence ⚠️

[#dataprotection](#) [#artificialintelligence](#) [#regulator](#)

[Vertaling weergeven](#)

Legal bases in data protection for the use of artificial intelli... <https://www.baden-wuerttemberg.datenschutz.de/legal-base...>

 Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

**Legal bases in data protection
for the use of artificial intelligence**

When and how may personal data be processed for the training and application of artificial intelligence?

– Discussion paper. Version 1.0 from 07.11.2023 –

Privacyvragen toezichthouder over ChatGPT



AUTORITEIT
PERSOONSgegevens

Waar bent u naar o

[Home](#) [Thema's](#) **Actueel** [Documenten](#) [Contact](#) [FG's](#)

[Home](#) > [Actueel](#) >

AP vraagt om opheldering over ChatGPT

07 juni 2023 Thema's: [Algoritmes, AI en de AVG](#), [Persoonsgegevens op internet](#)

De Autoriteit Persoonsgegevens (AP) maakt zich zorgen om de omgang met persoonsgegevens bij organisaties die gebruikmaken van zogeheten generatieve artificiële intelligentie (AI), zoals ChatGPT. De AP onderneemt daarom de komende tijd verschillende acties. Als eerste heeft de AP software-ontwikkelaar OpenAI per brief om opheldering gevraagd over chatbot ChatGPT. De AP wil onder meer weten hoe OpenAI omgaat met persoonsgegevens bij het trainen van het onderliggende systeem.

ChatGPT is een chatbot die ogenschijnlijk overtuigende antwoorden kan geven op veel verschillende vragen. Gebruikers kunnen ChatGPT bijvoorbeeld vragen hun wiskundehuiswerk te doen of computercode te schrijven. Of ze kunnen de chatbot gebruiken om advies te vragen bij



[Home](#) > [Actueel](#) >

Blogpost: zorgen om generatieve AI

07 december 2023 Thema's: [Coördinatie toezicht algoritmes & AI](#), [Algoritmes uitgelegd](#)

De Autoriteit Persoonsgegevens (AP) houdt toezicht op alle soorten verwerkingen van persoonsgegevens. Dus ook op algoritmes en AI waarbij persoonsgegevens worden verwerkt. Sinds dit jaar is ons toezicht op algoritmes en AI intensiever. In een aantal blogposts gaan we in op de maatschappelijke, juridische en technologische aspecten van de inzet van algoritmes en AI. We trappen af met Cecile Schut, directeur Systeemtoezicht, Beveiliging en Technologie bij de AP.

We zien een explosieve stijging van het gebruik van generatieve AI-toepassingen. Dagelijks komen er nieuwe apps bij. AI-tools, al dan niet gebaseerd op taalmodellen, lijken als paddenstoelen uit de grond te schieten. Overheden en bedrijven zien voordelen voor hun werknemers, maar ook voor burgers en klanten.

AI-toepassingen waarbij op basis van opdrachten ('prompts') inhoud wordt gecreëerd, heten generatieve AI. Bijvoorbeeld tekst, computercode, afbeeldingen, geluid of video. Naar verwachting zal generatieve AI de komende periode steeds meer worden toegepast.

Is AI-gegeneerd werk wel of niet IE beschermd?



Fulco Blokhuis • 1e
Experienced IP & Tech Lawyer @ Boekx Advocaten
1 w • Bewerkt •

Is a [#generative #ai](#) created work protected by [#copyright](#)?

✘ No, said the US Copyright office in several cases, such as , Zaria of the Dawn, Thaler and Suryas. (see the blog of [Franklin Graves https://lnkd.in/e2UQNGyj](https://lnkd.in/e2UQNGyj))

✔ In South Korea and China, the answer is yes. (<https://lnkd.in/e6qqWr7c>)

The film 'AI Suro's Wife' was entirely produced with generative artificial intelligence (GAI). It received copyright recognition from the Korea Copyright Commission (KCC) for the first time in South Korea and was registered as an 'edited work'. The KCC recognised the contribution of [#technology](#) and the efforts of a human.

A number of AI programs were used in production. After creating scenarios with large language models ([#LLM](#)) such as 'GPT-4', 'ClovaX', and 'GPT-3.5', images were created using 'Midjourney' and 'Stable Diffusion AI Art Generator'. Videos were created using video creation AI such as 'Zen 2' and 'D-ID', and even the characters' voices were created using 'Clova Dubbing'. Ultimately, music was created using 'Soundrow'.

According to the news article the producer Nara Knowledge Information played a very large role in editing as well as fine-tuning the creation AI.

To avoid copyright litigation such as the cases against Midjourney and Stable Diffusion, the producer added retouching work to the images. A somewhat similar retouching element was not sufficient for the US Copyright office to grant protection when a photo was mixed with a Van Gogh style with an GAI tool.

Aanpassing model auteursovereenkomst MEVW

Artikel 2.5

De Auteur voert de Opdracht persoonlijk uit. Het inschakelen van derden *en het gebruik van kunstmatige intelligentie* is niet toegestaan zonder toestemming van de Uitgever.

Artikel 4.3

De Auteur verklaart over het volledige auteursrecht op het Werk te beschikken en dit onbezwaard te kunnen overdragen. *De Auteur verklaart bij het tot stand brengen van de door Auteur aangeleverde inhoud niet zonder schriftelijke toestemming van de Uitgever en niet zonder adequate bronvermelding gebruik te hebben gemaakt van input van derden of van kunstmatige intelligentie die mogelijk beschermd is, inbreuk maakt op de rechten van derden of anderszins onrechtmatig is.* De Auteur vrijwaart de Uitgever tegen alle vorderingen van derden ten aanzien van de door Auteur aangeleverde inhoud.

Ook aan de toelichting bij de model auteursovereenkomst zijn twee zinnen toegevoegd:

1. Bij de toelichting op **artikel 2** is de zin toegevoegd: *De auteur wordt geacht het werk zelf tot stand te brengen. Gebruik van kunstmatige intelligentie is in verband met de bescherming, beloning en betrouwbaarheid van de inhoud alleen toegestaan met toestemming van de Uitgever.*
 2. Bij de toelichting op **artikel 4** is de zin toegevoegd: *Gebruik van kunstmatige intelligentie is in verband met de bescherming en betrouwbaarheid van de inhoud en in verband met de aansprakelijkheid alleen toegestaan met toestemming van de Uitgever en met adequate bronvermelding.*
-

AI uitsluiten in contracten



Arnoud Engelfriet (He/Him) • ...

Partner at ICTRecht B.V. and Co
Founder at Lynn Legal / JuriBlox...

1 u • 🌐

Goh, eerste keer dat ik zo expliciet AI modellen langs zie komen in een juridisch contract. Gelukkig maar dat NDA Lynn geen generatieve AI is...

1.5. Recipient shall not use any third-party generative AI models (such as ChatGPT, DALL-E2, Bing, Bard or any other similar models) in relation to the Confidential Information. Failure to comply with this clause shall be deemed an unauthorized disclosure of Confidential Information.

👍💡🗨️ 15

3 commentaren

Wat zijn de juridische aandachtspunten bij Gen AI?

Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity

35 Pages • Posted: 17 Jan 2024

[Claudio Novelli](#)

University of Bologna- Department of Legal Studies; Yale University - Digital Ethics Center

[Federico Casolari](#)

Alma Mater Studiorum - University of Bologna

[Philipp Hacker](#)

European University Viadrina Frankfurt (Oder) - European New School of Digital Studies

[Giorgio Spedicato](#)

Department of Legal Studies, University of Bologna

[Luciano Floridi](#)

Yale University - Digital Ethics Center; University of Bologna- Department of Legal Studies

Date Written: January 14, 2024

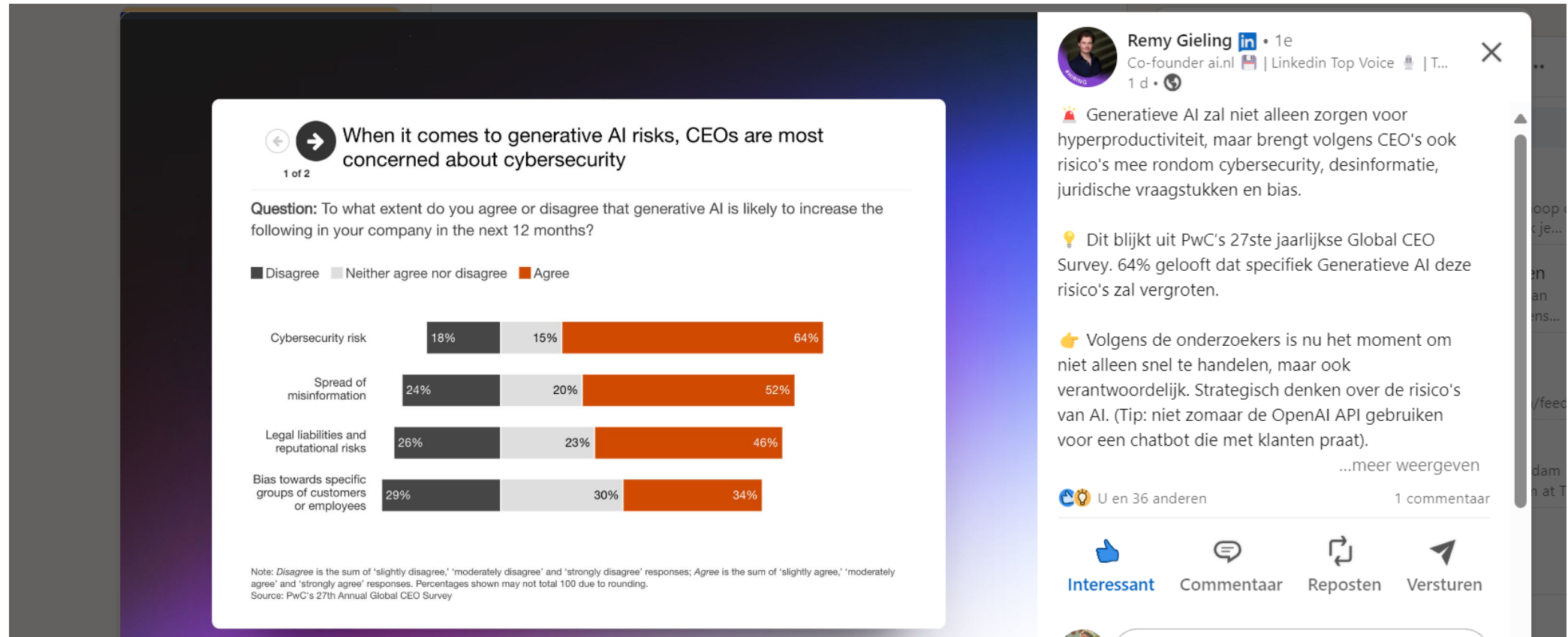
Abstract

The advent of Generative AI, particularly through Large Language Models (LLMs) like ChatGPT and its successors, marks a paradigm shift in the AI landscape. Advanced LLMs exhibit multimodality, handling diverse data formats, thereby broadening their application scope. However, the complexity and emergent autonomy of these models introduce challenges in predictability and legal compliance. This paper delves into the legal and regulatory implications of Generative AI and LLMs in the European Union context, analyzing aspects of liability, privacy, intellectual property, and cybersecurity. It critically examines the adequacy of the existing and proposed EU legislation, including the Artificial Intelligence Act (AIA) draft, in addressing the challenges posed by Generative AI in general and LLMs in particular. The paper identifies potential gaps and shortcomings in the legislative framework and proposes recommendations to ensure the safe and compliant deployment of generative models, ensuring they align with the EU's evolving digital landscape and legal standards.

De specifieke bedenkingen in de adviezen hebben betrekking op de volgende punten:

- De trainingsdata, veelal verkregen via grootschalige *scraping* (het extraheren van informatie van webpagina's) van openbare bronnen op internet of andere digitale bronnen, kunnen privacygevoelige gegevens bevatten;
- Het getrainde generatieve AI model kan onjuiste of bevooroordeelde gegevens over personen bevatten;
- De interactievragen van de gebruikers ('prompts') kunnen worden hergebruikt om het model te *finetunen*, waardoor onbedoeld gevoelige informatie openbaar kan worden gemaakt;
- Een generatieve AI-toepassing kan zeer gevoelige informatie afleiden uit de interactie met de gebruiker;
- De rechten van betrokkenen zoals de mogelijkheid tot inzage- en het eventueel verwijderen, of rectificeren van (onjuiste) persoonsgegevens zijn momenteel zeer beperkt;
- Het gebruik van generatieve AI brengt auteursrechtelijke risico's met zich mee, omdat onduidelijk is of aanbieders voldoende rekening houden met de rechten van auteurs, wiens werken zij bij de ontwikkeling van hun modellen gebruiken. Veel aanbieders zijn momenteel niet transparant over welke auteursrechtelijke werken zij gebruiken in het trainingsproces; en
- Vanuit de rechtspraak is er nog geen expliciet oordeel over of, en in welke vorm, *scraping* -ten behoeve van het trainen van generatieve AI modellen- auteursrechtelijk gezien toelaatbaar is.

Recent onderzoek PWC onder CEO's over GenAI





De risico's op een rijtje:

- Auteursrecht & Plagiaat
- Accuratesse resultaten
- Bias in output (discriminatie)
- Verlies van bedrijfsgeheimen en know-how
- Verlies / Risico's voor eigen IP
- Privacy inbreuken
- Schadelijke content, desinformatie
- Beveiligingsrisico's, zoals het maken van malware of ransomware code, phishing emails Reputational risk
- Reputatie

De belangrijkste risico's in een overzichtje

(met dank aan concullega Lokke):

Accuracy	Confidentiality	Intellectual Property	Data Protection
<ul style="list-style-type: none">• Incorrect or incomplete output• Hallucination (fake facts)	<ul style="list-style-type: none">• Unauthorized disclosure of confidential and proprietary information	<ul style="list-style-type: none">• Lack of license for use of copyrighted training data• Output infringes third-party IP• Lack of IP ownership on output	<ul style="list-style-type: none">• Lack of consent for use as training data• <u>Can't</u> comply with rights of data subjects to access and correction
<p style="text-align: center;">Regulatory Scrutiny Data protection, Unfair trade practice, Product safety & liability, IT security, anti-discrimination laws, human rights</p>			

Principes voor AI beleid

(met dank aan David Rosenthal)

How we deal with AI.

ABC AG

Safe, sensible and lawful use of AI at work? Watch the short video here: <https://vischerlnk.com/ai-intro>

Our principles for the use of AI

Accountability: Our organization ensures internal accountability and clear responsibilities for the development and use of AI. We act according to plan, not ad-hoc, and keep records of our AI applications. We understand and comply with legal requirements.

Transparency: We make the use of AI sufficiently transparent where this is likely to be important for people in relation to their dealings with us, for example where they would otherwise not be aware that they are interacting with AI, where AI plays a significant role in important decisions that affect them, and in the case of otherwise deceptive "deep fakes".

Fairness and non-harm: Our use of AI should be reasonable, fair and non-discriminatory for others. We pay attention to accessibility, a level playing field for us and those affected and to avoiding harm wherever possible – including to the environment. We are more cautious when it comes to vulnerable people.

Reliability: We ensure that our AI systems work as reliably as possible and achieve the most correct, predictable results. We take precautionary measures for the event that they do not do so.

Information security: We take measures to ensure the confidentiality, integrity and availability of AI applications and their information (including personal data, own/third-party secrets). We carefully regulate cooperation with third-party providers.

Proportionality and self-determination: We only use personal data where necessary and – where appropriate – leave the decision as to whether and to what extent AI is used to the people concerned. If AI is involved in important decisions, we check whether we must or should provide for human intervention for those affected.

Intellectual property: We observe copyright and industrial property rights in our use of AI and only use content and processes for which we have the necessary authorization. We also protect our own content.

Rights of data subjects: We ensure that we can grant data subjects their rights of access, correction and objection, despite of us using AI.

Explainability and human oversight: We only use AI systems that we can understand and control and that meet our quality requirements. We monitor them to detect and rectify errors and undesired effects.

Risk control: We understand and manage the risks associated with our use of AI, both for our organization and for individuals. We update our risk assessments on a regular basis.

Prevention of misuse: We implement measures to combat the misuse of our AI applications. We train our employees in the correct use of AI.

(Summary)

Which AI applications are permitted at our company and what for

Application	Allowed input	Further restrictions, comments	Owner
MS Copilot (commercial)	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Own personal data permitted	AB
VISCHER GPT	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		AB
DeepL Pro	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	You must be logged in	AB
	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		
	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		
	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		
	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		
	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		

Personal data, i.e. all information about others where third parties could determine who it relates to

Sensitive personal data, i.e. data relating to health, race, ethnicity, religious, political, ideological views or activities, privacy, administrative or criminal prosecution or sanctions, social welfare, genetic and uniquely identifying biometric data

Information that (where applicable) is subject to **professional or official secrecy** or a special statutory duty of confidentiality (e.g., social security secrecy)

Other **confidential information** or **proprietary content** of third parties, unless there is a confidentiality obligation or license agreement that prohibits any AI use of such info/content, even for own internal purposes

Our **own business secrets**, e.g., plans or internal financial indicators, except where highly confidential

→ Alternatively, personal data and confidential information can be anonymized or omitted as input

Remember this with every application:

- Inform** about the use of AI, if unexpected but relevant for those affected
- Use own or third-party **confidential data** and **personal data** only as permitted above
- Always **check the correctness of the output** manually before use

New AI application or use AI in a project? Unexpected **error** or **incident** caused by AI? Other **questions**?

petra.muster@abc.ch

The use of AI is only permitted if an owner has been designated for such use (in case of doubt, the person who orders/controls its use). He or she is internally responsible for ensuring compliance.





EU regulering van AI

Huidige ontwikkelingen

Artificial Intelligence Act

En:

Richtlijn AI-aansprakelijkheid

Modernisering Richtlijn Productaansprakelijkheid (political agreement bereikt op 14 december 2023)

Maar ook:

Verdrag over Artificiele Intelligentie, mensenrechten, democratie en de rechtsstaat

AI Act: Classificatie van verschillende AI

Een verdeling gebaseerd op risico

4 levels (in de Act staan er eigenlijk 3):

1. Onacceptabel risico (verboden)
2. Hoog risico (hier gaat de AI act vooral over)
3. Gelimiteerd risico (transparantieverplichtingen)
4. Geen risico (geen verplichtingen)



De AI - Act in één oogopslag (via Kees van den Tempel)

Overlap AVG	Regel AI-systemen	Risico	Soort systemen	Toezicht	Handhaving
N.V.T	Deze AI-systemen zijn verboden om te gebruiken of maken binnen de EU	Onacceptabel Risico = VERBODEN	AI-systemen die menselijk gedrag manipuleren of hun kwetsbaarheden misbruiken en zo hun vrije wil onzeilen. (Real-time) biometrische identificatiesystemen op afstand in openbare ruimtes. Biometrische categoriseringssystemen en/of voorspellend politiewerk met kenmerken zoals geslacht, etnische afkomst, religie, eerder crimineel gedrag. Emotieherkenning bij wetshandhaving, grenscontrole, werkplek en onderwijs. Biometrische gegevens van sociale media of videos tbv gezichtsherkenning. Sociale scores die leiden tot discriminatie in sociale contexten. AI die kwetsbaarheden van een specifieke groep mensen uitbuut.	Onaangekondigde inspecties door Autoriteit Persoonsgegevens (AP)	30 miljoen euro of 6 procent van de jaarlijkse wereldwijde omzet
Deze systemen gebruiken grote hoeveelheden persoonsgegevens, wat een uitdaging kan vormen voor naleving van de AVG, vooral in termen van gegevensminimalisatie, beveiliging en transparantie	VERPLICHT contact met toezichthouder over kwaliteits- en risicomanagement, Data governance. Kwaliteitseisen voor trainings-, test- en validatiegegevens, Logging, Documentatie van systeemarchitectuur, algoritme en werking, Effectbeoordeling van de grondrechten, Menselijk toezicht, Conformiteitsverklaring, CE-markering en registratie in EU-databank	Hoog Risico Voldoen aan EU-regels(en menselijk toezicht) tijdens hele levensduur	Systemen die een directe impact hebben op het leven van mensen zoals: biometrische en biometrisch ondersteunde systemen, Systemen tbv beheer en exploitatie van kritieke infrastructuur, Algemeen- en beroepsonderwijsystemen, Systemen van openbare (overheids) diensten, Systemen tbv werkgelegenheid, personeelsbeheer, politie, migratie, asiel en grenscontrole, justitie en democratische processen (politieke campagnes), fraude-detectie	Onaangekondigde inspecties ter plaatse en op afstand door AP, gecoördineerd door AI Office → ook sector specifieke toezichthouders	30, 20 of 10 miljoen euro of 6, 4 of 2 procent van de jaarlijkse wereldwijde omzet, afh van soort overtreding
Het gebruik van veel gegevens i.r.t.de AVG (minimale gegevensverwerking, juistheid en doelbinding) kan een uitdaging vormen	VERPLICHT: technische documentatie, het naleven van de EU-auteursrechtwetgeving, gedetailleerde samenvattingen van de training dataset, gedragscode, vijandige tests, rapportage ernstige incidenten en energie-efficiëntie	Gelimiteerd risico, high impact Strenge transparantie eisen tijdens de hele levensduur	Dit is een speciale categorie, General Purpose AI systemen (GPAI-systemen) zoals foundation models, large language models zoals Bard (google), ChatGPT (OpenAI), Q (Amazon), Claude (Anthropic), en overige generatieve AI-systemen zoals Midjourney, RunWay, Whisperer die onderdeel kunnen zijn van een ander IT-systeem.	Onaangekondigde inspecties ter plaatse en op afstand door de AI Office (zie onder) → ook sector specifieke toezichthouders	Nog onduidelijk, maar in lijn met boven- en onderstaande boetes
Consumenten informeren komt overeen met de vereisten van de AVG voor transparantie en informatieverstrekking	Consumenten informeren over het AI-systeem, Gedragscode (aanbevolen)	Gelimiteerd risico Transparantie eisen tijdens de hele levensduur	AI-systemen die rechtstreeks met mensen communiceren: o.a. emotieherkenningssystemen, biometrische categoriseringssystemen, door AI gegenereerde of gewijzigde inhoud die lijkt op echte personen, objecten, plaatsen of gebeurtenissen (deep fake)	Onaangekondigde inspecties ter plaatse en op afstand door AP, gecoördineerd door AI Office → ook sector specifieke toezichthouders	10 miljoen euro of 2 procent van de jaarlijkse wereldwijde omzet, i.h.g.v. onvolledige info
Basisprincipes van gegevensbescherming onder de AVG in acht nemen, zoals gegevensbeveiliging en gebruikersconsent	Gedragscode (aanbevolen)	Minimaal Risico: Geen verplichtingen	Alle systemen die niet in bovenstaande categorieën vallen: systemen t.b.v. voorspellend onderhoud, Spam filters, video games, magazijn systemen, research & development (in sandbox), systemen die geen impact hebben op individuele personen	N.v.t.	N.v.t

Ontwikkelaars, importeurs, leveranciers van AI-systemen passen zelf de regels toe en bepalen zelf de risico-classes (self-assessment)
De EU-Act bevordert zogenaamde 'regulatory sandboxes' en 'real-world-tests', opgezet door nationale autoriteiten om innovatieve AI te ontwikkelen

Copyright © 2024, drs Kees van den Tempel mba, AI-Labs BV



Franse toezichthouder: leverancier AI is Verantwoordelijke

CNIL on re-use of data

Opinie CNIL (Frans toezichthouder)

Analyse over rollen van AI-leveranciers in context van de AVG

- Onderscheid tussen datagebruik voor dienstverlening aan eigen klanten en datagebruik om AI-oplossingen voor derden te ontwikkelen en te trainen.

Verwerker (cloudopslagdienst/chatbotleverancier) wil trainen met gegevens die ze hebben van de vww. Mag dat?

- Dat mag, maar wel met uitdrukkelijke toestemming van verwerkingsverantwoordelijke
- Het moet aansluiten op doel waarvoor gegevens zijn verstrekt

Bron: Adviesrapport CNIL

Zaak Google Spain/Gonzalez

Gerechtvaardigd belang:

- Belangenafweging
- Bijzondere persoonsgegevens



Zaak Meta

- Meta verzamelde persoonsgegevens van gebruikers, op het Facebookplatform, maar ook via andere website en diensten van Meta;
- Deze persoonsgegevens verkocht Meta aan andere partijen, zodat deze persoonlijke advertenties aan Facebookgebruikers konden tonen;
- Tussen deze verzamelde persoonsgegevens konden ook bijzondere persoonsgegevens zitten (het geheel moet als bijzonder worden gezien);
- Meta plaatste het verwerken onder de rechtsgrond *noodzakelijk voor het uitvoeren van de overeenkomst*, en later onder hun *gerechtvaardigde belang*;
- Het Hof heeft aangegeven dat Meta zich niet op deze rechtsgronden kan beroepen: er is *toestemming* van de gebruiker nodig.





Italiaanse privacywaakhond: OpenAI schendt AVG

ChatGPT: Italian DPA notifies breaches of privacy law to OpenAI

The Italian DPA (Garante per la protezione dei dati personali) notified breaches of data protection law to OpenAI, the company behind ChatGPT's AI platform.

Following the [temporary ban](#) on processing imposed on OpenAI by the Garante on 30 March of last year, and based on the outcome of its fact-finding activity, the Italian DPA concluded that the available evidence pointed to the existence of breaches of the provisions contained in the EU GDPR.

OpenAI may submit its counterclaims concerning the alleged breaches within 30 days.

The Italian Garante will take account of the work in progress within the ad-hoc [task force](#) set up by the European Data Protection Framework (EDPB) in its final determination on the case.

Rome, 29 January 2024

AI & IE



Oude wijn in nieuwe zakken? (auteursrecht van een aap)



Is AI-gegenereerd werk wel of niet IE beschermd?



Fulco Blokhuis • 1e
Experienced IP & Tech Lawyer @ Boekx Advocaten
1 w • Bewerkt •

Is a [#generative #ai](#) created work protected by [#copyright](#)?

✗ No, said the US Copyright office in several cases, such as , Zaria of the Dawn, Thaler and Suryas. (see the blog of [Franklin Graves https://lnkd.in/e2UQNGyj](https://lnkd.in/e2UQNGyj))

✓ In South Korea and China, the answer is yes. (<https://lnkd.in/e6qqWr7c>)

The film 'AI Suro's Wife' was entirely produced with generative artificial intelligence (GAI). It received copyright recognition from the Korea Copyright Commission (KCC) for the first time in South Korea and was registered as an 'edited work'. The KCC recognised the contribution of [#technology](#) and the efforts of a human.

A number of AI programs were used in production. After creating scenarios with large language models ([#LLM](#)) such as 'GPT-4', 'ClovaX', and 'GPT-3.5', images were created using 'Midjourney' and 'Stable Diffusion AI Art Generator'. Videos were created using video creation AI such as 'Zen 2' and 'D-ID', and even the characters' voices were created using 'Clova Dubbing'. Ultimately, music was created using 'Soundrow'.

According to the news article the producer Nara Knowledge Information played a very large role in editing as well as fine-tuning the creation AI.

To avoid copyright litigation such as the cases against Midjourney and Stable Diffusion, the producer added retouching work to the images. A somewhat similar retouching element was not sufficient for the US Copyright office to grant protection when a photo was mixed with a Van Gogh style with an GAI tool.

USCO: notice of inquiry and request for comments



Franklin Graves • 2e

Attorney passionate about emerging technology, intellectual p...

4 d • 🌐

+ Volgen

Grab your quill pen, fountain pen, or glitter gel pen, folks! It's time to write to the [U.S. Copyright Office](#) with our thoughts on [#AI](#) and [#copyright](#)!

The official notice of inquiry (NOI) and request for comments is live, with comments due by October 18th. Reply comments by November 15th.

The USCO identifies four issue areas of focus:

- (1) the use of copyrighted works to train AI models;
- (2) the copyrightability of material generated using AI systems;
- (3) potential liability for infringing works generated using AI systems; and
- (4) the treatment of generative AI outputs that imitate the identity or style of human artists.

The questions start high-level, and then get into more granular topics.

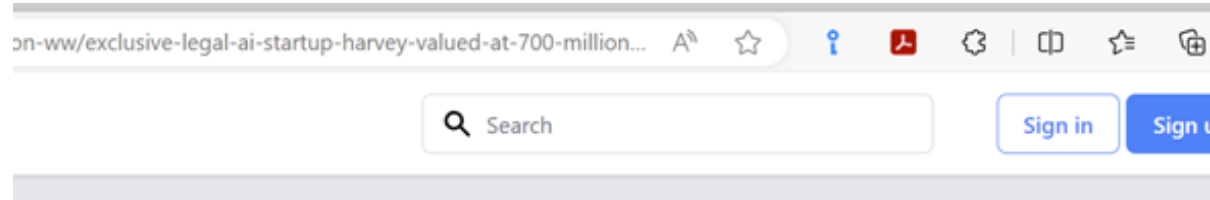
The USCO also included a glossary of terms, which is super helpful this time around! We needed one for the NFT one last year.

Excited to dive in and work on helping prepare comments to the USCO through various organizations I support 🤝

I've still yet to decide which pen will be used... but for sure Taylor Swift will be helping to keep focused 🙌

<https://lnkd.in/eSNqpBKZ>

Legal AI start-up Harvey gewaardeerd op 700 mio



I The Information

Harvey, a one-year-old startup that sells artificial intelligence-powered legal software, is in talks to raise between \$70 million and \$80 million in a round that would value it at \$700 million including the investment, two people familiar with financing said. The funding more than quadruples its valuation announced in April, indicating investors are still hungry for AI startups that can show revenue growth.

Venture firm Kleiner Perkins and solo investor Elad Gil, who previously invested in the company's seed and Series A rounds, are set to co-lead the round, the people familiar said. Existing investors Sequoia Capital and OpenAI Startup Fund will participate as well, these people said.

[READ THE FULL STORY](#)



Roep om AI in advocatuur/juristerij is er al langer

Opinie • 1 mei '23 15:00

De tekstverwerking van juristen kan met AI veel beter en goedkoper

 Douwe Groenevelt

Advocatenkantoren sturen stevige facturen voor wat in de kern gewoon tekstverwerking is. De komst van GPT-4 maakt het werk van juristen een stuk goedkoper voor de cliënt, voorspelt Douwe Groenevelt.

Advertentie

FD eerder dit jaar over AI in advocatuur (1)

5 jan 16:42

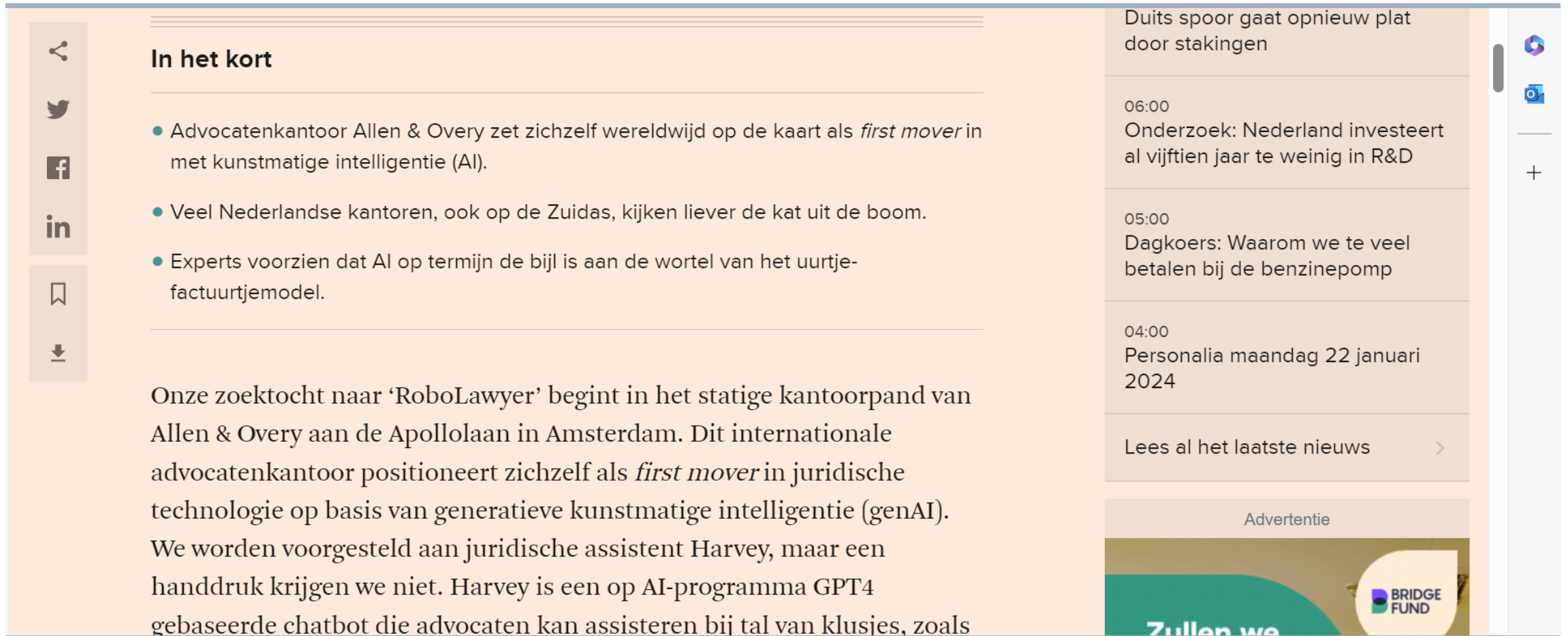
Wat doet een kunstmatig intelligente advocaat nu eigenlijk de hele dag?



Joris Polman, Edwin van der Schoot, Johan Leupen

Steeds meer advocaten werken met generatieve kunstmatige intelligentie. Dat bespaart tijd en kosten, zo luidt de belofte. Aanleiding voor het FD om te onderzoeken hoe goed 'RoboLawyer' al is, en de hype van de werkelijkheid te scheiden.

FD recent over AI in advocatuur (2)



In het kort

- Advocatenkantoor Allen & Overy zet zichzelf wereldwijd op de kaart als *first mover* in met kunstmatige intelligentie (AI).
- Veel Nederlandse kantoren, ook op de Zuidas, kijken liever de kat uit de boom.
- Experts voorzien dat AI op termijn de bijl is aan de wortel van het uurtje-factuurtjemodel.

Onze zoektocht naar ‘RoboLawyer’ begint in het statige kantoorpand van Allen & Overy aan de Apollolaan in Amsterdam. Dit internationale advocatenkantoor positioneert zichzelf als *first mover* in juridische technologie op basis van generatieve kunstmatige intelligentie (genAI). We worden voorgesteld aan juridische assistent Harvey, maar een handdruk krijgen we niet. Harvey is een op AI-programma GPT4 gebaseerde chatbot die advocaten kan assisteren bij tal van klusjes, zoals

Duits spoor gaat opnieuw plat door stakingen

06:00
Onderzoek: Nederland investeert al vijftien jaar te weinig in R&D

05:00
Dagkoers: Waarom we te veel betalen bij de benzinepomp

04:00
Personalia maandag 22 januari 2024

[Lees al het laatste nieuws](#)

Advertentie

Zullen we

BRIDGE FUND

Allen & Overy lanceert AI contractsonderhandelaar



British law firm [Allen & Overy](#) has introduced an artificial intelligence (AI)-powered contract negotiation tool.

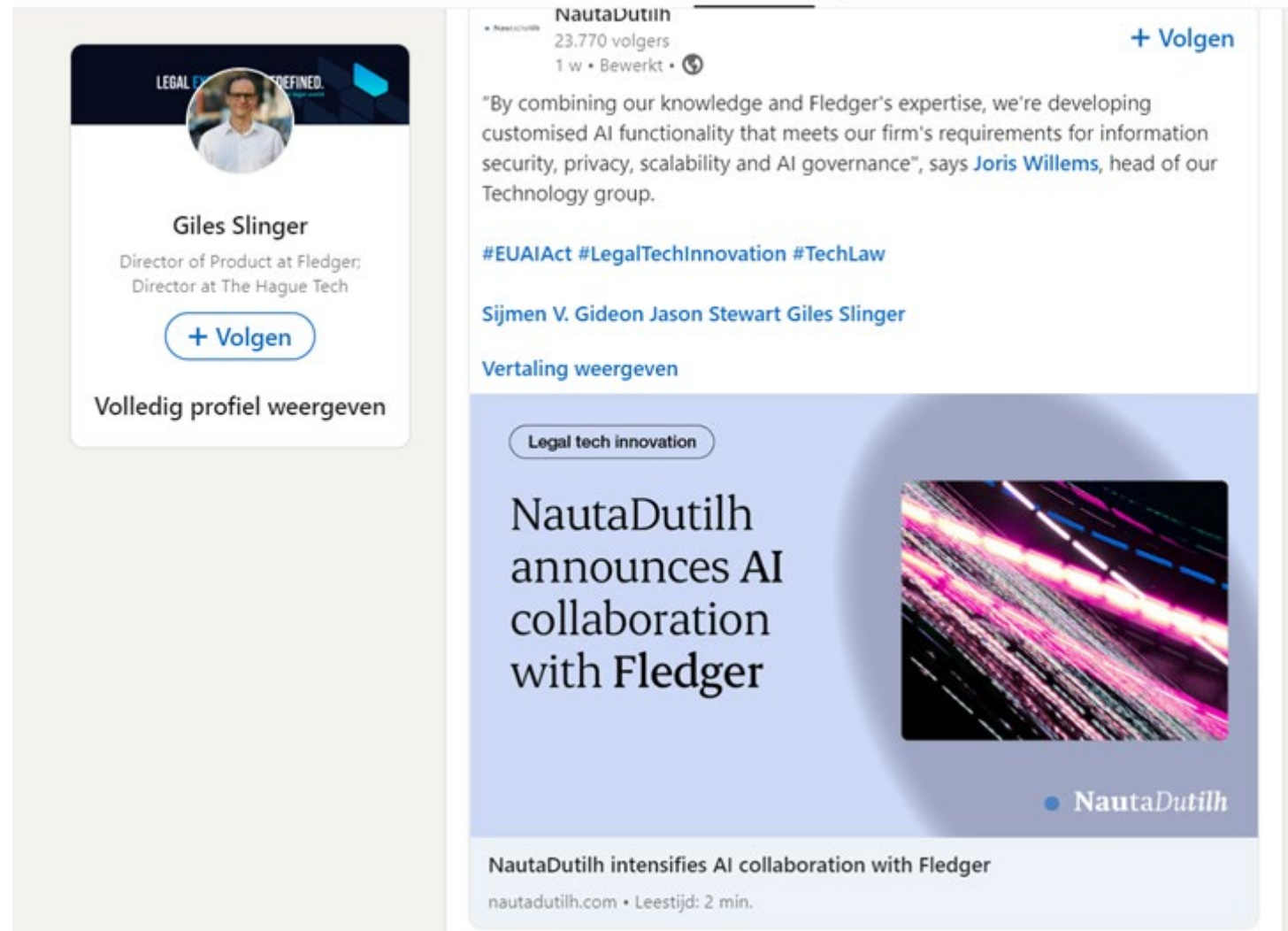
The new product, the subject of a Thursday (Dec. 21) [Financial Times \(FT\) report](#), was created in partnership with [Microsoft](#) and AI legal startup [Harvey](#), and comes as the technology is increasingly being incorporated into the legal world.

According to the report, the service – called ContractMatrix – draws on existing contract templates to create new agreements that attorneys can then amend or accept. Allen & Overy (A&O) estimated it would trim up to seven hours off contract negotiations.

The firm says more than 1,000 attorneys are using the tool, with five of its clients signed up to begin using the platform starting next month.


The FT report notes that generative AI's entry into the legal world could lead to job losses and reduced revenue by cutting billable hours and entry-level work.

Nauta kondigt recent ook een samenwerking aan met Fledger AI



The image shows a LinkedIn profile and a post. On the left is the profile of Giles Slinger, Director of Product at Fledger and Director at The Hague Tech. On the right is a post from NautaDutilh (23,770 followers) dated 1 week ago. The post text reads: "By combining our knowledge and Fledger's expertise, we're developing customised AI functionality that meets our firm's requirements for information security, privacy, scalability and AI governance", says [Joris Willems](#), head of our Technology group. The post includes hashtags #EUAIAct, #LegalTechInnovation, and #TechLaw, and lists users Sijmen V. Gideon, Jason Stewart, and Giles Slinger. Below the text is a video player with a thumbnail showing colorful light trails and the title "NautaDutilh announces AI collaboration with Fledger". The video player includes a "Legal tech innovation" tag and the NautaDutilh logo. At the bottom of the video player, it says "NautaDutilh intensifies AI collaboration with Fledger" and "nautadutilh.com • Leestijd: 2 min."

Giles Slinger
Director of Product at Fledger;
Director at The Hague Tech
[+ Volgen](#)
Volledig profiel weergeven

NautaDutilh
23.770 volgers
1 w • Bewerkt • 

[+ Volgen](#)

"By combining our knowledge and Fledger's expertise, we're developing customised AI functionality that meets our firm's requirements for information security, privacy, scalability and AI governance", says [Joris Willems](#), head of our Technology group.


[#EUAIAct](#) [#LegalTechInnovation](#) [#TechLaw](#)

[Sijmen V. Gideon](#) [Jason Stewart](#) [Giles Slinger](#)

[Vertaling weergeven](#)

[Legal tech innovation](#)

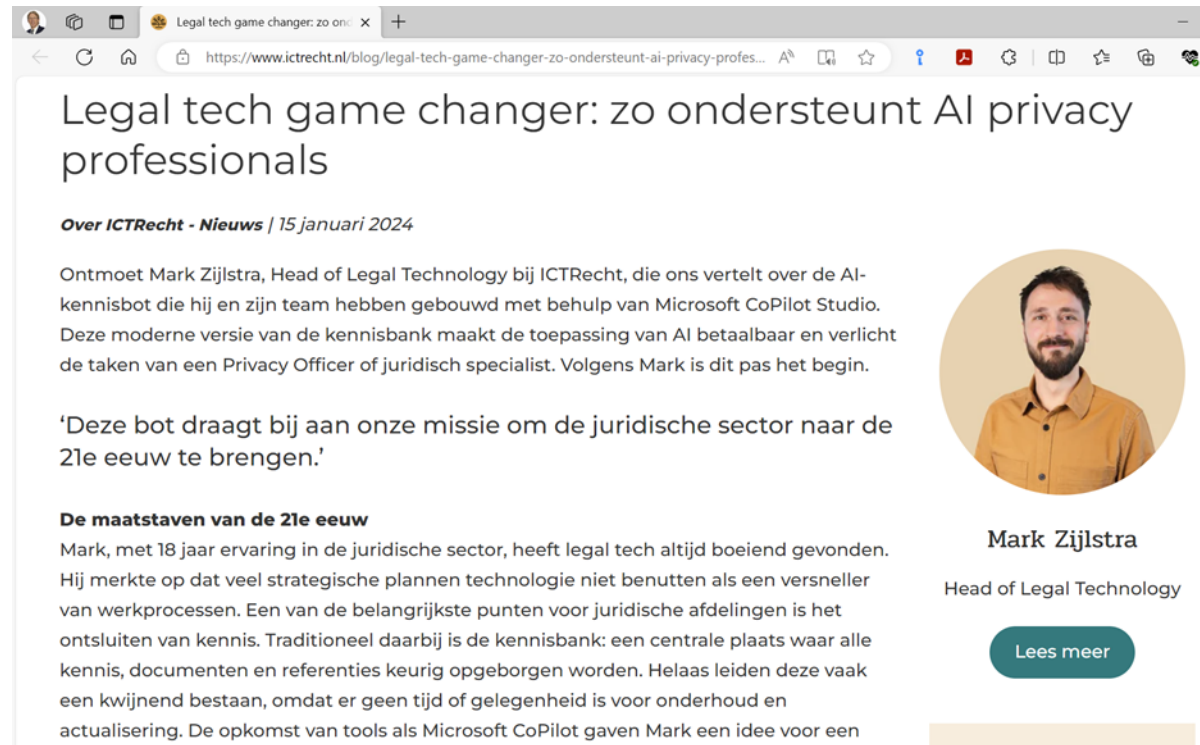
NautaDutilh
announces AI
collaboration
with Fledger



[NautaDutilh](#)

NautaDutilh intensifies AI collaboration with Fledger
nautadutilh.com • Leestijd: 2 min.

AI bot ter ondersteuning van Privacy



Legal tech game changer: zo ondersteunt AI privacy professionals


Over ICTRecht - Nieuws / 15 januari 2024

Ontmoet Mark Zijlstra, Head of Legal Technology bij ICTRecht, die ons vertelt over de AI-kennisbot die hij en zijn team hebben gebouwd met behulp van Microsoft CoPilot Studio. Deze moderne versie van de kennisbank maakt de toepassing van AI betaalbaar en verlicht de taken van een Privacy Officer of juridisch specialist. Volgens Mark is dit pas het begin.

'Deze bot draagt bij aan onze missie om de juridische sector naar de 21e eeuw te brengen.'

De maatstaven van de 21e eeuw

Mark, met 18 jaar ervaring in de juridische sector, heeft legal tech altijd boeiend gevonden. Hij merkte op dat veel strategische plannen technologie niet benutten als een versneller van werkprocessen. Een van de belangrijkste punten voor juridische afdelingen is het ontsluiten van kennis. Traditioneel daarbij is de kennisbank: een centrale plaats waar alle kennis, documenten en referenties keurig opgeborgen worden. Helaas leiden deze vaak een kwijnend bestaan, omdat er geen tijd of gelegenheid is voor onderhoud en actualisering. De opkomst van tools als Microsoft CoPilot gaven Mark een idee voor een



Mark Zijlstra
Head of Legal Technology

[Lees meer](#)



Tim van Heugten • 2e

Hellorider 🚲 We put the ease in bicycle lease

2 w • 🌐

+ Volgen

👤 JURISTEN GEZOCHT 👤

Niet omdat ik zelf in de problemen zit. Maar omdat ik momenteel mijn "hobby project" [Deflekt.ai](#) aan het herbouwen ben. Een tool waarmee je interne (collega's) en externe (klanten) vragen automatisch beantwoordt (via mail, website chat, Slack of Teams).

Om de technologie achter [Deflekt.ai](#) eens goed te testen dacht ik dat het leuk was om alle Nederlandse wetsartikelen te scrapen en in te lezen in [Deflekt.ai](#) en zo een "WetGPT" chatbot te bouwen.

Leuke manier om een paar avonden alleen op je zolderkamer te zitten, maar nu zoek ik mensen die het willen proberen en van feedback willen voorzien. Iemand die de wet ook kent is uiteraard ideaal. Zelf een keer proberen of delen met juristen in je netwerk? Ik ben je dankbaar 🙏

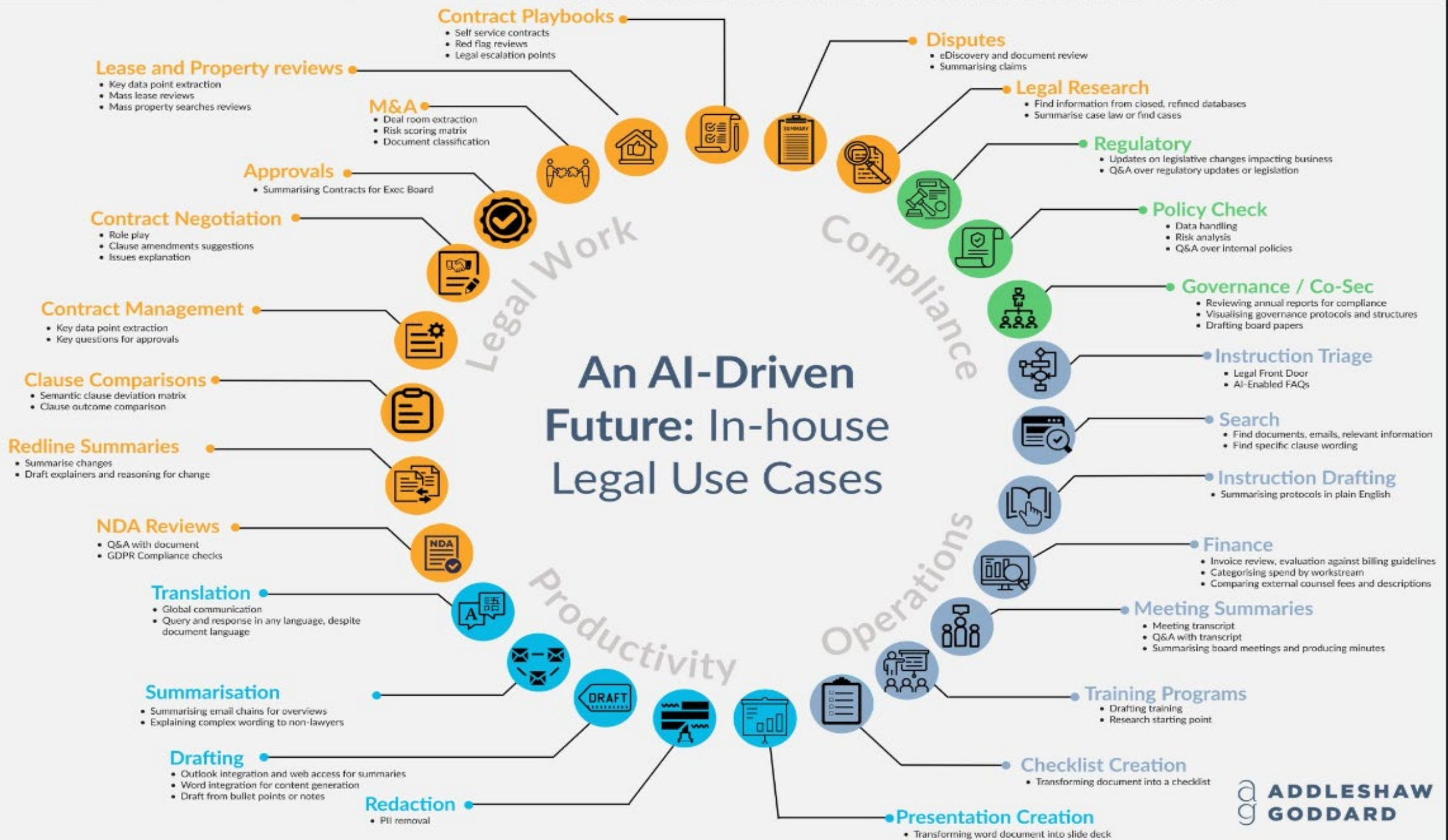
Gratis te proberen op <https://lnkd.in/erF4ppHy>



WetGPT - Een showcase van de kracht van Deflekt.ai.

deflekt.ai • Leestijd: 1 min.

An AI-Driven Future: In-house Legal Use Cases



AI in een juridische context

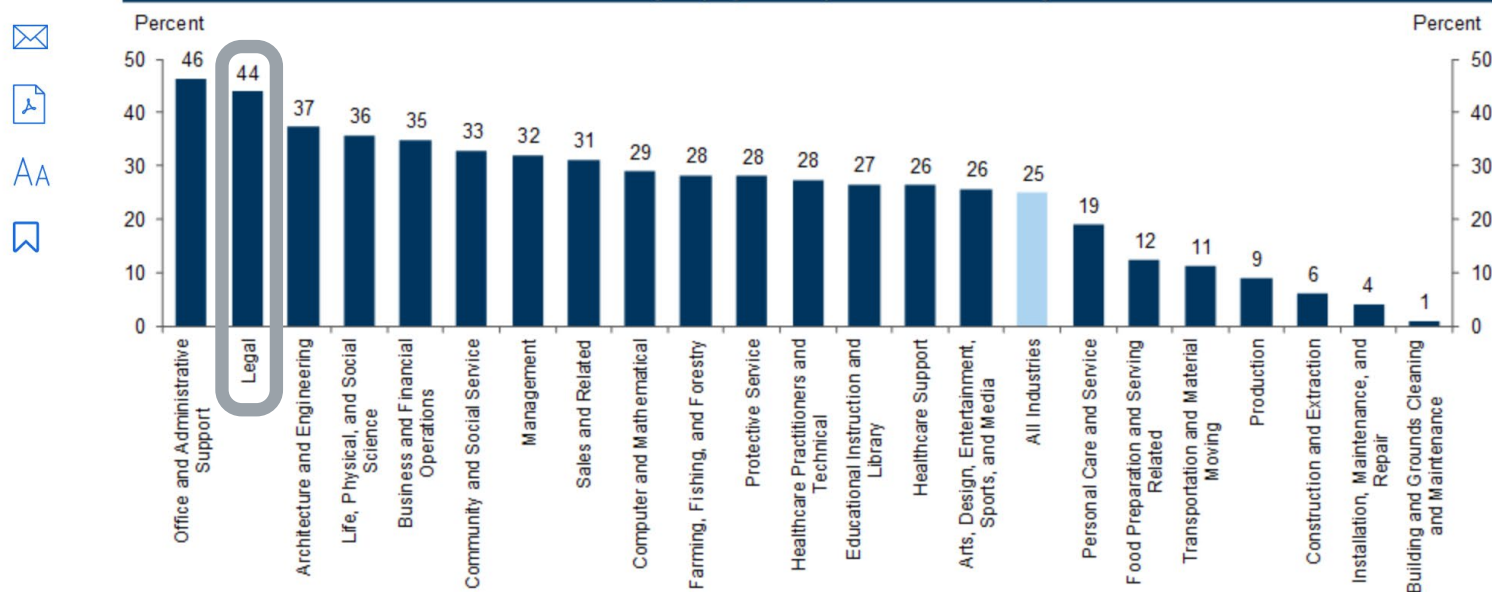
Goldman Sachs

Table of Contents

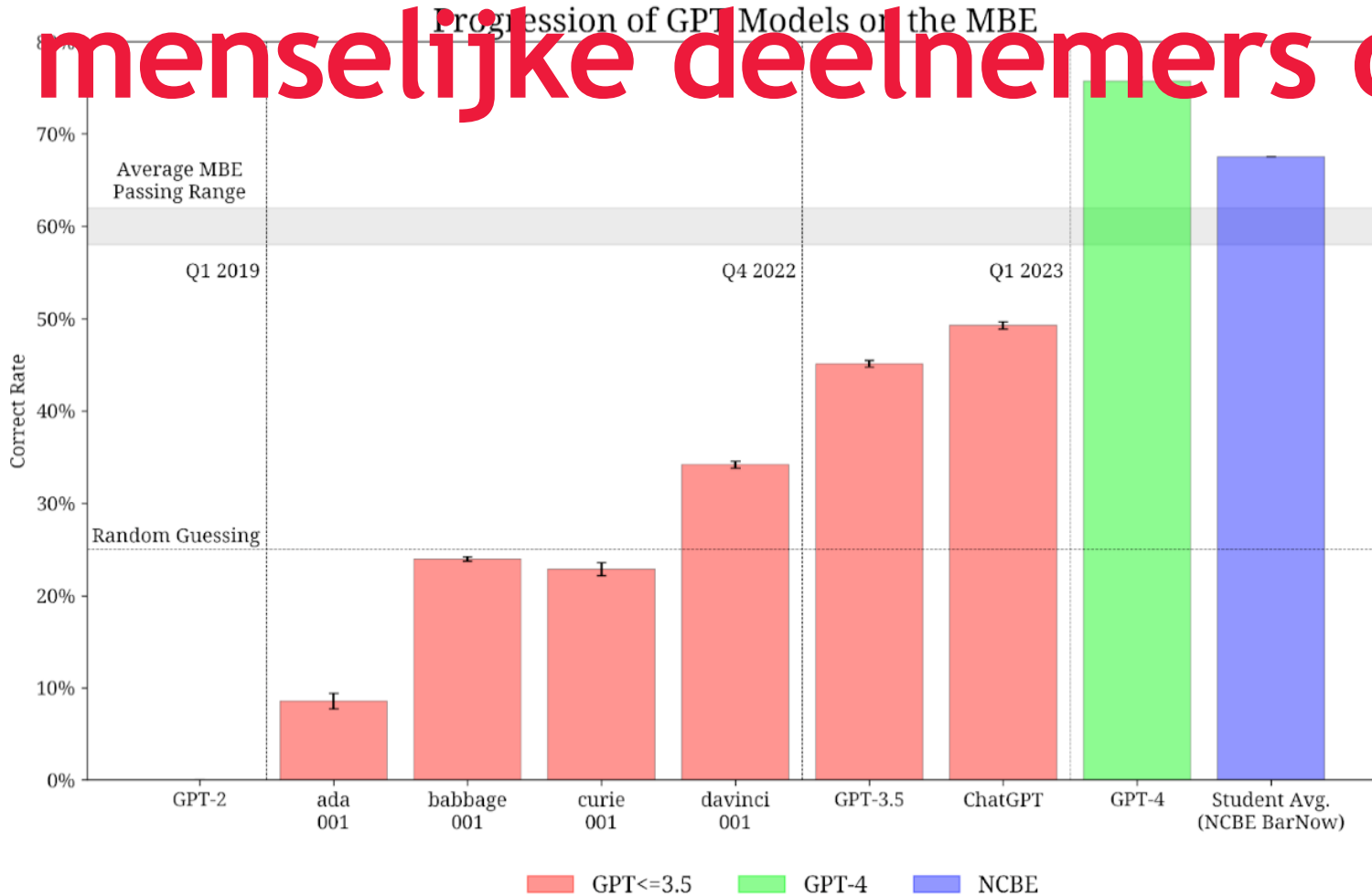
26 March 2023 | 9:05PM EDT

Exhibit 5: One-Fourth of Current Work Tasks Could Be Automated by AI in the US and Europe

Share of Industry Employment Exposed to Automation by AI: US



GPT4 scoort beter dan 90% van de menselijke deelnemers op BAR exam



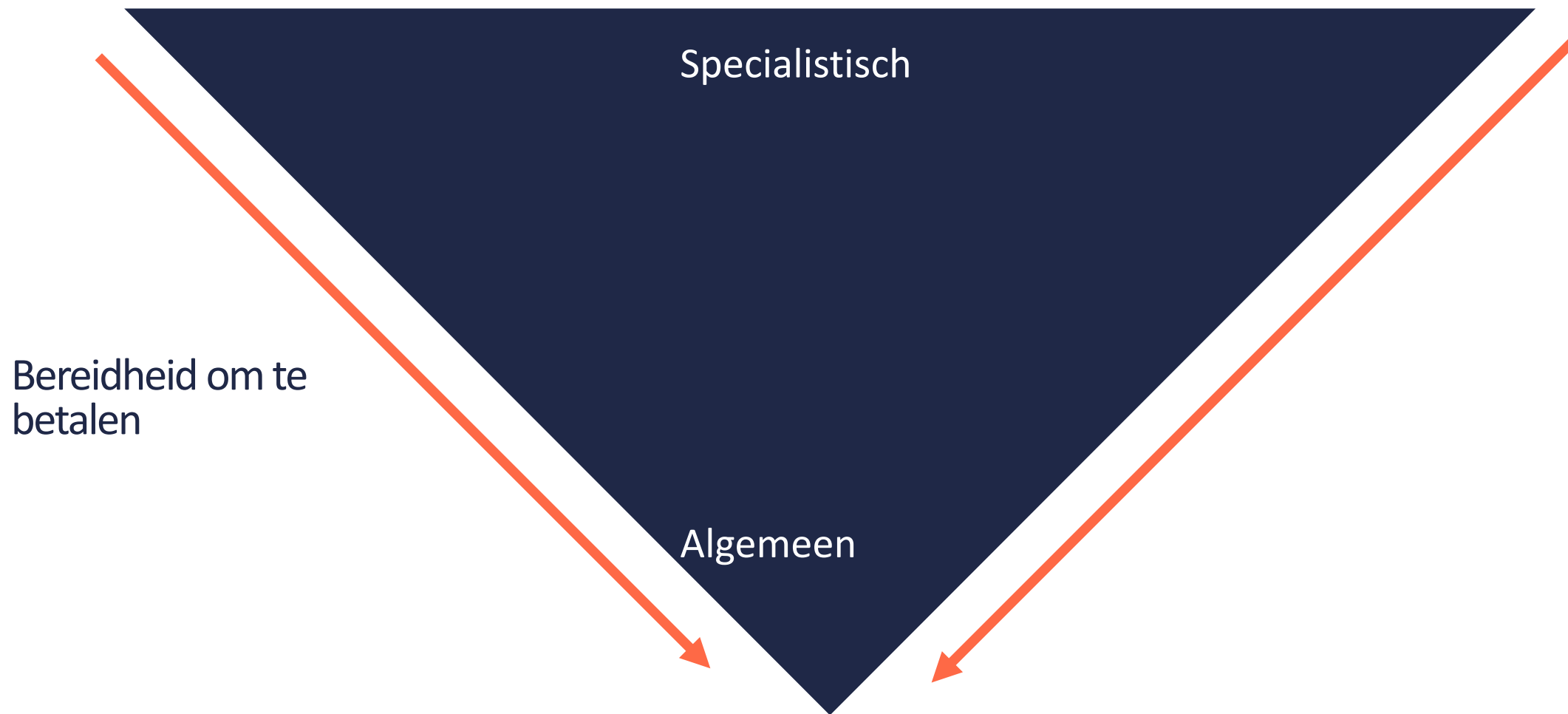
Bron: <https://www.iit.edu/news/gpt-4-passes-bar-exam>

<https://www.reuters.com/technology/bar-exam-score-shows-ai-can-keep-up-with-human-lawyers-researchers-say-2023-03-15/>

Juridische toepassingen



Juridische toepassingen



Juridische toepassingen

Draft & review

- Tekst genereren
- Legal research
- Formulering
- Red linen
- Vertalen
- Samenvatten

Legal AI assistent

- Formuleren van vragen op basis van de feiten
- Legal research
- Memo schrijven met bronvermelding

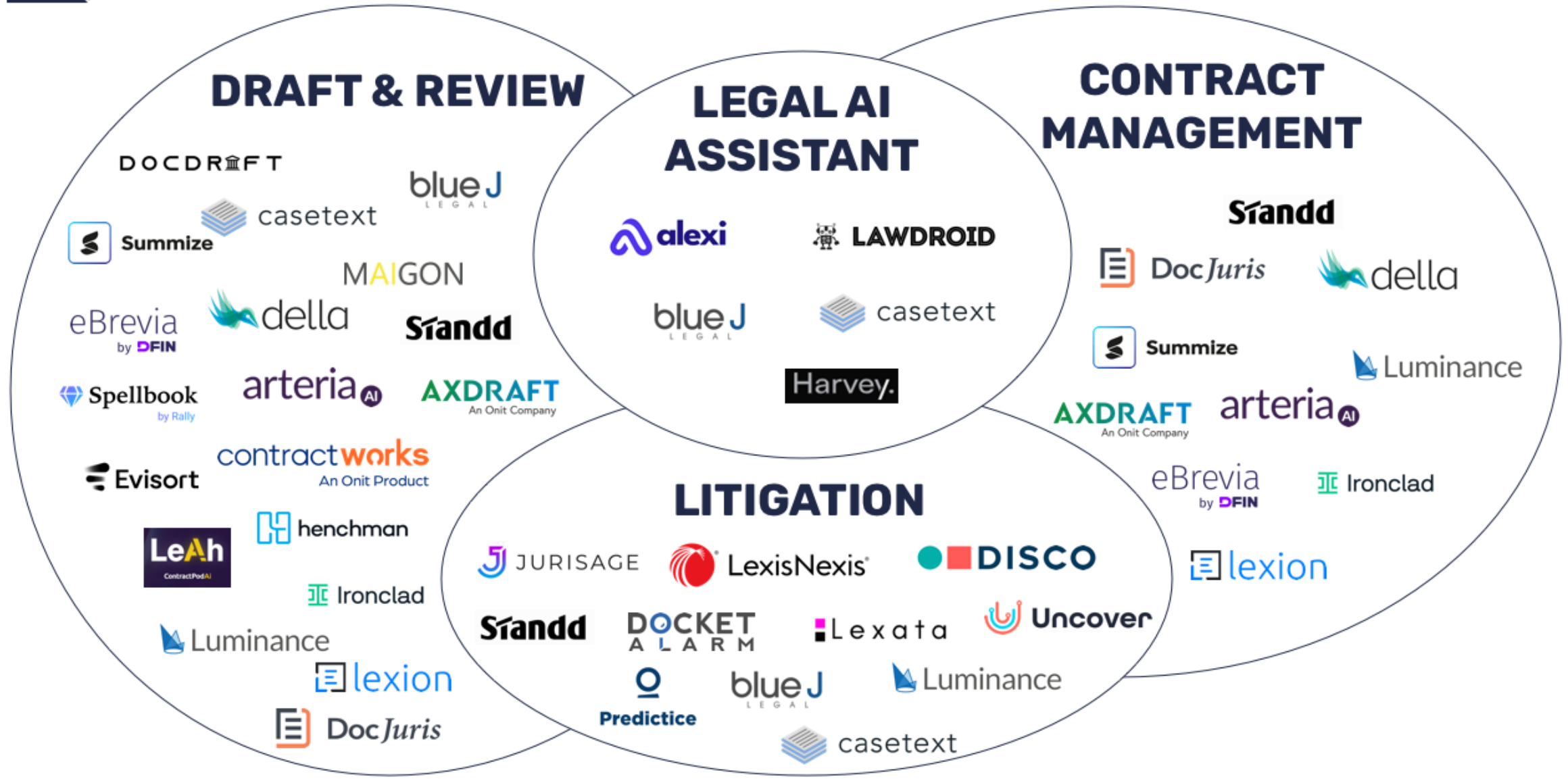
Contract management

- Data extractie
- Workflows
- Onderhandelen

Litigation

- Uitkomst voorspellen
- Structureren van stukken
- Dossier doorzoeken
- Tijdslijn van gebeurtenissen

MyGPT Generative AI and NLP solutions for the legal sector



BEDANKT VOOR JULLIE AANDACHT!

Menno Weij

Partner Tech & Privacy Law

M +31 (0)6 10 91 90 24

E menno.weij@bdo.nl

