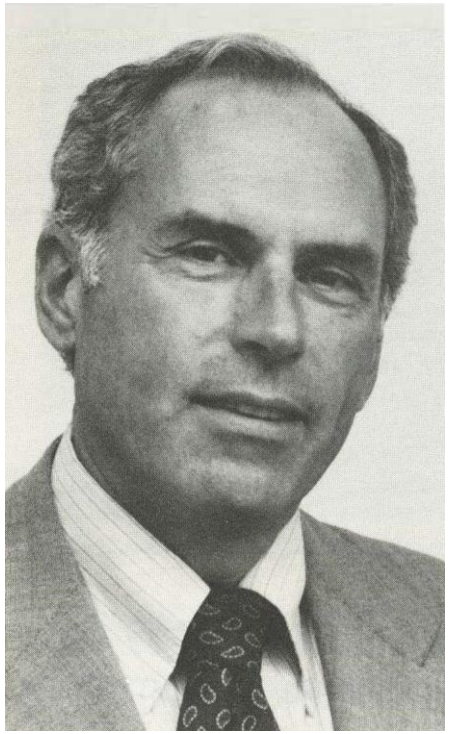
universität wien

Auf dem Weg zu einer geregelten Künstlichen Intelligenz: Herausforderungen und Perspektiven

Nikolaus Forgó

Amara‘s Law



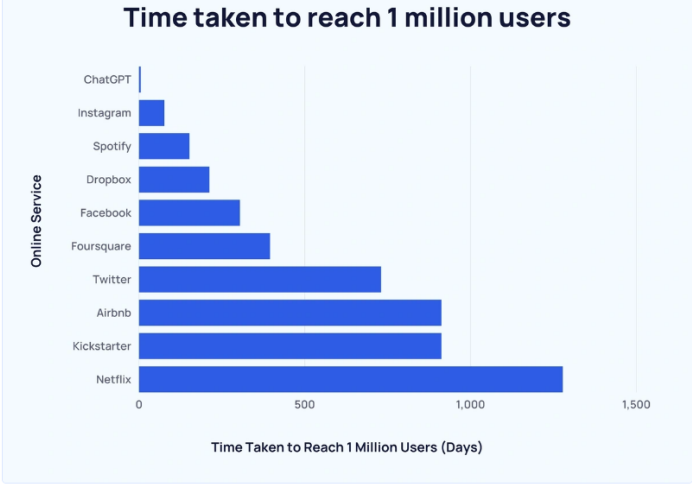
“We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run.”

 By Rochester Institute of Technology - News & Events 1980 at the RIT Digital Archive, Public Domain, https://commons.wikimedia.org/w/index.php?curid=115552843

Was ist „long run“?

Was is „short run“?

2023



Here's a breakdown of the approximate time taken to reach 1 million users for various online services:

Online Service	Launch Year	Time Taken to Reach 1 Million Users
ChatGPT	2022	5 days

5 Tage

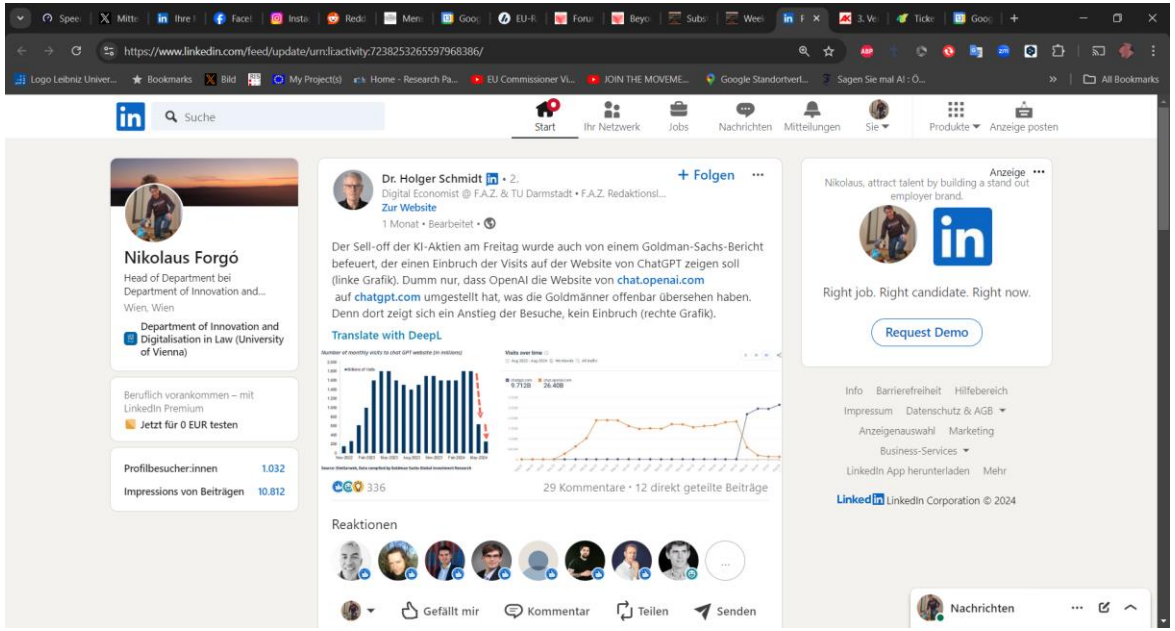
universität wien

Month	Number of Visits	Change Over Previous Month	Change Over Previous Month (%)
November 2022	152.7 million	-	-
December 2022	266 million	↑ 113.3 million	↑ 74.2%
January 2023	616 million	↑ 350 million	↑ 131.58%
February 2023	1 billion	↑ 384 million	↑ 62.34%
March 2023	1.6 billion	↑ 600 million	↑ 60%
April 2023	1.8 billion	↑ 200 million	↑ 12.5%
May 2023	1.8 billion	-	-
June 2023	1.6 billion	↓ 200 million	↓ 12.5%

April 2024	1.8 billion	-	-
May 2024	637 million	↓ 1.2 billion	↓ 64.6%
June 2024	260 million	↓ 377 million	↓ 59.2%

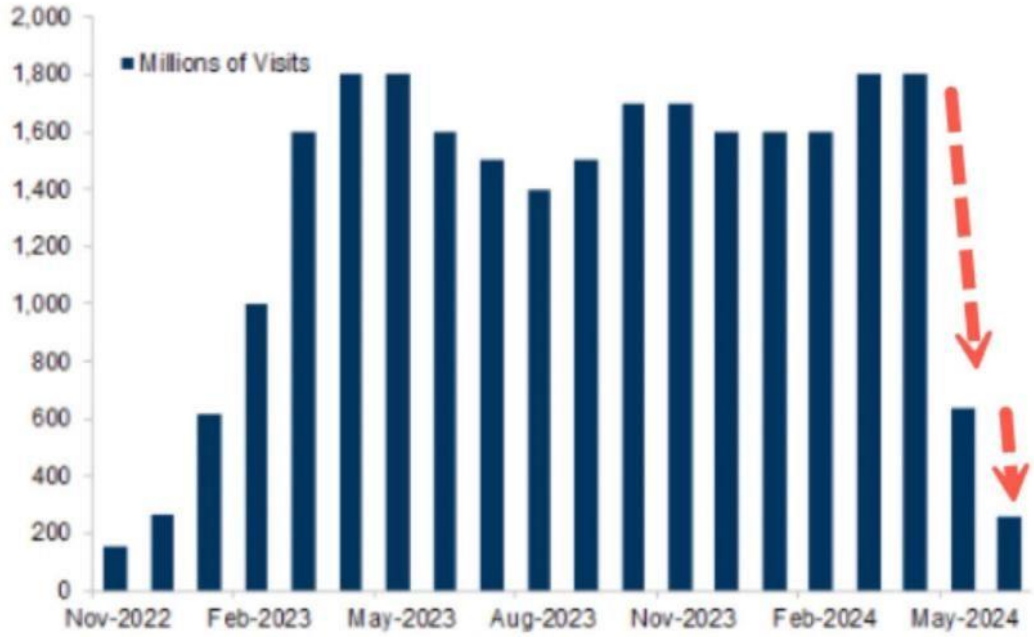
60 % Rückgang pro Monat ?!

Aber

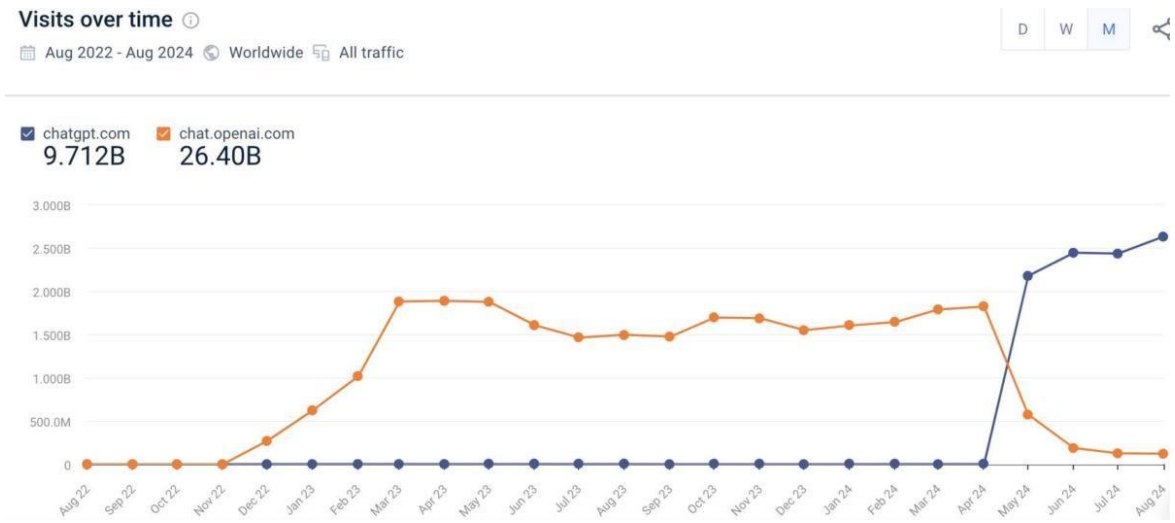


Dumm nur, dass OpenAI die Website von chat.openai.com auf chatgpt.com umgestellt hat, was die Goldmänner offenbar übersehen haben.

Number of monthly visits to chat GPT website (in millions)



Source: Similarweb, Data compiled by Goldman Sachs Global Investment Research



Was is „short run“?

Was ist „long run“?

Hype vorbei?

Was ist „long run“?

Was is „short run“?

universität wien

Ich

universität wien

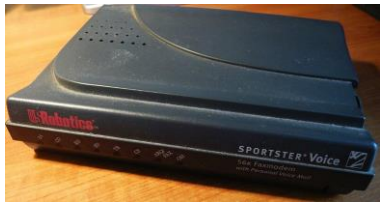
1968

https://artblart.files.wordpress.com/2013/12/en-089-computer-room-detroit-1968-web.jpg

universität wien

1985

1995



2007

2022

Informational Self Determination

Internet Bubble Directives

Digital Agenda

AI

KI ist (längst schon) überall.

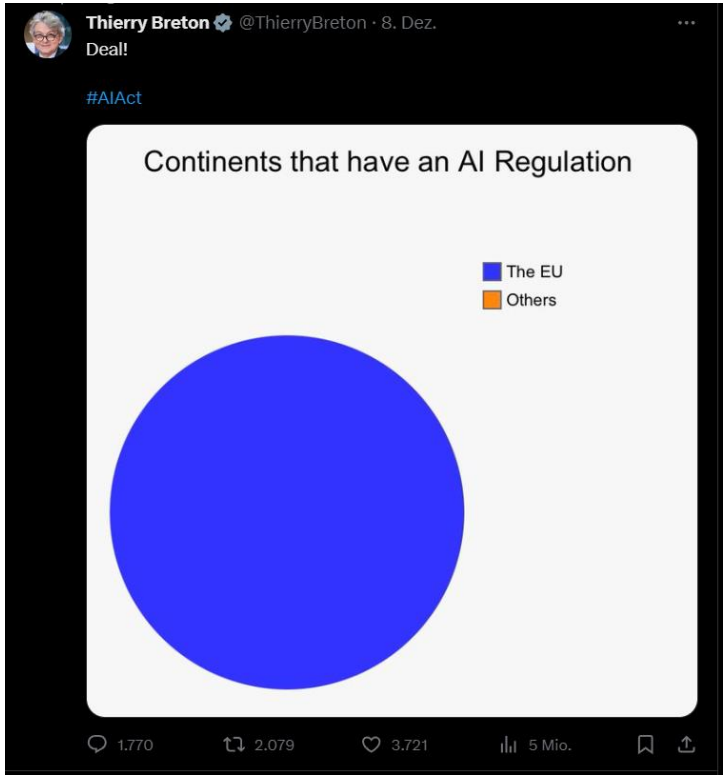
universität wien

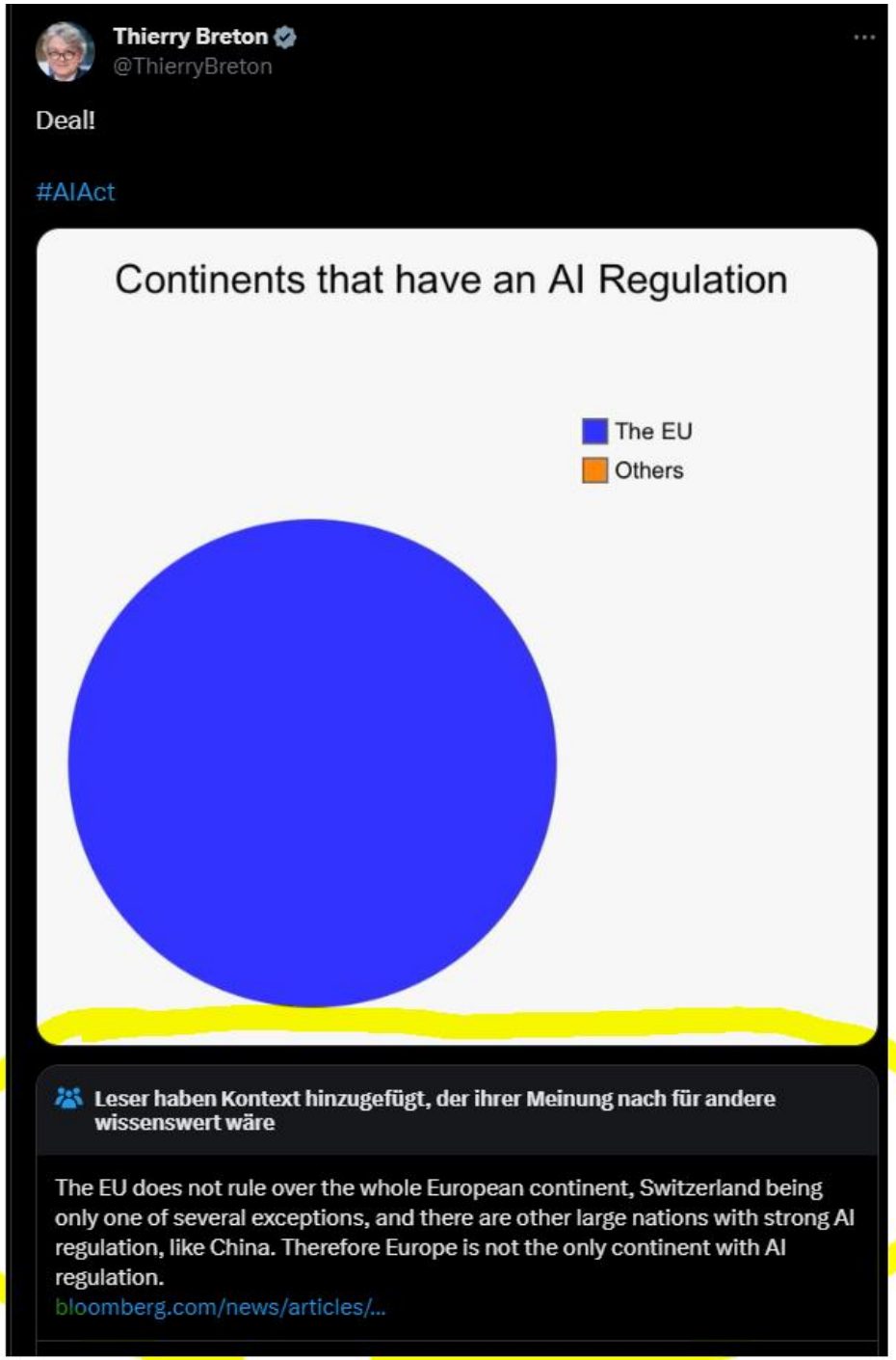
Rahmenbedingungen


EU
Artificial
Intelligence Act

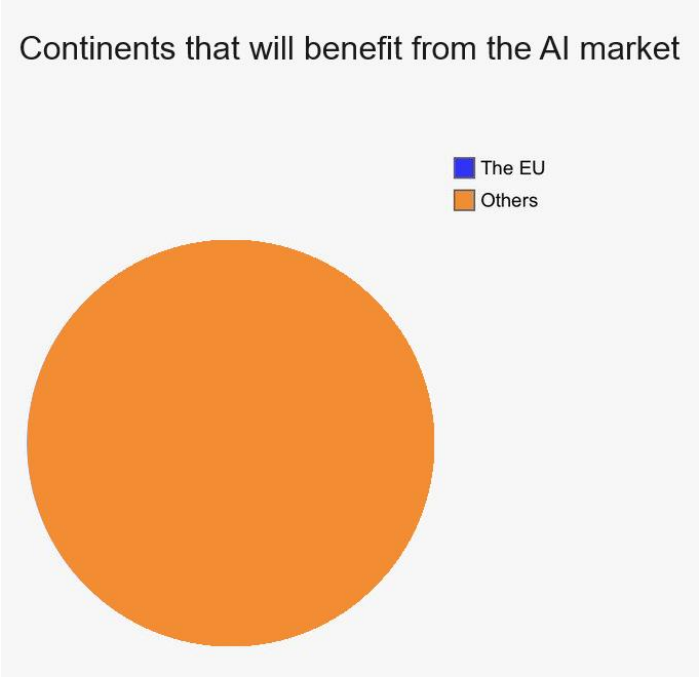
universität wien

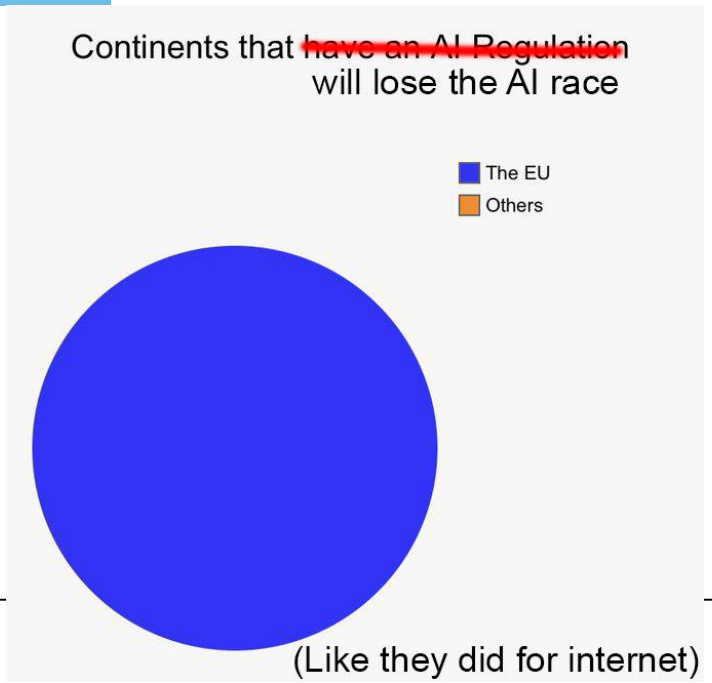
Dezember 2023

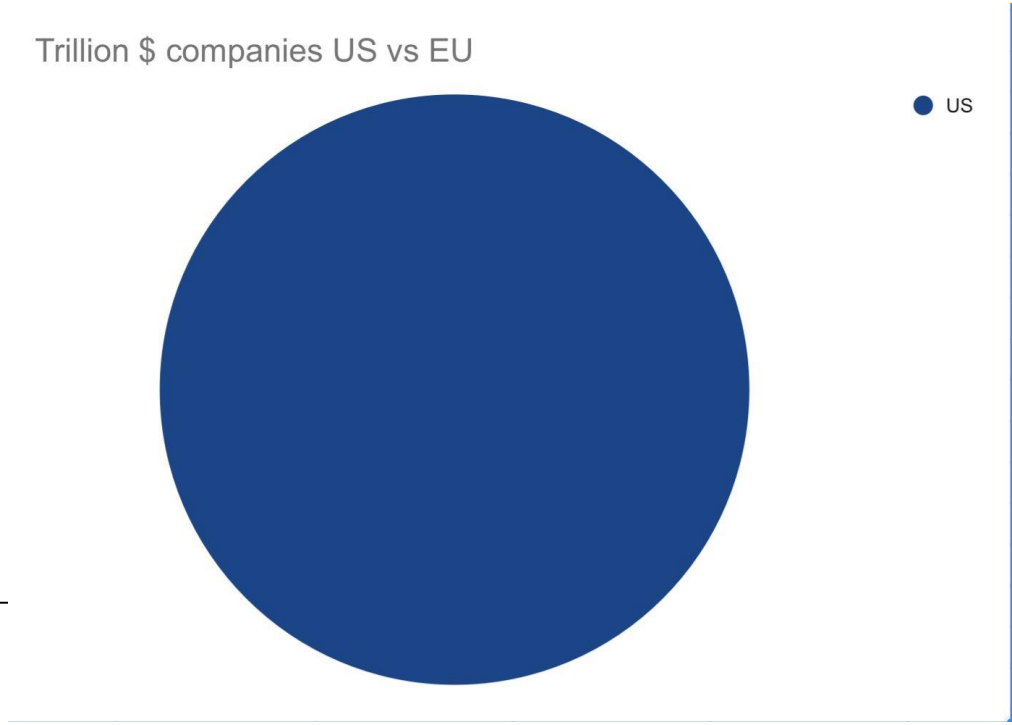




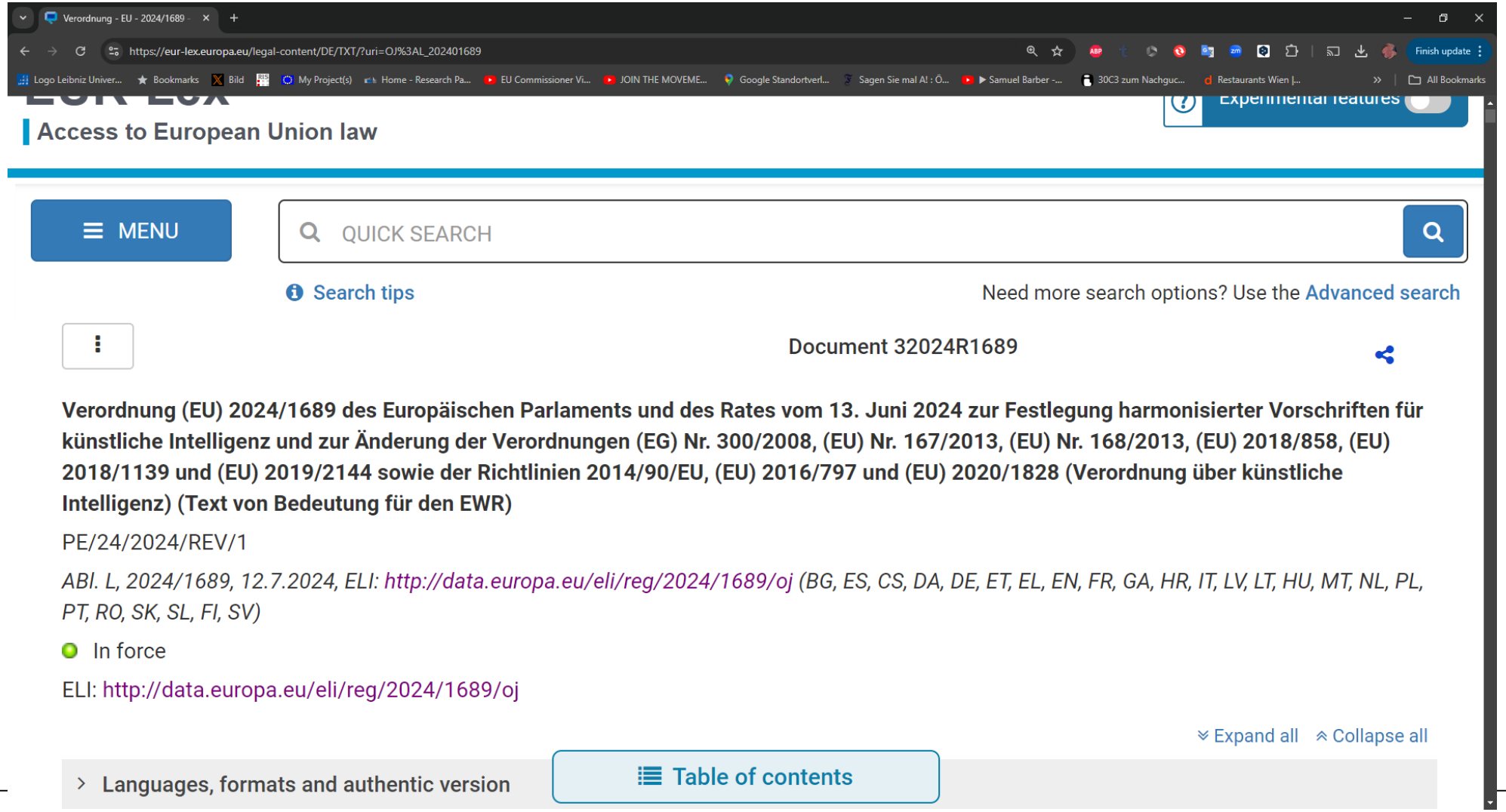

CECI EST L'EUROPE
CECI EST L'UE
Bruxelles
Strasbourg
NE CONFONDEZ PAS.


Continents that will benefit from the AI market
The EU
Others


Continents that have an AI Regulation will lose the AI race
The EU
Others
(Like they did for internet)


Trillion $ companies US vs EU
US

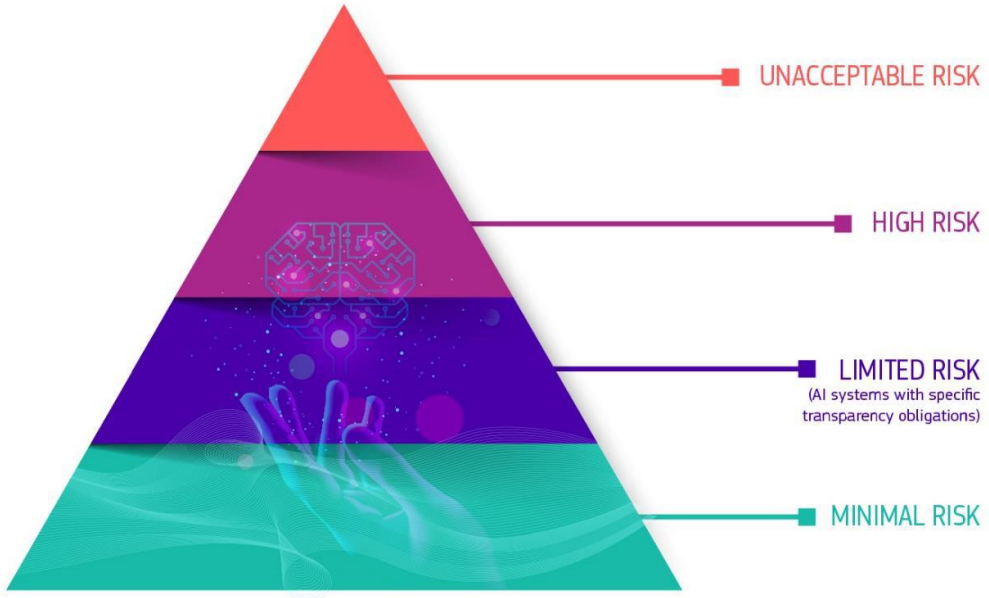
universität wien



universität wien

Worum geht es überhaupt?

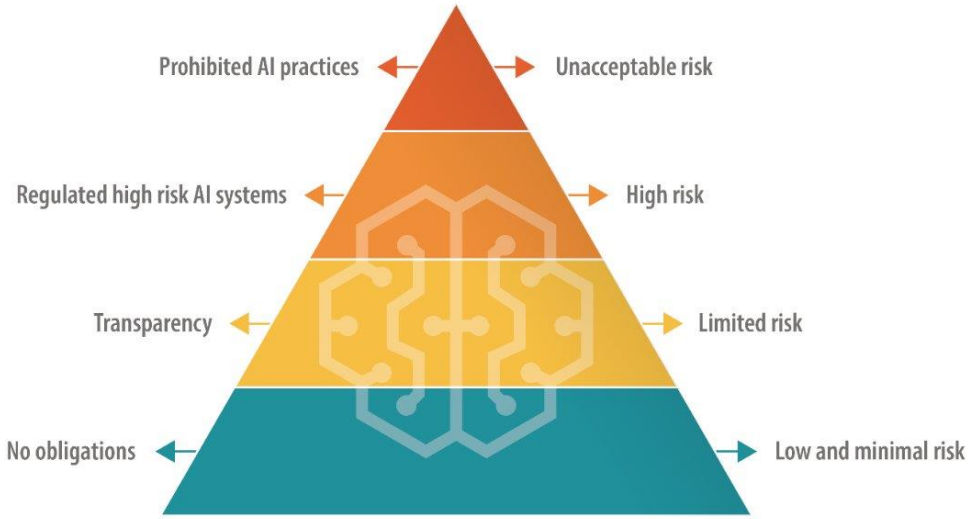
Risiko!



Risk-based approach

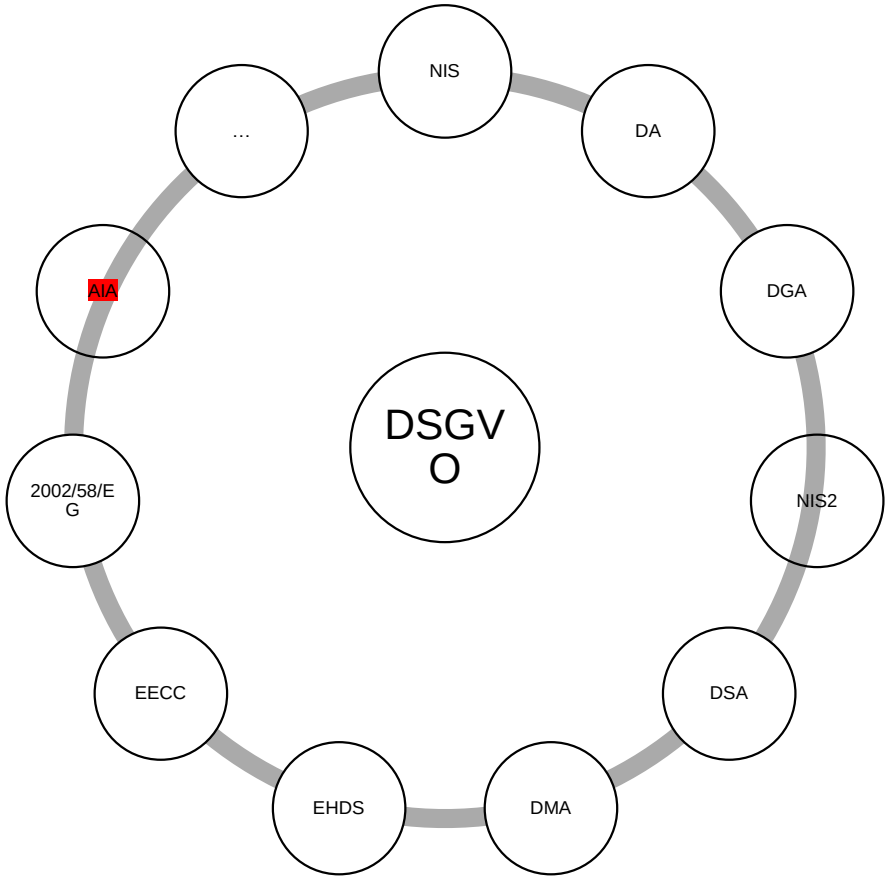
Pyramid of risks

The use of AI, with its specific characteristics (e.g. opacity, complexity, dependency on data, autonomous behaviour), can adversely affect a number of fundamental rights and users' safety. To address those concerns, the draft AI act follows a **risk-based approach** whereby legal intervention is tailored to concrete level of risk. To that end, the draft AI act distinguishes between AI systems posing (i) **unacceptable risk**, (ii) **high risk**, (iii) **limited risk**, and (iv) **low or minimal risk**. Under this approach, AI applications would be regulated only as strictly necessary to address specific levels of risk.[20]



Data source: European Commission.

https://futurium.ec.europa.eu/sites/default/files/2021-10/Kop_EU%20Artificial%20Intelligence%20Act%20-%20The%20European%20Approach%20to%20AI_21092021_0.pdf
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN;
https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf



Stand heute
DSGVO unangetastet

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495

EG 10 KI-VO

„Diese Verordnung soll die Anwendung des bestehenden Unionsrechts zur Verarbeitung personenbezogener Daten, einschließlich der Aufgaben und Befugnisse der unabhängigen Aufsichtsbehörden, die für die Überwachung der Einhaltung dieser Instrumente zuständig sind, nicht berühren. Sie lässt ferner die Pflichten der Anbieter und Betreiber von KI-Systemen in ihrer Rolle als Verantwortliche oder Auftragsverarbeiter, die sich aus dem Unionsrecht oder dem nationalen Recht über den Schutz personenbezogener Daten ergeben, unberührt […].

universität wien

Vortrag in 20 Sekunden

- Die DSGVO gilt weiter.
- Die Verarbeitung personenbezogener Daten ist verboten.

universität wien

~~Auf dem Weg zu einer geregelten Künstlichen Intelligenz: Herausforderungen und Perspektiven:~~ nichts Neues!

Nikolaus Forgó

universität wien

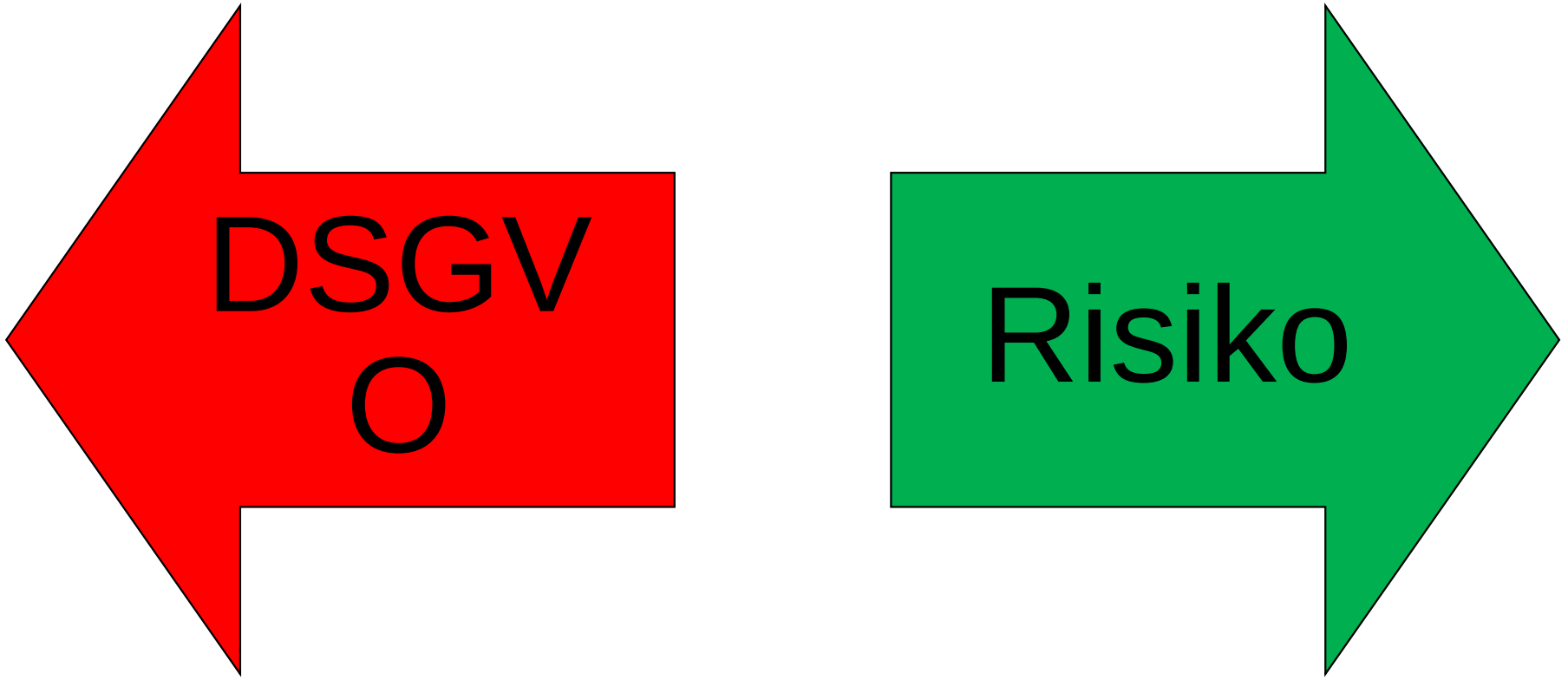
KI am Arbeitsplatz: Chance, Bedrohung oder nichts Neues!

Nikolaus Forgó

universität wien

Vortrag in 20 Minuten

Ausgangspunkte



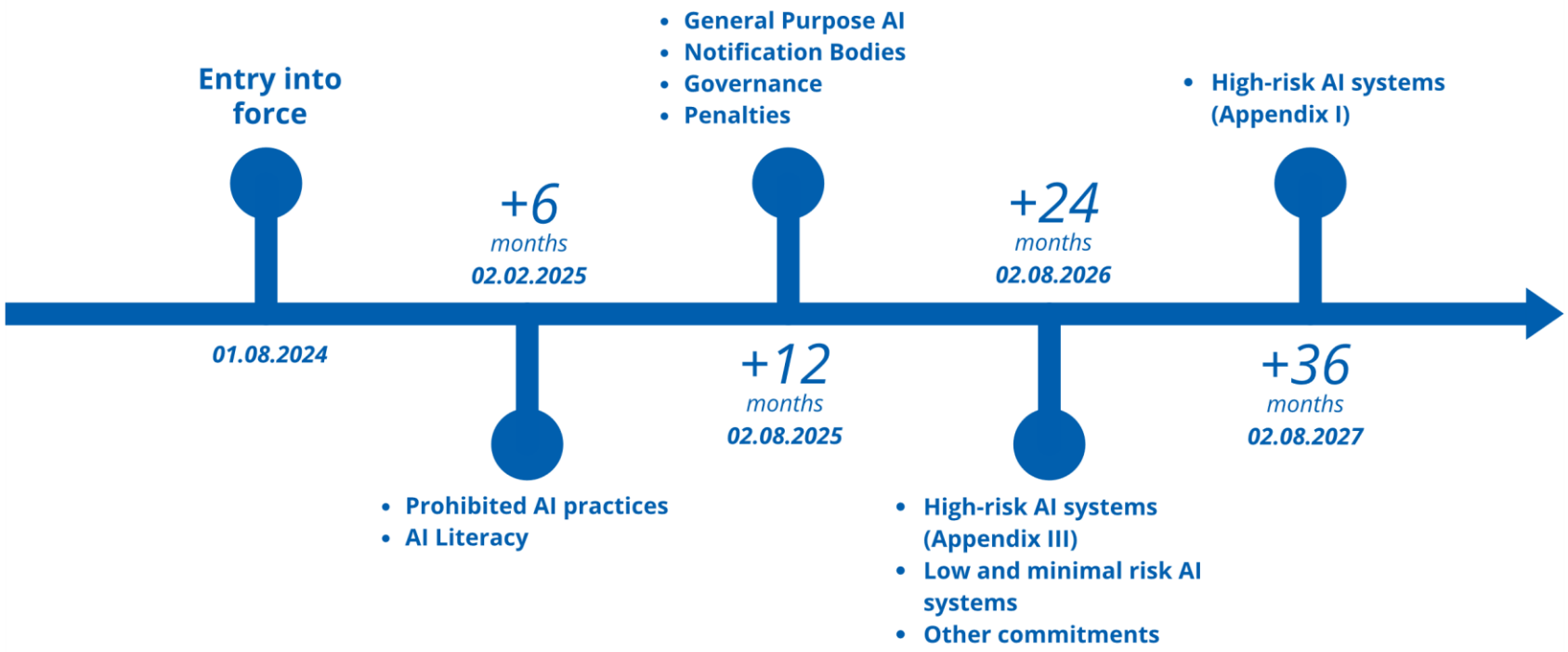
universität wien

Ab wann?

universität wien

AI Act: Time Frame

Overview of the most important provisions that will only gradually become valid



AI Service Desk ai.rtr.at RTR

universität wien

KI-System?

Art. 3 Zif. 1 KI-VO

„KI-System“

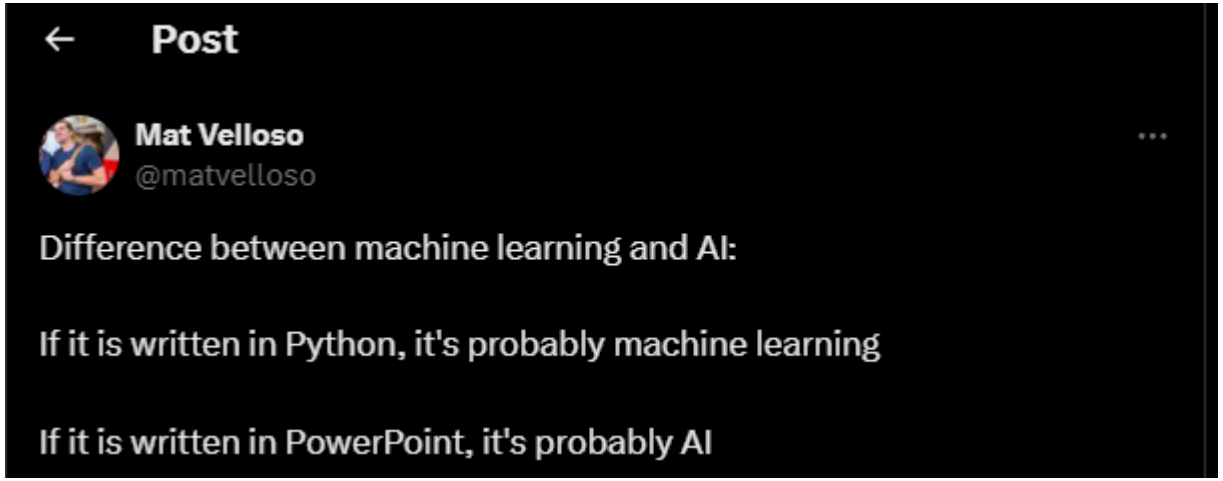
- ein maschinengestütztes System,
  - das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist
  - und das nach seiner Betriebsaufnahme anpassungsfähig sein kann
  - und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet,
    - wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden,
    - die physische oder virtuelle Umgebungen beeinflussen können;

universität wien

My positive Definition

Something that is doing something (not rule based)

My negative Definition



universität wien

Risiko

462 Seiten

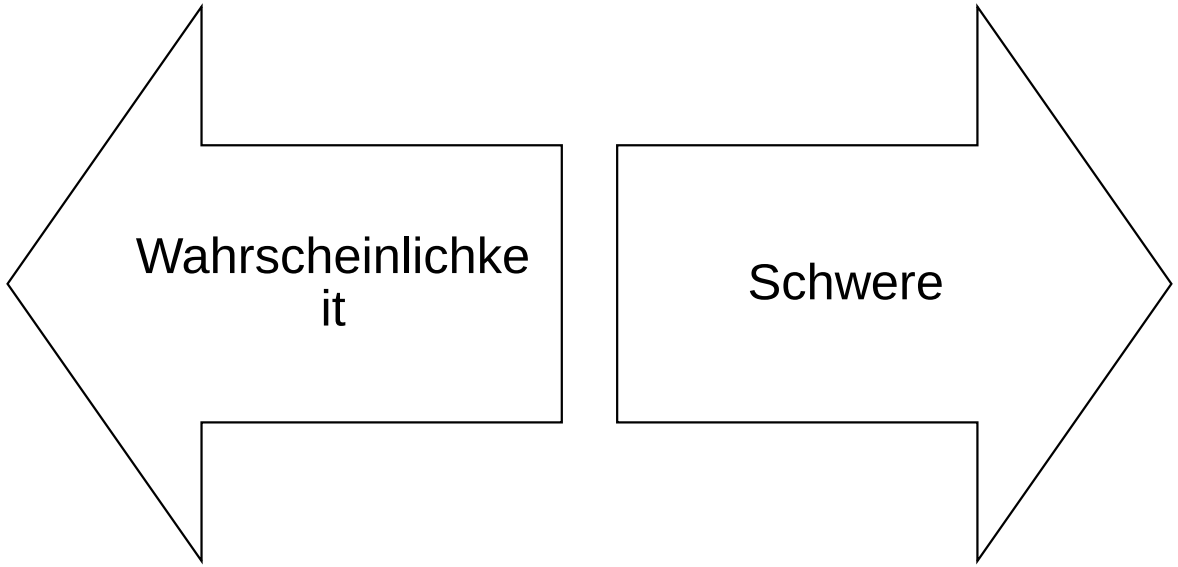
624 Treffer

1,4 Treffer/Seite

Risiko
Obsession

Risiko

- Art. 3 Zif. 2 KI-VO
- die Kombination aus der Wahrscheinlichkeit des Auftretens eines Schadens und der Schwere dieses Schadens;



universität wien

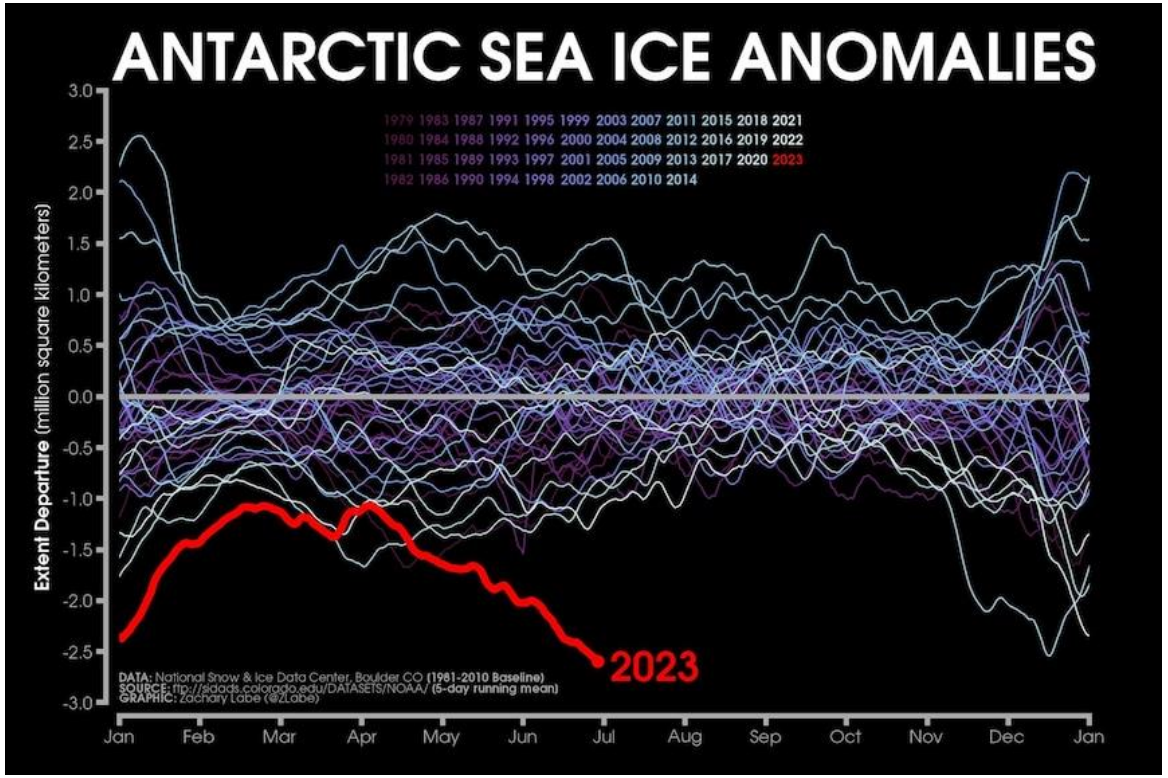
Was ist ein inakzeptables Risiko?

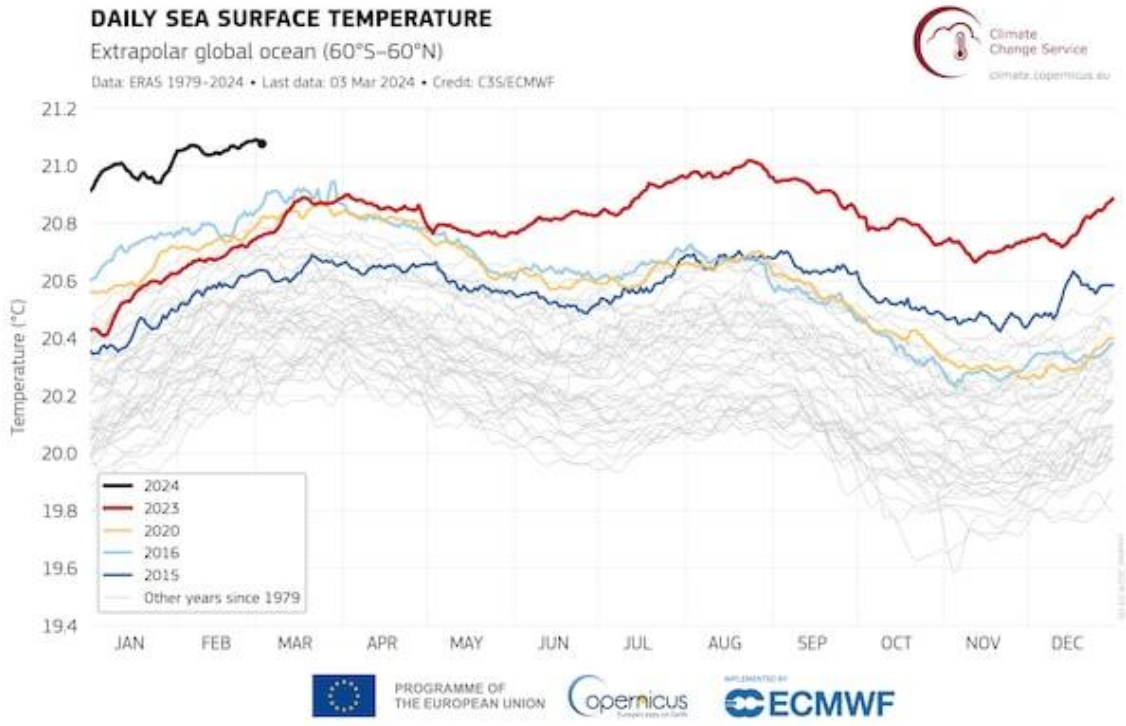
universität wien

Was ist ein inakzeptables Risiko?

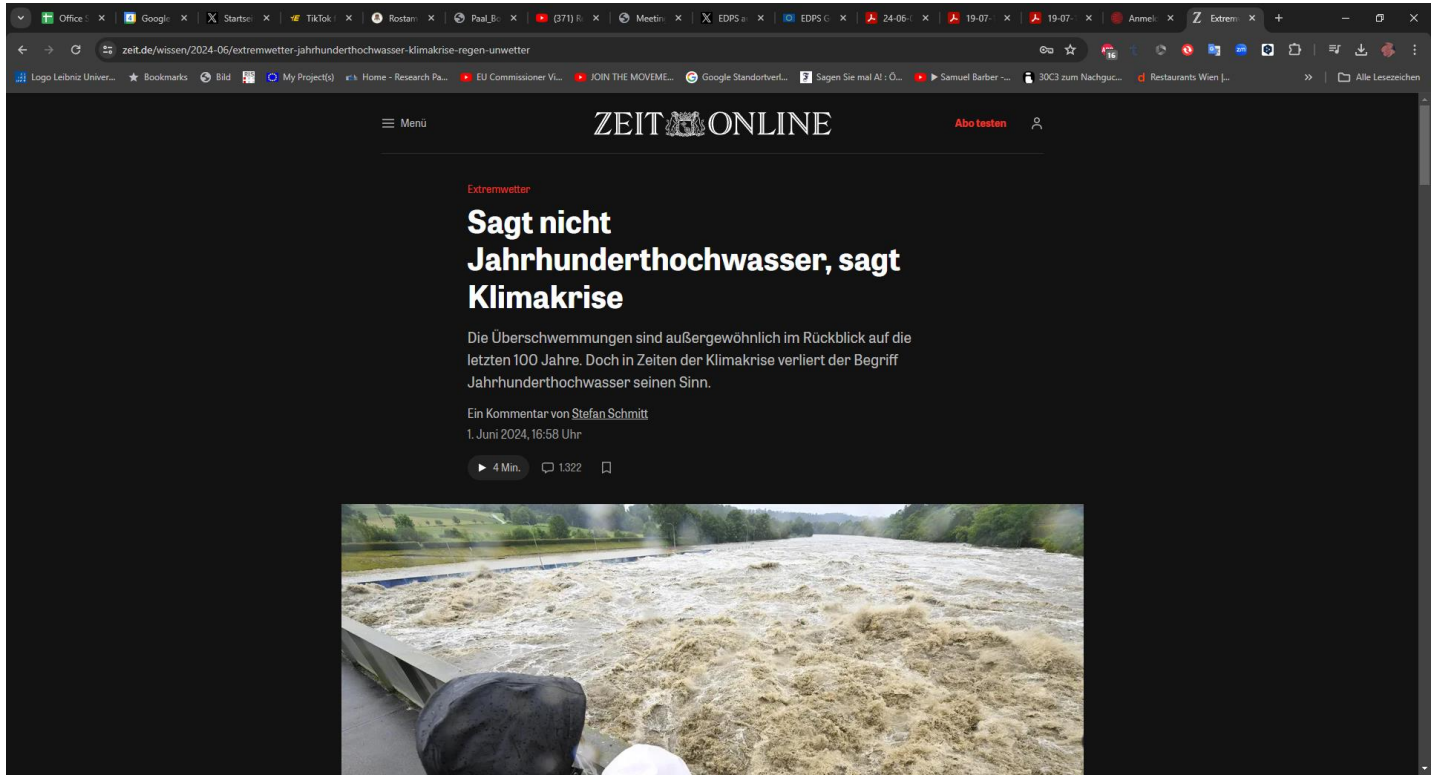
universität wien

??





https://www.abc.net.au/news/2023-07-08/climate-records-shattered-in-2023-ice-deficit-grows/102577168
https://www.focus.de/earth/analyse/obwohl-el-nino-schwaechelt-hinter-erschreckendem-waerme-rekord-steckt-ungeloeste-atlantik-anomalie_id_259740161.html


zeit.de/wissen/2024-06/extremwetter-jahrhunderthochwasser-klimakrise-regen-unwetter
Menü
ZEIT ONLINE
Abo testen
Extremwetter
Sagt nicht Jahrhunderthochwasser, sagt Klimakrise
Die Überschwemmungen sind außergewöhnlich im Rückblick auf die letzten 100 Jahre. Doch in Zeiten der Klimakrise verliert der Begriff Jahrhunderthochwasser seinen Sinn.
Ein Kommentar von Stefan Schmitt
1. Juni 2024, 16:58 Uhr
4 Min.
1.322

IEEE ComSoc
IEEE Communications Society
Technology Blog

ENHANCED BY Google

Home | About the Blog | About the Techblog Editorial Team | Call for Blog Post Submissions

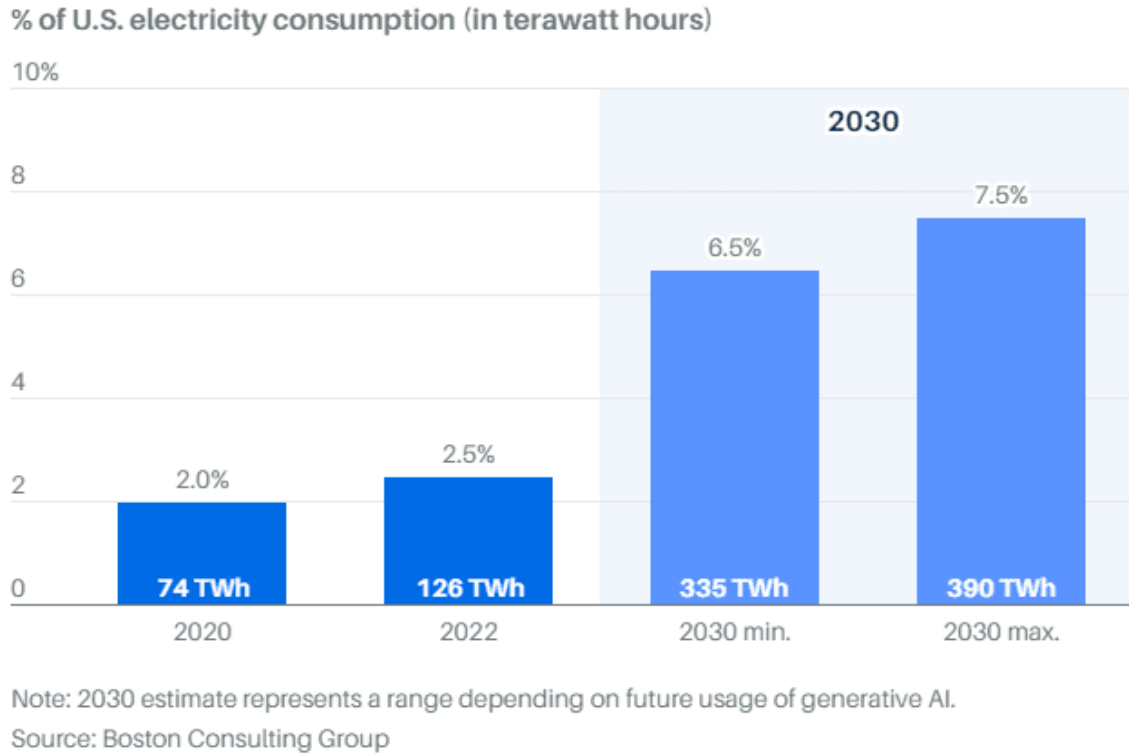
AI sparks huge increase in U.S. energy consumption and is straining the power grid; transmission/distribution as a major problem

Posted on March 16, 2024 by Alan Weissberger

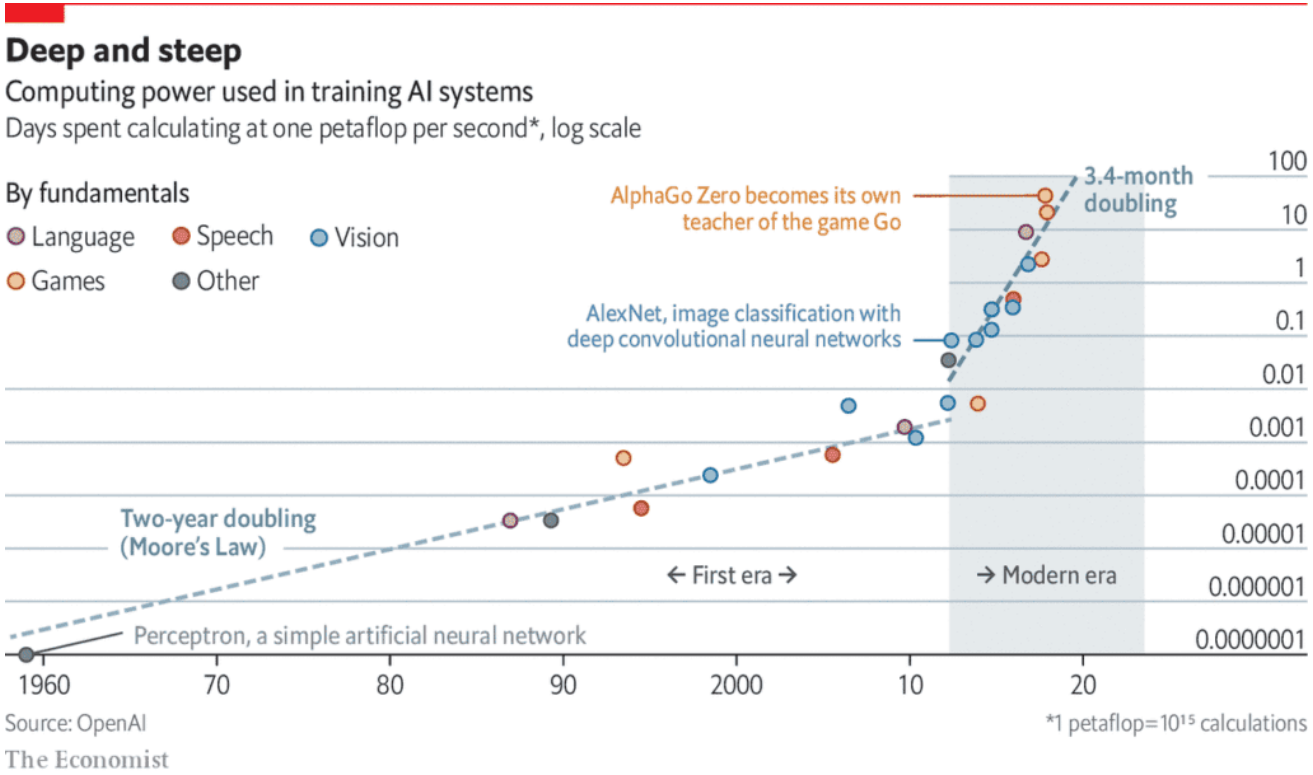
The **AI boom** is changing how data centers are built and where they're located, and it's already sparking a **reshaping of U.S. energy infrastructure,** according to Barron's. Energy companies increasingly cite **AI power consumption** as a leading contributor to new demand. That is because AI compute servers in data centers require a tremendous amount of power to process large language models (**LLMs**). That was explained in detail in this recent IEEE Techblog post.

Fast Company reports that "The surge in AI is straining the U.S. power grid." AI is pushing demand for energy significantly higher than anyone was anticipating. "The U.S. electric grid is not prepared for significant load growth," **Grid Strategies** warned. AI is a major part of the problem when it comes to increased demand. Not only are industry leaders such as OpenAI, Amazon, Microsoft, and Google either building or looking for locations on which to build enormous data centers to house the infrastructure required to power large language models, but smaller companies in the space are also making huge energy demands, as the ***Washington Post*** reports.

Georgia Power, which is the chief energy provider for that state, recently had to increase its projected winter megawatt demand by as much as 38%. That's, in part, due to the state's incentive policy for computer operations, something officials are now rethinking. Meanwhile, Portland General Electric in Oregon, recently doubled its five-year forecast for new electricity demand.

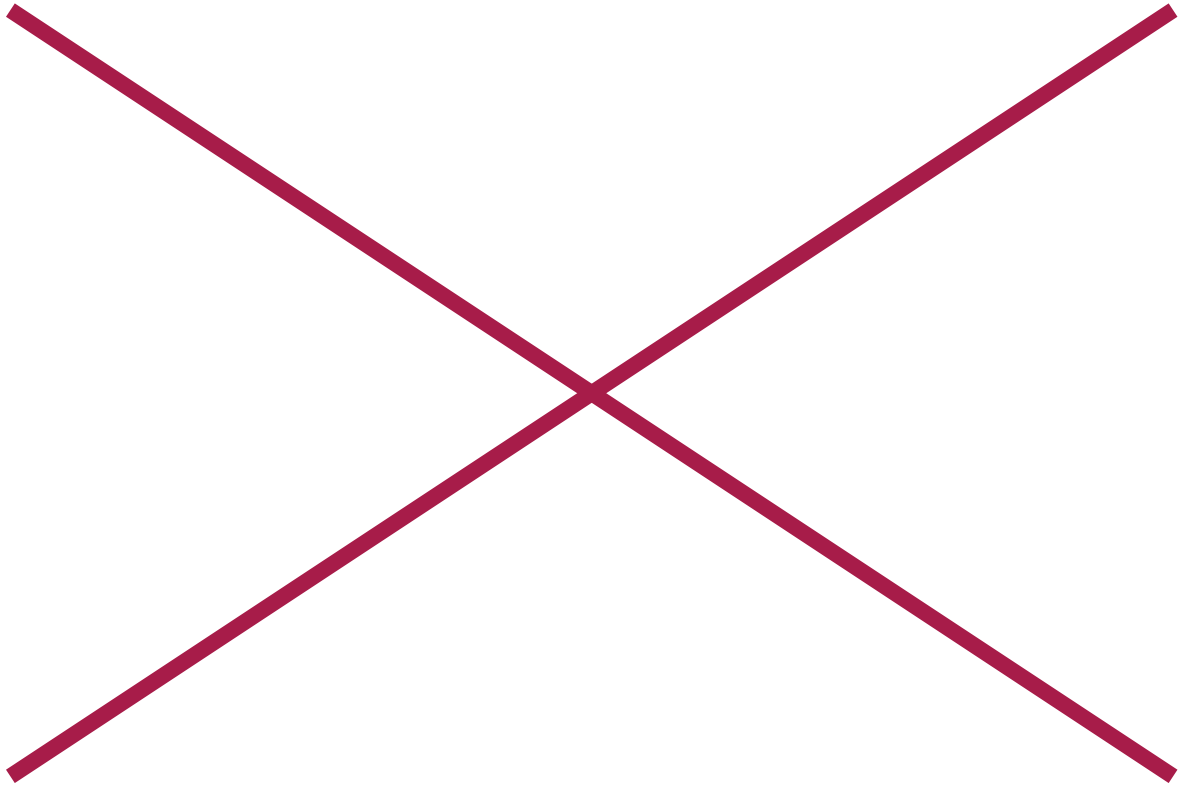


Note: 2030 estimate represents a range depending on future usage of generative AI.
Source: Boston Consulting Group


Deep and steep
Computing power used in training AI systems
Days spent calculating at one petaflop per second*, log scale
By fundamentals
Language
Speech
Vision
Games
Other
AlphaGo Zero becomes its own teacher of the game Go
3.4-month doubling
AlexNet, image classification with deep convolutional neural networks
Two-year doubling (Moore's Law)
Perceptron, a simple artificial neural network
← First era →
→ Modern era
100
10
1
0.1
0.01
0.001
0.0001
0.00001
0.000001
0.0000001
1960
70
80
90
2000
10
20
Source: OpenAI
*1 petaflop=10¹⁵ calculations
The Economist

- Wo stehen die Maschinen und wer kann sie bezahlen?
- Carbon Footprint?

Antwort AIA?

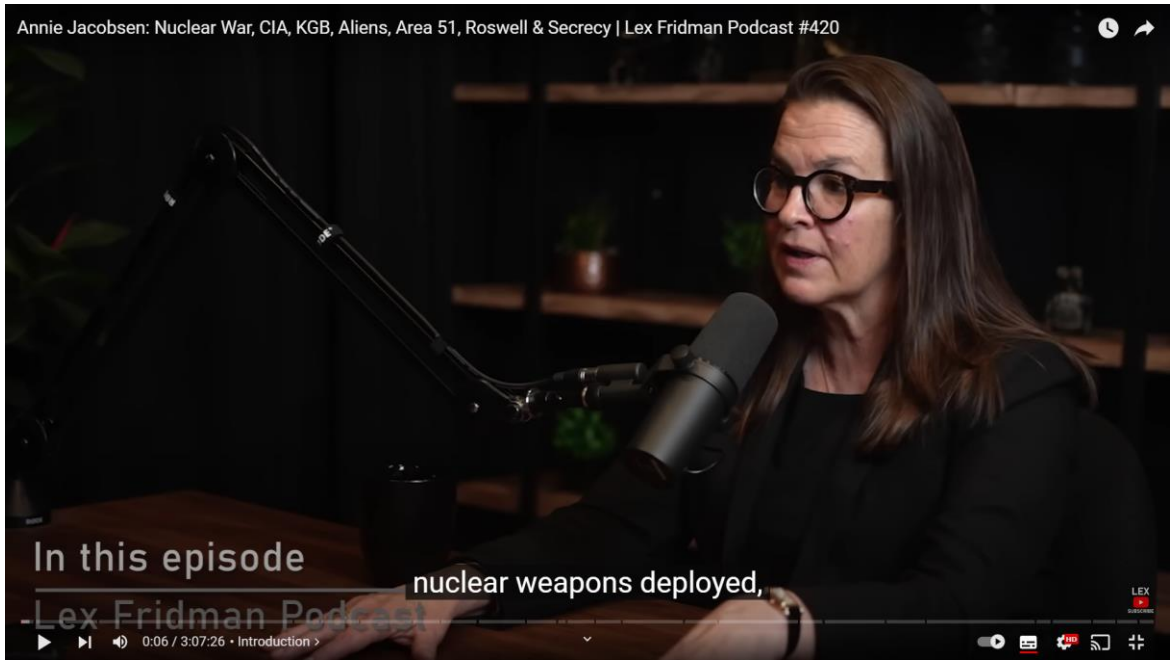


universität wien

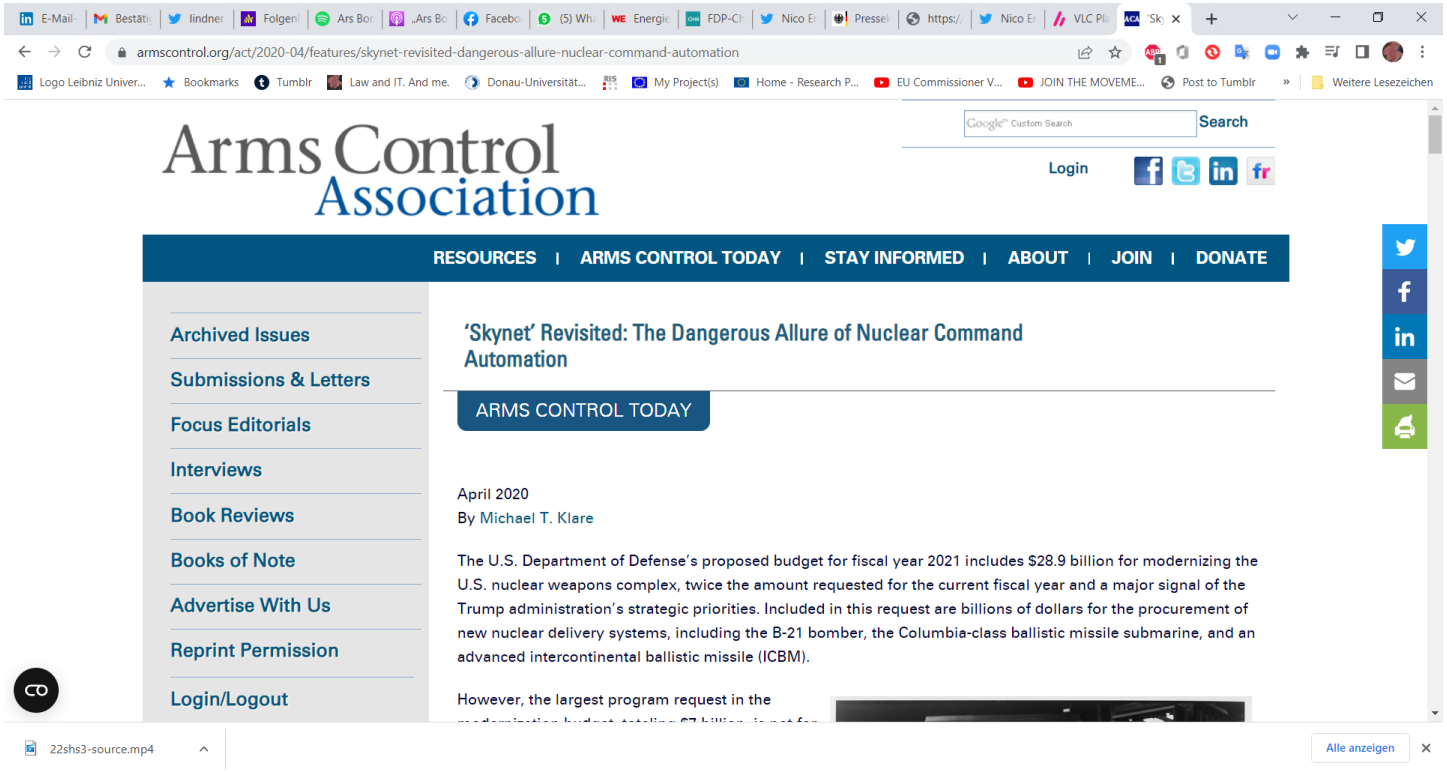
Was ist ein inakzeptables Risiko?

universität wien

6 Minuten



USA, April 2020



universität wien

Militärausgaben

„The U.S. Department of Defense's proposed budget for fiscal year 2021 includes $28.9 billion for modernizing the U.S. nuclear weapons complex"

However, the largest program request in the modernization budget, totaling $7 billion, is not for any of those weapons but for modernizing the nation's nuclear command, control, and communications (NC3) infrastructure, the electronic systems that inform national leaders of a possible enemy attack and enable the president to order the launch of U.S. bombers and missiles."

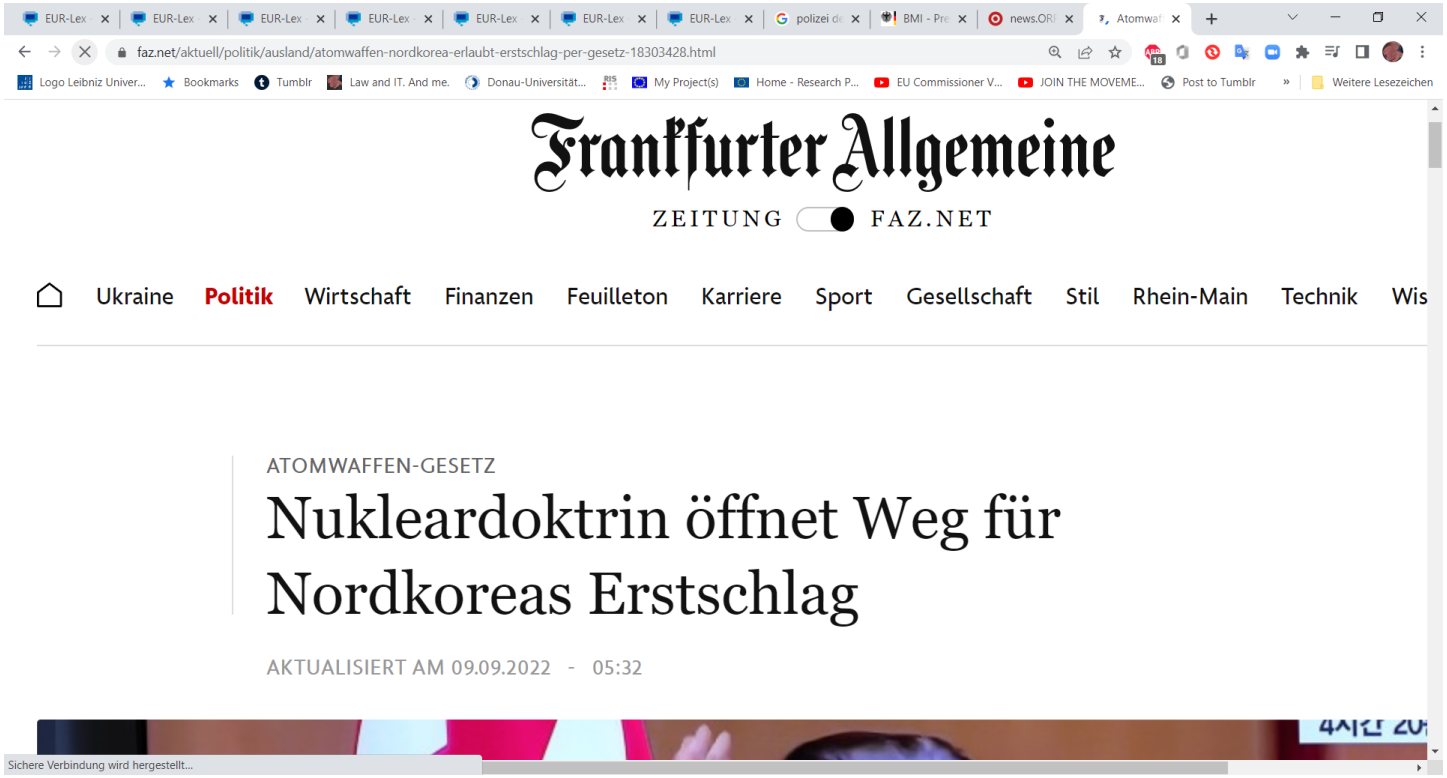
universität wien

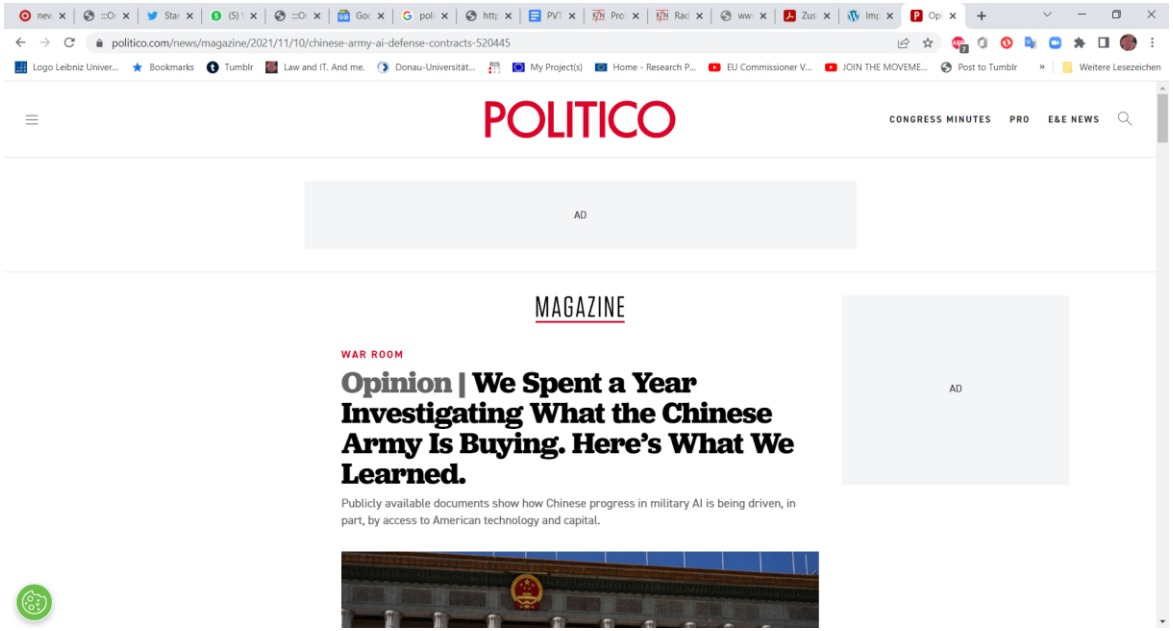
2020 (!)

„Thus, it may be necessary to develop a system based on [AI], with predetermined response decisions, that detects, decides, and directs strategic forces with such speed that the attack-time compression challenge does not place the United States in an impossible position.”

universität wien

09.09.2022



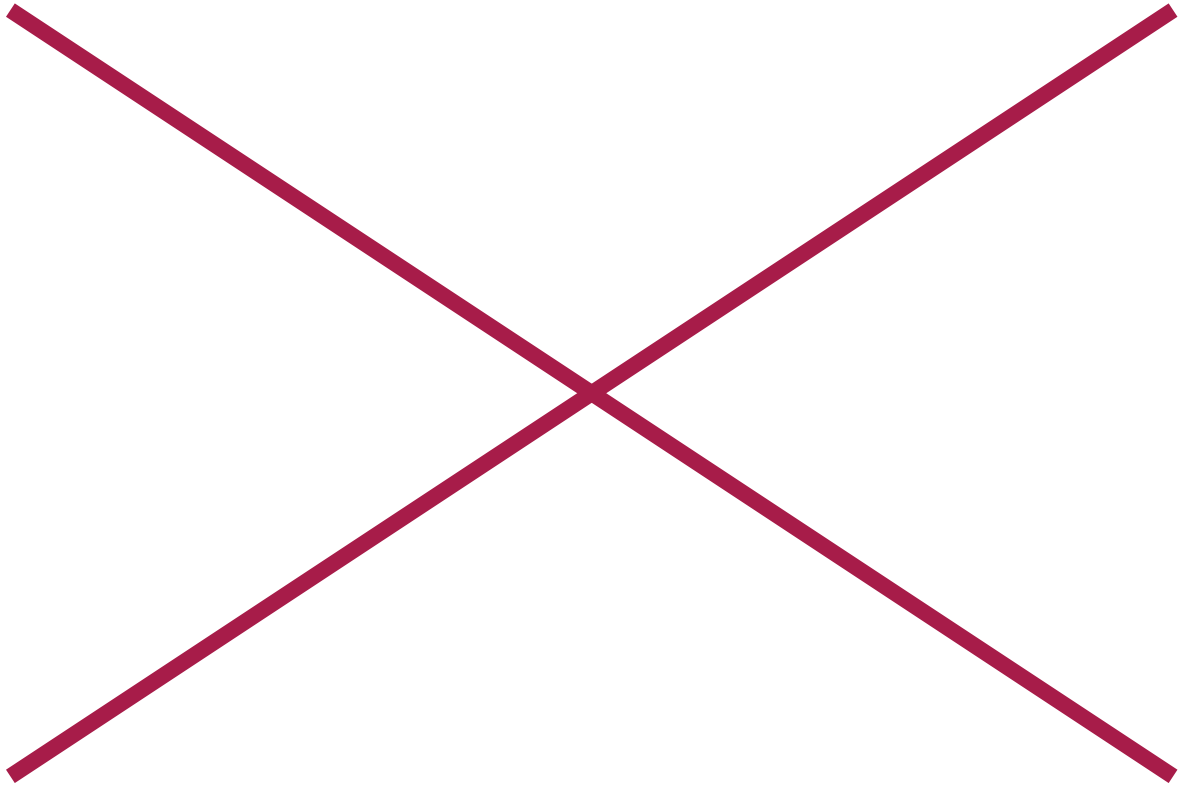


„We found that the Chinese military is "intelligentizing" warfare by **purchasing AI systems** for all manner of applications, including autonomous vehicles, intelligence analysis, decision support, electronic warfare and cyber operations."

universität wien

AI-Entscheidung über den Einsatz von Atomwaffen?

Antwort AIA?



universität wien

Was ist ein inakzeptables Risiko?

Art. 5 Abs. 1 Buchstabe (h)

[…]

„die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken”

[…]

Aber

universität wien

außer wenn und insoweit dies im Hinblick auf eines der folgenden Ziele unbedingt erforderlich ist

I. gezielte Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie die Suche nach vermissten Personen;

II. Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr eines Terroranschlags;

III. Aufspüren oder Identifizieren einer Person, die der Begehung einer Straftat verdächtigt wird, zum Zwecke der Durchführung von strafrechtlichen Ermittlungen oder von Strafverfahren oder der Vollstreckung einer Strafe für die in Anhang II aufgeführten Straftaten, die in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens vier Jahren bedroht ist.

Aber

Art. 5 hat nun 5 Absätze mehr

2. The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall only be deployed for the purposes under paragraph 1, point d) to confirm the specifically targeted individual's identity and it shall take into account the following elements:

(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;

(b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use in accordance with national legislations authorizing the use thereof, in particular as regards the temporal, geographic and personal limitations. The use of the 'real-time' remote biometric identification system in publicly accessible spaces shall only be authorised if the law enforcement authority has completed a fundamental rights impact assessment as provided for in Article 29a and has registered the system in the database according to Article 51. However, in duly justified cases of urgency, the use of the system may be commenced without the registration, provided that the registration is completed without undue delay.

3. As regards paragraphs 1, point (d) and 2, each use for the purpose of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or an independent administrative authority whose decision is binding of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation provided that, such authorisation shall be requested without undue delay, at the latest within 24 hours. If such authorisation is rejected, its use shall be stopped with immediate effect and all the data, as well as the results and outputs of this use shall be immediately discarded and deleted.

The competent judicial authority or an independent administrative authority whose decision is binding shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request and, in particular, remains limited to what is strictly necessary concerning the period of time as well as geographic and personal scope. In deciding on the request, the competent judicial authority or an independent administrative authority whose decision is binding shall take into account the elements referred to in paragraph 2. It shall be ensured that no decision that produces an adverse legal effect on a person may be taken by the judicial authority or an independent administrative authority whose decision is binding solely based on the output of the remote biometric identification system.

3a. Without prejudice to paragraph 3, each use of a 'real-time' remote biometric identification system in publicly accessible spaces for law enforcement purposes shall be notified to the relevant market surveillance authority and the national data protection authority in accordance with the national rules referred to in paragraph 4. The notification shall as a minimum contain the information specified under paragraph 5 and shall not include sensitive operational data.

4. A Member State may decide to provide for the possibility to fully or partially authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement within the limits and under the conditions listed in paragraphs 1, point (d), 2 and 3. Member States *concerned* shall lay down in their national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision and reporting relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point (d), including which of the criminal offences referred to in point (iii) thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement. Member States shall notify those rules to the Commission at the latest 30 days following the adoption thereof. Member States may introduce, in accordance with Union law, more restrictive laws on the use of remote biometric identification systems.

5. National market surveillance authorities and the national data protection authorities of Member States that have been notified of the use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes pursuant to paragraph 3a shall submit to the Commission annual reports on such use. For that purpose, the Commission shall provide Member States and national market surveillance and data protection authorities with a template, including information on the number of the decisions taken by competent judicial authorities or an independent administrative authority whose decision is binding upon requests for authorisations in accordance with paragraph 3 and their result.

6. The Commission shall publish annual reports on the use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes based on aggregated data in Member States based on the annual reports referred to in paragraph 5, which shall not include sensitive operational data of the related law enforcement activities.

963

Wörter

?

universität wien

Was ist ein hohes Risiko?


20 EURO
50 EURO
100 EURO
200 EURO

Hohes Risiko

- Risk Management (Art. 9)
- Data Governance (Art. 10)
- Technical Documentation (Art. 11)
- Record Keeping (Art. 12)
- Transparency (Art. 13)
- Human Oversight (Art. 14)
- Accuracy, Robustness, Cybersecurity (Art. 15)
- …

(2)Das Risikomanagementsystem versteht sich als ein kontinuierlicher iterativer Prozess während des gesamten Lebenszyklus eines KI-Systems, der eine regelmäßige systematische Aktualisierung erfordert. Es umfasst folgende Schritte:

a)Ermittlung und Analyse der bekannten und vorhersehbaren Risiken, die von jedem Hochrisiko-KI-System ausgehen;

b)Abschätzung und Bewertung der Risiken, die entstehen können, wenn das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird;

c)Bewertung anderer möglicherweise auftretender Risiken auf der Grundlage der Auswertung der Daten aus dem in Artikel 61 genannten System zur Beobachtung nach dem Inverkehrbringen;

d)Ergreifung geeigneter Risikomanagementmaßnahmen gemäß den Bestimmungen der folgenden Absätze.

Hohes Risiko

- Anhang I
- Anhang III

Art. 6 Abs. 1

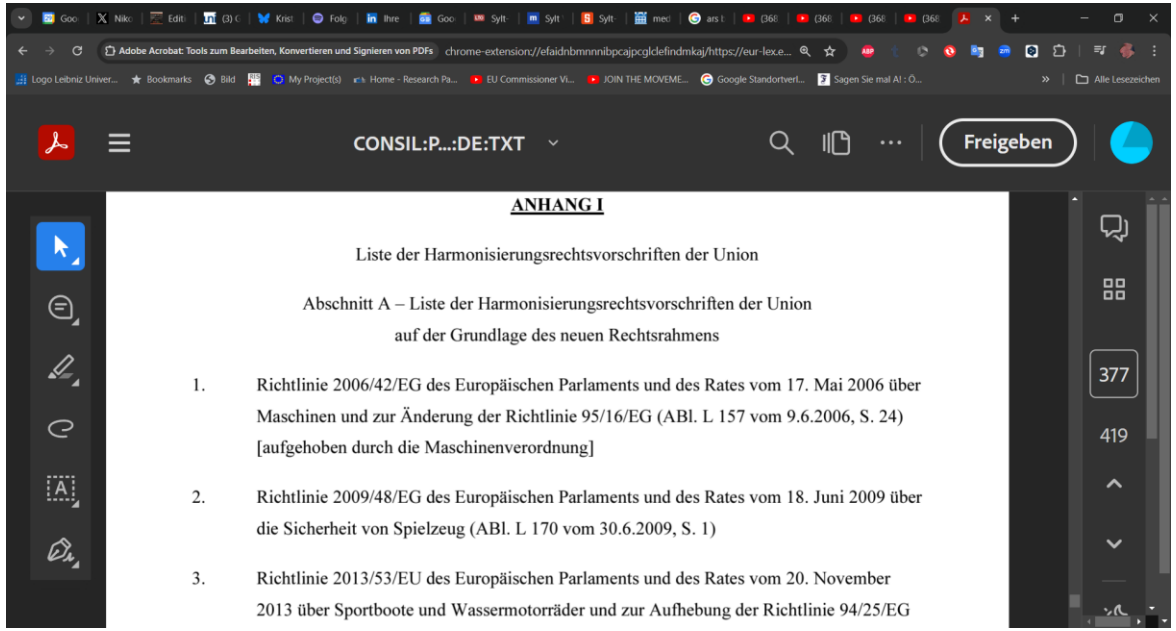
Ein KI-System [gilt] als Hochrisiko-KI-System, wenn die beiden folgenden Bedingungen erfüllt sind:

a) das KI-System soll als Sicherheitsbauteil eines unter die in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union fallenden Produkts verwendet werden oder das KI-System ist selbst ein solches Produkt;

b) das Produkt, dessen Sicherheitsbauteil gemäß Buchstabe a das KI-System ist, oder das KI-System selbst als Produkt muss einer Konformitätsbewertung durch Dritte im Hinblick auf das Inverkehrbringen oder die Inbetriebnahme dieses Produkts gemäß den in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union unterzogen werden.

Produktrisiko!

Annex 1



11. Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte

12. Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika

Anhang 3

a) KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, insbesondere um gezielte Stellenanzeigen zu schalten, Bewerbungen zu sichten oder zu filtern und Bewerber zu bewerten;

b) KI-Systeme, die bestimmungsgemäß für Entscheidungen, die die Bedingungen von Arbeitsverhältnissen, Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen beeinflussen, für die Zuweisung von Aufgaben aufgrund des individuellen Verhaltens oder persönlicher Merkmale oder Eigenschaften oder für die Beobachtung und Bewertung der Leistung und des Verhaltens von Personen in solchen Beschäftigungsverhältnissen verwendet werden soll.

- Recruiting
- MitarbeiterInnenüberwachung

Hohes Risiko

- Risk Management (Art. 9)
- Data Governance (Art. 10)
- Technical Documentation (Art. 11)
- Record Keeping (Art. 12)
- Transparency (Art. 13)
- Human Oversight (Art. 14)
- Accuracy, Robustness, Cybersecurity (Art. 15)
- …

(2)Das Risikomanagementsystem versteht sich als ein kontinuierlicher iterativer Prozess während des gesamten Lebenszyklus eines KI-Systems, der eine regelmäßige systematische Aktualisierung erfordert. Es umfasst folgende Schritte:

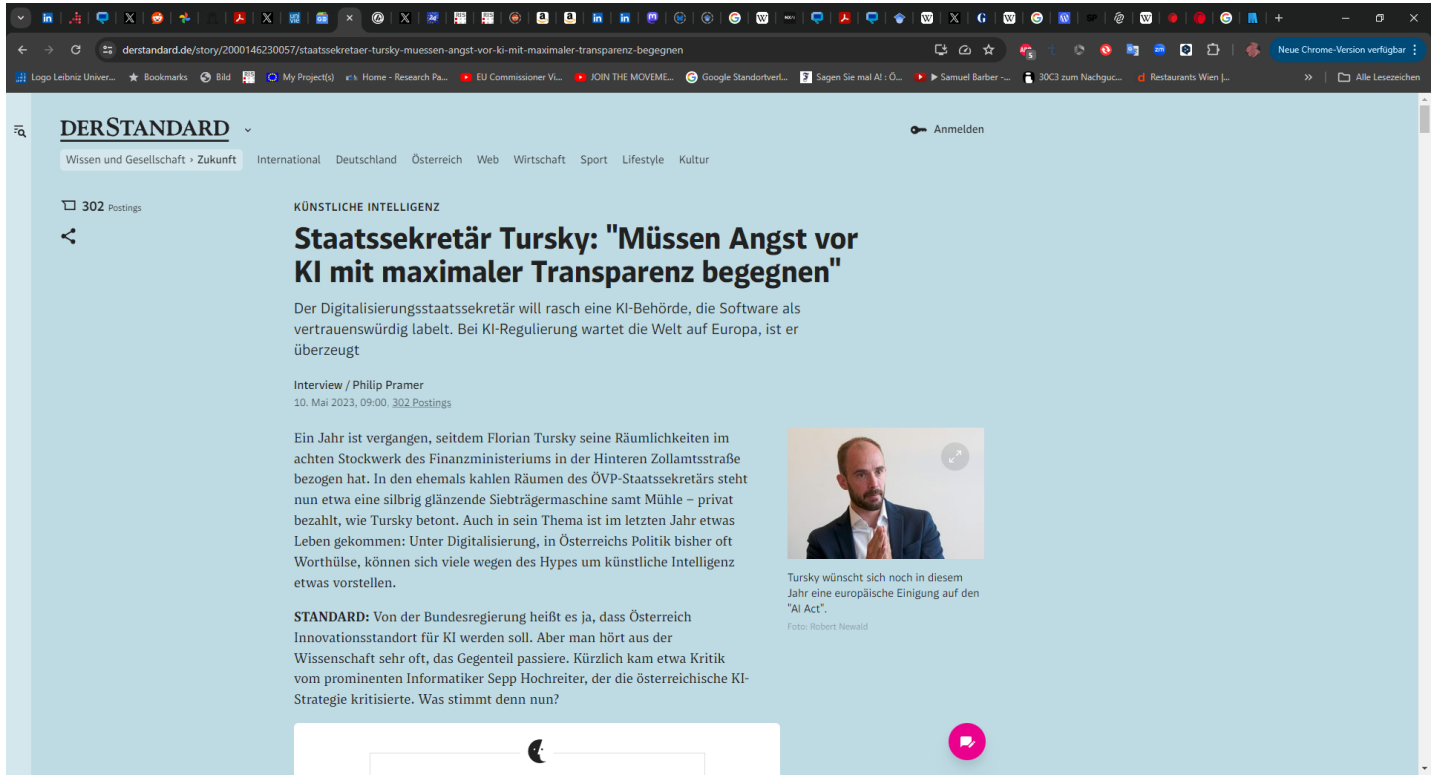
a)Ermittlung und Analyse der bekannten und vorhersehbaren Risiken, die von jedem Hochrisiko-KI-System ausgehen;

b)Abschätzung und Bewertung der Risiken, die entstehen können, wenn das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird;

c)Bewertung anderer möglicherweise auftretender Risiken auf der Grundlage der Auswertung der Daten aus dem in Artikel 61 genannten System zur Beobachtung nach dem Inverkehrbringen;

d)Ergreifung geeigneter Risikomanagementmaßnahmen gemäß den Bestimmungen der folgenden Absätze.

2 Werbeeinschaltungen



DERSTANDARD

Anmelden

Wissen und Gesellschaft › Zukunft | International | Deutschland | Österreich | Web | Wirtschaft | Sport | Lifestyle | Kultur

302 Postings

KÜNSTLICHE INTELLIGENZ

Staatssekretär Tursky: "Müssen Angst vor KI mit maximaler Transparenz begegnen"

Der Digitalisierungsstaatssekretär will rasch eine KI-Behörde, die Software als vertrauenswürdig labelt. Bei KI-Regulierung wartet die Welt auf Europa, ist er überzeugt

Interview / Philip Pramer

10. Mai 2023, 09:00, 302 Postings

Ein Jahr ist vergangen, seitdem Florian Tursky seine Räumlichkeiten im achten Stockwerk des Finanzministeriums in der Hinteren Zollamtsstraße bezogen hat. In den ehemals kahlen Räumen des ÖVP-Staatssekretärs steht nun etwa eine silbrig glänzende Siebträgermaschine samt Mühle – privat bezahlt, wie Tursky betont. Auch in sein Thema ist im letzten Jahr etwas Leben gekommen: Unter Digitalisierung, in Österreichs Politik bisher oft Worthülse, können sich viele wegen des Hypes um künstliche Intelligenz etwas vorstellen.

Tursky wünscht sich noch in diesem Jahr eine europäische Einigung auf den "AI Act".

Foto: Robert Newald

STANDARD: Von der Bundesregierung heißt es ja, dass Österreich Innovationsstandort für KI werden soll. Aber man hört aus der Wissenschaft sehr oft, das Gegenteil passiere. Kürzlich kam etwa Kritik vom prominenten Informatiker Sepp Hochreiter, der die österreichische KI-Strategie kritisierte. Was stimmt denn nun?

§ 20c KOG

1.Die RTR-GmbH hat im Rahmen der ihr gemäß § 17 Abs. 8 unter der gemeinsamen Verantwortung der beiden Geschäftsführer zum Auftrag gemachten **Servicestelle zum Kompetenzaufbau bei der Konzeption und der Nutzung von Anwendungen im Bereich der Künstlichen Intelligenz** für die Bereitstellung eines vielfältigen Informations- und Beratungsangebots zu sorgen und als zentrale Serviceeinrichtung für KI-Projekte und Anwendungen in den Fachbereichen Medien und Telekommunikation und Post zu fungieren („Servicestelle“).Die RTR-GmbH hat im Rahmen der ihr gemäß Paragraph 17, Absatz 8, unter der gemeinsamen Verantwortung der beiden Geschäftsführer zum Auftrag gemachten Servicestelle zum Kompetenzaufbau bei der Konzeption und der Nutzung von Anwendungen im Bereich der Künstlichen Intelligenz für die Bereitstellung eines vielfältigen Informations- und Beratungsangebots zu sorgen und als zentrale Serviceeinrichtung für KI-Projekte und Anwendungen in den Fachbereichen Medien und Telekommunikation und Post zu fungieren („Servicestelle“).

Abs. 2, Abs. 3

(2) Als Beitrag zur Erfüllung des in Abs. 1 dargestellten Zwecks hat die RTR-GmbH ein Informationsportal zu betreiben […]

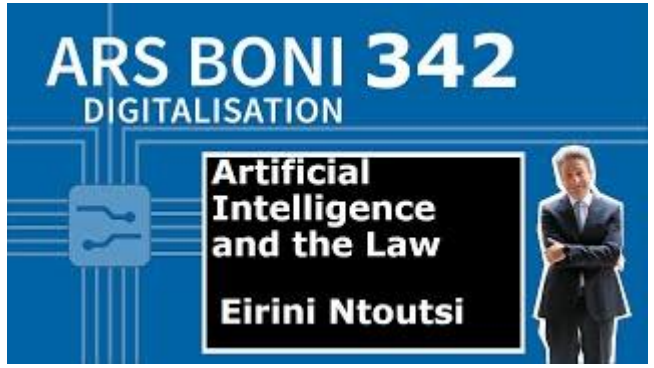
(3) Im Rahmen dieser Servicestelle umfasst die Aufgabe der RTR-GmbH im Fachbereich Medien die nachstehenden Tätigkeiten:

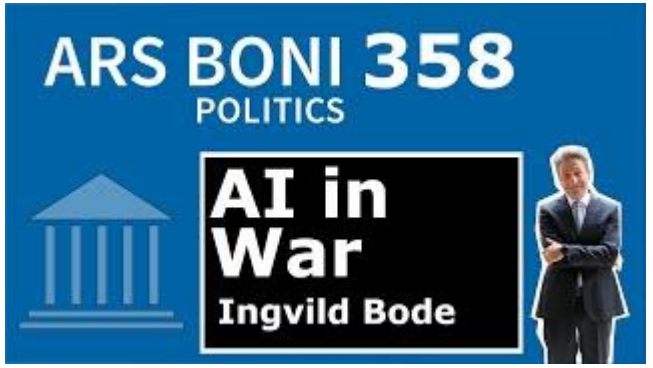
1. Bereitstellung von KI-Informationen für die interessierte Fachöffentlichkeit, insbesondere Web-Leitfäden für KI-Einsatz und Best Practices im Medienbereich;
2. Beratung öffentlicher und privater Rechtsträger zum KI-Einsatz im Medienbereich;
3. Durchführung von Studien und Analysen zum KI-Einsatz im Medienbereich;
4. Erstellung und Veröffentlichung von Publikationen zu Fragen der KI im Medienbereich;
5. Planung und Durchführung von Fachveranstaltungen zu Fragen der KI im Medienbereich;
6. regelmäßige zielgerichtete Kommunikation und regelmäßiger Austausch mit den von KI im Medienbereich betroffenen Marktteilnehmern.

universität wien

#arsboni

Werbeeinschaltung
https://www.youtube.com/@arsboni_idlaw/





universität wien

Danke!

Nikolaus Forgó, Department of Innovation and Digitalisation in Law, Universität Wien

nikolaus.forgo@univie.ac.at, @nikolausf