LAGALEGAR ÁSKORANIR OG TÆKIFÆRI VIÐ NOTKUN GERVIGREINDAR

TÓMAS KRISTJÁNSSON

LÖGFRÆÐINGUR, PERSÓNUVERNDARFULLTRÚI

ADVANIA ISLAND

TIL AÐ BYRJA MEÐ

Lagalegar áskoranir og tækifæri við notkun gervigreindar

Gervigreind og spunagreind

Tungumálalíkön (e. LLM) og það sem á íslensku hefur verið kallað spunagreind (e. Gen AI) hafa þegar haft mikil áhrif og er fyrirséð að svo verði áfram. Einfaldasta skilgreining á gervigreind er að þetta sé tækni sem nýtir algríma (e. algorithms) til að leysa af hendi verkefni sem áður voru einungis talin á færi okkar mannanna.

GDPR og AI act

Persónuverndarlög og nýlega samþykkt gervigreindarlöggjöf Evrópusambandsins veitir einstaklingum réttindi og leggur skyldur á stofnanir sem vinna með persónuupplýsingar með gervigreind. Lykilatriðið er að skilja getu og takmarkanir gervigreindar til að tryggja gagnsæi og löglega vinnslu persónuupplýsinga.

Hagnýting í samræmi við lög

Tækifærin felast í því að nýta gervigreind á löglegan og siðferðislega réttan hátt. Hröð þróun gervigreindar krefst stöðugrar endurskoðunar og það er gríðarlega mikilvægt að við missum ekki sjónar af tækninni. Fyrirtæki sem nýta gervigreind til að vinna með viðkvæmar upplýsingar ættu að setja sér reglur um örugga notkun.

HÖFUNDARÉTTUR

Lagalegar áskoranir og tækifæri við notkun gervigreindar

Tækniframfarir

Notkun gervigreindar ýtir undir nýjungar og getur hjálpað okkur að auka skilvirkni og skapa nýja hluti. Þessar breytingar eru ekki einungis til þess fallnar að hafa áhrif á núverandi störf, heldur má ætla að störf eins og við þekkjum þau í dag breytist talsvert og að ný störf verði til á sviði tækni og nýtingu hennar.

Höfundaréttur

Framleiðsla efnis með gervigreind getur vakið spurningar varðandi höfundarétt, sérstaklega þar sem gervigreind gæti framleitt vörumerki eða einhver form af list sem fellur undir höfundaréttarlög. Svo eru það álitaefni um efni sem matað er inn í tungumálalíkönin og möguleg lögbrot sem eru í rannsókn um þessar mundir.

Höfundaréttur algríma

Enn er ósvarað spurningunni um hver hefur höfundarétt á efni sem framleitt er af algrími og gervigreind. T.a.m. eru ákvæði íslensku höfundalaganna ekki líklegt til að ná til efnis sem framleitt er með gervigreind. Hugsanlega ætti löggjafinn að aðlaga sig að breyttu tækniumhverfi, en hugsanlega ekki?

PERSÓNUVERND

Lagalegar áskoranir og tækifæri við notkun gervigreindar

- **Meginreglur PVL**: Lögmæti, sanngirni, gagnsæi, tilgangstakmörkun, lágmörkun gagna og að upplýsingarnar séu áreiðanlegar, hafi takmarkaðan geymslutíma og að einhver sé ábyrgur fyrir vinnslunni.
- **Vinnsluheimildir:** Samþykki notenda er í raun eina vinnsluheimildin sem hægt er að styðjast við með góðu móti. En samþykki fylgja líka kvaðir um að það sé gefið af frjálsum vilja og að hægt sé að draga það til baka. Erfitt með mállíkön.
- Gervigreindarkerfi verða að uppfylla þessar kröfur til að tryggja að vinnsla persónuupplýsinga sé lögmæt.

PERSÓNUVERND

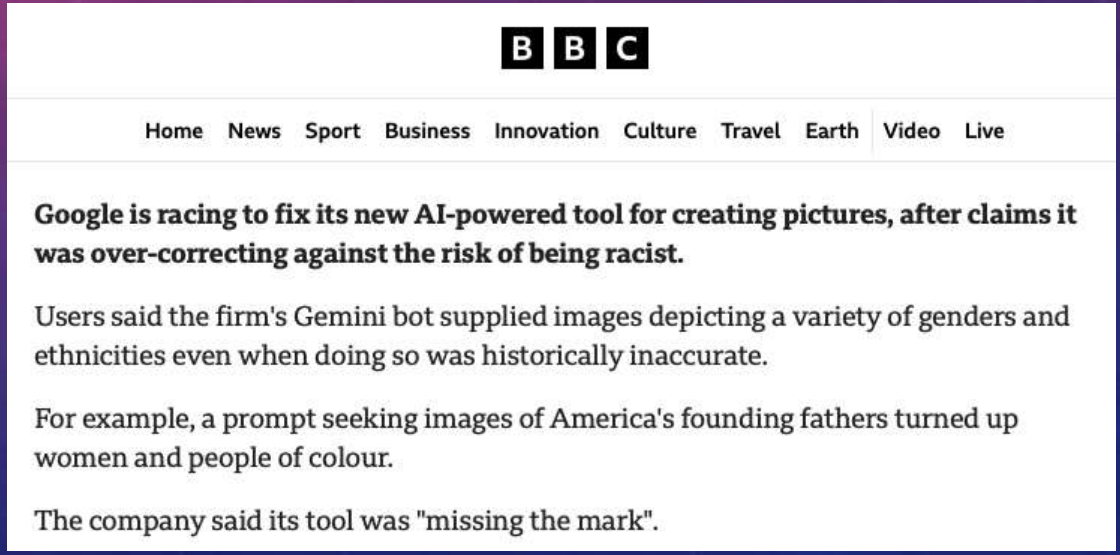
Lagalegar áskoranir og tækifæri við notkun gervigreindar

- Einn vandi mállíkana er, enn sem komið er, að eftir því sem lengur er rætt við þær eykst hætta á að þau fari að bulla.
- Bullið getur falist í að „skapa“ rangar persónuupplýsingar.

MANNRÉTTINDI

Lagalegar áskoranir og tækifæri við notkun gervigreindar

- Mállíkönin geta innihaldið eða framkallað hlutdrægni í svörum (Algorithmic Bias).
- Spunagreind erfir í eðli sínu þá hlutdrægni sem liggur í gögnunum sem hún er mötuð af (Data Bias).



BBC

Home News Sport Business Innovation Culture Travel Earth Video Live

Google is racing to fix its new AI-powered tool for creating pictures, after claims it was over-correcting against the risk of being racist.

Users said the firm's Gemini bot supplied images depicting a variety of genders and ethnicities even when doing so was historically inaccurate.

For example, a prompt seeking images of America's founding fathers turned up women and people of colour.

The company said its tool was "missing the mark".

MANNRÉTTINDI

Lagalegar áskoranir og tækifæri við notkun gervigreindar

- **Réttindi í hættu**: Ef gervigreind er ekki rétt beitt getur notkun á henni brotið á grundvallarmannréttindum, þar með talið friðhelgi, tjáningarfrelsi og jafnræði. Að greina þessi áhættu er nauðsynlegt fyrir siðferðilega þróun gervigreindar.

- **Hugsanleg brot**: Fram hafa komið áhyggjur af því að notkun gervigreindar, sérstaklega í eftirliti eða til persónugreiningar, geti leitt til mannréttindabrota. Framleiðendur og notendur að gervigreind verða að viðurkenna þessi hugsanlegu vandamál og innleiða varúðarráðstafanir í samræmi við þau.

- **Lagarammi**: Þróun lagaramma sem tekur á mannréttindaáhrifum gervigreindar er mikilvægur. Þetta felur í sér alþjóðasamninga, innlendar reglugerðir og siðareglur til að tryggja að framfarir í gervigreind séu í takt við samfélagsgildi og réttindi.

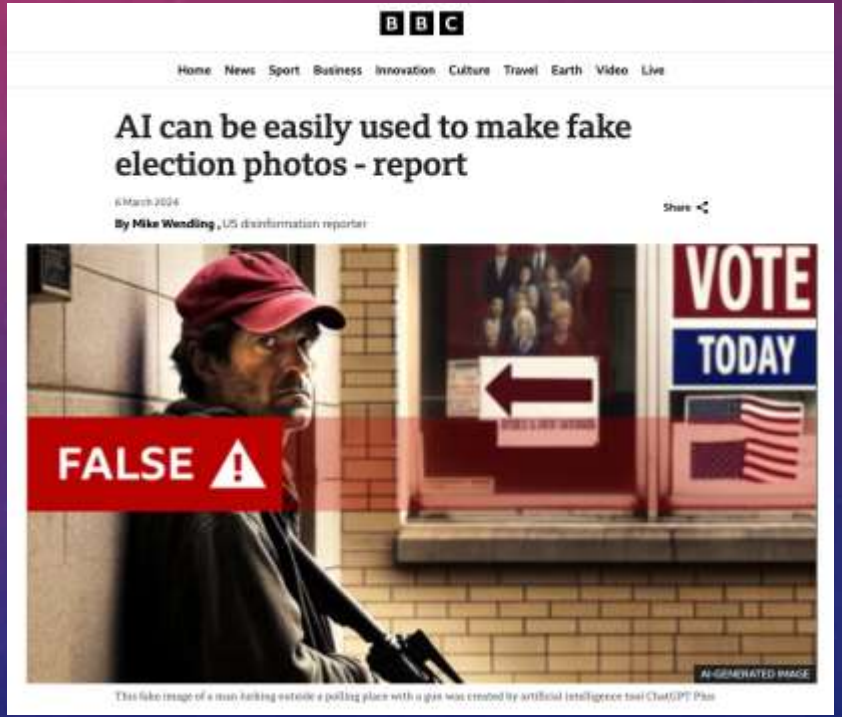
UPPLÝSINGAÓREIÐA

Lagalegar áskoranir og tækifæri við notkun gervigreindar

Misupplýsingar (e. misinformation) og rangupplýsingar (e. disinformation): Röngum eða misvísandi upplýsingum er deilt af/án ásetnings, ýmist til að valda skaða eða ekki.

- **Falsfréttir**: Spunagreind getur framleitt sannfærandi en rangar upplýsingar, sem stuðlað að útbreiðslu rangra upplýsinga. Falsfréttir, framleiddar af spunagreind, geta líka endað sem þjálfunargögn.

- **Djúpfalsanir**: Djúpfölsun sem framleidd er af spunagreind er hægt að nota til að blekkja fólk eða hafa áhrif á fjölmiðla.



ÁHRIF OG ÁVINNINGUR

Lagalegar áskoranir og tækifæri við notkun gervigreindar

Mismunun
Gervigreind getur haft neikvæð áhrif á störf og þjónustu – gæti mismunað fólki vegna t.d. kynþáttar, kyns og aldurs.

Það sem ber að varast
Ávinningur af notkun spunagreindar er hugsanlega ekki dreift jafnt, sem gæti aukið efnahagslegan ójöfnuð.

Stórfyrirtæki/ríkisstjórnir gætu notað spunagreind til að stjórna eða hafa áhrif á almenningsálit.

Vinnumarkaðurinn
Innleiðing spunagreindar í ýmsum atvinnugreinum gæti leitt til verulegs atvinnutaps og jafnvel að ákveðin störf leggist af. Ekki óþekkt með tæknibyltingar.

ÁHRIF OG ÁVINNINGUR

Lagalegar áskoranir og tækifæri við notkun gervigreindar

Ávinningurinn
Sé rétt staðið að notkun gervi- og spunagreindar er ávinningurinn augljós. Þekkingin getur gert okkur afkastameiri og þróað ný störf. Þeir notendur sem setja sér skýrar reglur um notkun gervigreindar eru öðrum framar á markaðnum.

Notendur
Það þarf að passa að ábyrgir framleiðendur séu notaðir og að viðkvæmar upplýsingar séu ekki mataðar inn í gervigreind og endi þar sem þjálfunargögn fyrir “opna” gervigreind. Einnig þarf að rýna það sem spunagreindin skilar okkur, t.a.m. útfrá persónuvernd og upplýsingaöryggi ef gervigreind er notuð í hugbúnaðargerð.

Samtalið
Þróun gervigreindar mun alltaf kalla á samtal um siðferðileg álitamál og löglega notkun. Löggjafinn, þróunaraðilar og notendur verða að eiga samtal um að samræma tæknilega getu við samfélagsleg gildi og viðmið.

AÐ LOKUM

Lagalegar áskoranir og tækifæri við notkun gervigreindar

Framhaldið

Það er ljóst að til að geta nýtt þessa tækni sem best þurfa notendur hennar að tileinka sér hraðar breytingar. Breytingarnar krefjst aðlögunarhæfni og þurfa að byggja á áhættustjórnun, tækniþekkingu og skuldbindingu við mannréttindi og siðferðislega notkun.

Af hverju?

Árangursríkar aðferðir til að tryggja hlítingu við lög felur í sér skuldbindingu um siðferðislega notkun gervigreindar og að hún sé þróuð og notuð á samfélagslega ábyrgan hátt.

Mikilvægt er að slaka ekki á reglunum þegar gervigreindin verður betri og passa verður að reglur um notkun séu uppfærar reglulega og í t.d. leiðbeiningar European AI Office og ISO/IEC 42001

Að lokum

Áhuginn á gervigreindinni er óvenjumikill miðað við flestar tækninýjungar sem við höfum upplifað. Fyrirtæki sem hyggjast nýta sér þessa tækni ættu ekki að eiga í vandræðum með að laða til sín fólk sem uppfyllir þau skilyrði sem þarf til að meðhöndla gervigreind á þann hátt sem tæknin krefst.