LÖGFRÆÐI
Lára Herborg Ólafsdóttir
lögmaður og eigandi á LEX lögmannsstofu

Spjallmennið ChatGPT

Í síðasta mánuði kynnti fyrirtækið Open AI að gervigreindarlíkan á vegum félagsins, Chat GPT, yrði þróað á íslensku sem verður þá annað tungumálið sem notast má við í líkaninu á eftir ensku. Gervigreindarlíkanið, sem er nú aðgengilegt í 4. útgáfu, hefur marga eiginleika enda styðst það við sífellt þróaðri og öflugri gervigreindartækni. Aðspurt segir spjallmennið að nýta megi það til forritunar ýmissa tölvuforrita á borð við tölvuleiki, ýmiss konar listsköpunar, gagnagreiningar fyrirtækja sem og markaðsrannsókna ásamt því að geta svarað tölvubréfum.

Verður að telja það sérstakt fagnaðarefni að útbreiddasta forritið af þessum toga skuli aðgengilegt á íslensku og mun það vonandi nýtast í ýmsum störfum og til framþróunar á innlendum vettvangi. Sá böggull fylgir skammrifi að veigamiklar lagalegar áskoranir geta fylgt notkun gervigreindarlíkana og því mikilvægt að varlega sé af stað farið í notkun þeirra.

Í *fyrsta lagi* má nefna að gervigreindarlíkan vinnur með fyrirliggjandi gögn, og þegar verið er að nota líkanið við listsköpun, þá kann eftir atvikum afurð líkansins að brjóta í bága við höfundarréttarvernd þess er skapaði upphafleg(t) verk, svo sem texta, tónsmíð, o.fl., og þá þannig að notandi líkansins gerist, óafvitandi, sekur um brot á höfundarrétti og eftir atvikum sæmdarrétti viðkomandi.

> Sá böggull fylgir skammrifi að veigamiklar lagalegar áskoranir geta fylgt notkun gervigreindarlíkana

Í *annan stað* kunna þau gögn sem gervigreindarlíkanið vinnur með að innihalda persónuupplýsingar, jafnvel viðkvæmar upplýsingar, um tilgreinda einstaklinga og getur slík vinnsla farið í bága við persónuverndarreglur.

Í því samhengi má nefna að ítalska persónuverndarstofnunin mælti í síðasta mánuði fyrir um að ChatGPT skyldi, meðan á frekari rannsókn máls stæði, hætta allri vinnslu persónuupplýsinga um einstaklinga búsetta á Ítalíu. Í ákvörðuninni var tiltekið að ChatGPT virti ekki gagnsæiskröfur við notkun persónuupplýsinga, ekki væri lagastoð fyrir vinnslu persónuupplýsinga í forritinu, ónákvæmni gætti við vinnslu slíkra upplýsinga þar sem svör er ChatGPT birti væru ekki ávallt í samræmi við undirliggjandi gögn auk þess sem ekki væru aðgangshindranir að forritinu m.t.t. aldurs notanda. Þá hefur einnig verið skipaður starfshópur á vegum Evrópska persónuverndarráðsins til að taka starfsemi OpenAI og ChatGPT til sérstakrar skoðunar og má vænta þess að persónuverndaryfirvöld innan EES-svæðisins fylgist náið með frekari notkun gervigreindarlíkana og hvort vinnsla með persónuupplýsingar í þeim samrýmist persónuverndarreglugerðinni.

Í *þriðja* lagi má jafnframt nefna að gervigreindarlíkön líkt og ChatGPT kunna að geta ljóstrað upp ýmsum leyndarmálum sem leynst geta í gagnasöfnum, svo sem viðskiptaleyndarmálum, og þannig sett notanda þeirra í óheppilega stöðu í lagalegu tilliti sé unnið frekar með slíkar upplýsingar.

Auk þess má nefna að þegar bornar eru undir gervigreindarlíkön spurningar um tiltekin álitamál byggjast svörin á fyrirliggjandi gögnum. Þau svör kunna þannig að styðjast við gögn sem birta sögulega mismunun og eiga ekki að vera lögð til grundvallar, svo sem er varðar kyn, kynþátt eða lífsviðhorf. Sé stuðst við niðurstöður gervigreindarlíkana, svo sem við mat á lánshæfi, starfsumsókn eða beiðni um félagslegt úrræði, kann því að halla á þjóðfélagshópa sem á árum áður stóðu höllum fæti í samfélaginu án þess að tækar forsendur búi þar að baki. Sams konar sviðsmyndir má ímynda sér ef dómstólar nýttu þjónustu gervigreindarlíkana við úrlausn dómsmála.

Í Evrópusambandinu er á allra næstunni fyrirhugað að lögfesta gervigreindarreglugerð sem hefur að markmiði að marka skýrar lagaumhverfi um gerð og notkun gervigreindar. Reglugerðardrögin ráðgera fyrst og fremst kvaðir á þá sem þróa og markaðssetja slíkar vörur eða hugbúnað, en ákveðnar skyldur hvíla auk þess á innflytjendum slíks búnaðar, dreifingaraðilum og eftir atvikum notendum. Væntanleg reglugerð veitir notendum og framleiðendum gervigreindarlausna skýrari leiðsögn um heimilar og óheimilar aðferðir við gerð og notkun gervigreindar en svarar þó ekki öllum álitamálum þar um.

Gervigreindarlíkön á borð við ChatGPT búa yfir miklum möguleikum. Á hinn bóginn er mikilvægt fyrir fyrirtæki, sem og einstaklinga, að þekkja takmarkanir þeirra og áhættu. Skynsamlegt kann að vera fyrir fyrirtæki að setja sér reglur varðandi notkun gervigreindarlíkana, sem hluta af áhættustýringu sinni, og þannig að dregið sé úr líkindum válegra lögfylgna.