



Gagnavernd og Gervigreind



Gögn & AI

Samspil gagnaverndar og gervigreindar—tvö öfl sem móta hvernig við verndum upplýsingar á stafrænum tímum.“

Hjörtur Árnason





Verndun gagna

Þar sem gögn verða sífelld mikilvægari fyrir fyrirtæki og samfélög er vernd þeirra mikilvægari en nokkru sinni fyrr. Á sama tíma umbreytir gervigreind atvinnugreinum, en hún skapar líka nýjar áhættur og áskoranir. Í þessari kynningu skoðum við hvernig gervigreind styrkir öryggi, hvar hún getur skapað veikleika og hvaða bestu aðferðir hjálpa okkur að vera örugg.“

Hvað er gagnavernd?

„Gagnavernd byggir á þremur stöðum:

- **Trúnaður**—að aðeins réttir aðilar hafi aðgang að viðkvæmum upplýsingum.
- **Heilleiki**—að gögnum séu ekki breytt eða skemmd.
- **Aðgengi**—að kerfi séu virk og gögn tiltæk þegar þeirra er þörf. Þessar meginreglur mynda grunn trausts í stafrænum kerfum.“

Gervigreind í gagnavernd

„Gervigreind er öflugur bandamaður í netöryggi. Hún getur greint ógnir hraðar en menn með því að sjá óvenjuleg mynstur. Hún getur spáð fyrir um mögulegar árásir áður en þær gerast og hún getur sjálfvirknivætt viðbrögð til að draga úr tjóni. Með öðrum orðum, gervigreind hjálpar okkur að fara frá varnarviðbrögðum yfir í fyrirbyggjandi vernd.“

Áhættur gervigreindar í öryggi

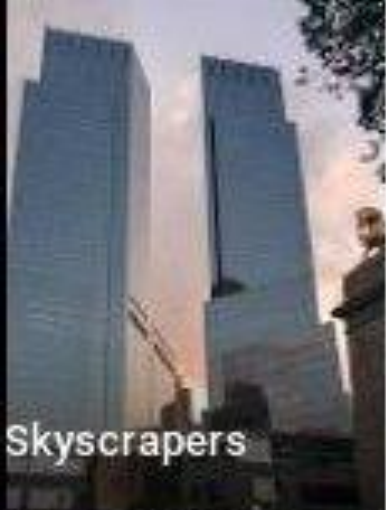
„Auðvitað er gervigreind ekki gallalaus. Árásaraðilar geta nýtt sér veikleika með árásum, sem blekkja líkön til að taka rangar ákvarðanir. Skekkja í gervigreindarkerfum getur leitt til ósanngjarnra eða ónákvæmra niðurstaðna. Og sú gríðarlega gagnasöfnun sem gervigreind krefst vekur alvarlegar **persónuverndarspurningar**. Þannig að þótt hún hjálpi, skapar hún líka nýjar áskoranir.“



McDonald's – AI bílalúga

- 🍔 McDonald's – AI í bílalúgu (2024)
- **Hvað gerðist:** McDonald's prófaði AI-kerfi til að taka niður pantanir í bílalúgu.
- **Hneykslið:** Viðskiptavinir upplifðu fáránleg mistök, eins og að AI stækkaði McNuggets-pöntun í **260 stykki** eða mistúlkaði einfaldar pantanir. Myndbönd fóru á flug á netinu og vöktu háð.
- **Áhrif:** McDonald's hætti verkefninu árið 2024 vegna slæmrar upplifunar viðskiptavina og orðsporsskaða.

Google Photos (2015)



Skyscrapers



Airplanes



Cars



Bikes



Gorillas



Graduation

- **Rangt merkingarkerfi (2015)**
- **Hvað gerðist:** AI-kerfi Google til að merkja myndir flokkaði ranglega myndir af svörtum einstaklingum sem „górillur“.
- **Hneykslið:** Petta olli reiði og ásökunum um kynpáttafordóma í AI-kerfum.
- **Áhrif:** Google baðst afsökunar, slökkti á eiginleikanum og varð fyrir alþjóðlegri gagnrýni á hættuna af hlutdrægum þjálfunargögnum.



Bestu aðferðir

„Til að halda jafnvægi milli nýsköpunar og öryggis þarf að:

- Nota **dulkóðun** til að vernda gögn í geymslu og flutningi.
- Beita **aðgangsstýringu** svo aðeins réttir aðilar sjái viðkvæm gögn.
- Framkvæma **reglulegar úttektir** til að finna veikleika snemma.
- Viðhalda **mannlegu eftirliti** til að tryggja ábyrgð. Þessar aðferðir halda gervigreindarkerfum öruggum og traustum.“

AITól og ávinningur þeirra

- Auka framleiðni:** Rafræn endurtekning verkefna og fríar mannlegan tíma.
- Bæta ákvörðunartöku:** Veita innsýn úr stórum gagnahæimur hratt.
- Bæta sköpunargáfu:** Mynda nýjar hugmyndir, hönnun og efni.
- Auka nákvæmni:** minnka mannleg mistök í greiningu og spám.
- Persónuleggja upplifanir:** Aðlaga tillögur og samskipti að einstaklingum.
- Skala aðgerðir:** Meðhöndla stór úthlutanir án þess að kostnaður hækkar hlutfallslega.

AI	Tól	Ávinningur
1	ChatGPT	"Málsniðskilningur fyrir skrif, spurning og svör, og hugmynda auðgi"
2	MidJourney	sköpun sniðugra mynda út frá texta tilmælum
3	DALL·E	Sérsniðnar teikningar og hönnunareignir
4	Grammarly	Rauntíma skriftaraðstoð með málfræðikönnunum og tónprófunum
5	Jasper AI	Markaðssetning texta fyrir blogg, auglýsingar og tölvupósta.
6	Synthesia	"AI myndagerð með persónum og raddmáli"
7	Hugging Face	opinn-gagnagrunnur AI líkön fyrir NLP, sjón og meira
8	IBM Watson	fyrirtækja-gervigreindarlausnir fyrir greiningu og þjónustu við viðskiptavinum
9	Google Bard	"Leitarauki AI svör fyrir rannsóknir og könnun"
10	DataRobot	Sjálfvirk vélafræðsla fyrir spágreiningu

Framtíðarsýn

„Í framtíðinni mun gervigreind halda áfram að knýja fram snjallari netöryggislausnir. Á sama tíma munu alþjóðlegar reglugerðir eins og GDPR og væntanleg AI-lög móta hvernig stofnanir meðhöndla gögn á ábyrgan hátt. Siðferðileg gervigreind—gegnsæ, sanngjörn og útskýrandi—verður lykillinn að trausti.“

Öryggisflokkun gagna á Íslandi

Opin gögn

Ópersónugreinanleg gögn eða gögn sem eru opin og aðgengileg til notkunar og endurnotkunar. Svo gögn teljist opin þurfa þau að vera tiltæk án umsókna / beiðna og vera aðgengileg óháð tíma.

Varin gögn

Öll gögn önnur en opin gögn sem eru hluti af daglegum rekstri ríkisaðila. Varin gögn geta þó verið misviðkvæm og krafist sérsniðinna öryggisúrræða í samræmi við niðurstöður áhættumats. Gögn sem verja skal bæði vegna hagsmuna einstaklinga (Persónuvernd) og lögaðila.

Sérvarin gögn

Gögn sem vegna viðkvæmrar stöðu m.t.t. tímasetninga eða innihalds geta valdið víðtæku og langvarandi tjóni fyrir hópa einstaklinga, lögaðila eða ríkisaðila.

Afmörkuð gögn

Gögn sem eru viðkvæm fyrir samfélagið í heild eða stöðu þjóðarinnar á alþjóðavettvangi

Niðurstaða

„Til að draga saman niðurstöður: Gervigreind er bæði öflugt verkfæri og á sama tíma möguleg áhætta í gagnavernd. Sterkar aðferðir eru áfram nauðsynlegar, og samvinna milli manna og gervigreindar er lykillinn að árangri. Með því að sameina tækni og ábyrgð getum við verndað gögn á sama tíma og við tökum á móti nýsköpun.“

„Hvernig sjáið þið jafnvægið milli nýsköpunar og öryggis í ykkar eigin starfi eða atvinnugrein?“

Bestu starfsvenjur fyrir AI-uppsetningu í
Microsoft 365





Samanburðartafli

Útgáfa	Kostnaður	Samþætting	Helstu kostir
Copilot Ókeypis	Ókeypis	Sjálfstætt	Spjall, vefleit, myndagerð
Copilot Pro	Greidd áskrift	Sjálfstætt + hraði	Forgangur að GPT-5, skapandi verkfæri
M365 Personal/Family	Áskrift	Office forrit	Skjöl, tölvupóstur, töflureiknir
M365 Enterprise Premium	Fyrirtækjalykill	Öll vistkerfi	Öryggi, samræmi, sérhæfðir Copilot

Miðað við áherslur fyrirtækja á **öryggi og stjórnarháttum í upplýsingatækni**, er **Enterprise Premium** útgáfan sú sem hentar best fyrirtækjum. Hún styður við **ISO 27001, NIST og aðrar samræmisramma** með rekjanleika, gagnavernd og stjórnendastýringu.

Verð samanburður

Útgáfa	Verð (USD/mán)	Verð (ISK/mán, áætlað)	Helstu kostir
Copilot Ókeypis	0	0	Spjall, vefleit, myndagerð
Copilot Pro	~20	~2.800	Forgangur að GPT-5, hraðari svör
M365 Personal/Family	~30	~4.200	Samþætting við Office forrit
M365 Business	~36	~5.000	Office + Copilot fyrir fyrirtæki
M365 Enterprise Premium	36–84,75	~5.000–12.000	Öryggi, samræmi, sérhæfðir Copilot

Útgáfur af Copilot og helstu kostir

Copilot - ókeypis

- **Aðgangur:** Í boði á copilot.microsoft.com og í Edge, Windows og farsímaforritum.

- **Hæfni:**

- Spjall og svör byggð á gervigreind
- Vefleit og almennar upplýsingar
- Myndagerð og myndvinnsla

- **Takmarkanir:**

- Engin samþætting við Microsoft 365 forrit (Word, Excel, Outlook, Teams)
- Hægari svör á álagstímum

Copilot Pro

Fyrir: Notendur sem vilja hraðari og öflugri gervigreind.

•Kostir:

- Forgangaðgangur að GPT-5 (hraðari og stöðugri svör)
- Betri myndagerð og skapandi verkfæri
- Aðgangur að nýjum eiginleikum fyrr en almennir notendur

•Takmarkanir:

- Aðallega fyrir einstaklinga, ekki fyrirtæki

Microsoft 365 Personal & Family

- **Sambætting:** Copilot innbygggt í Word, Excel, PowerPoint, Outlook og Teams.
- **Kostir:**
 - Sjálfvirk drög að skjölum og samantektir úr tölvupósti
 - Greining á töflureiknum og fundarglósum
 - Family útgáfan leyfir mörgum notendum að deila áskrift
- **Best fyrir:** Nemendur, fagfólk og fjölskyldur sem nota Office daglega.

Microsoft 365 Enterprise Premium

- **Fyrir:** Fyrirtæki og stofnanir í ströngu reglubundnu umhverfi.
- **Kostir:**
 - Fyrirtækjaöryggi, samræmi og stjórnun
 - Sérhæfðir Copilot fyrir hlutverk (t.d. Sales Copilot, Security Copilot)
 - Samþætting við Azure, SharePoint og Teams
 - Stjórnendastýring, gagnageymsla og rekjanleiki (audit logs)
- **Best fyrir:** Skipulögð fyrirtæki sem þurfa **áhættustjórnun, samræmi og rekstrarþol.**

Dæmigerð vandamál

Hver í sínu horni

Ekki samræmi í
notendaviðmótinu

Mikill tími í
reddingar eftir á

Margar lausnir
sem gera það
sama

Kalla til ráðgjafa í
öll
kerfisstjóráverkefni

Vantar
forgangsroðun
verkefna



Copilot áskoranir



Óreiðukenndar heimildir
og ofdeiling gagna



Að meðhöndla AI sem „bara hlut af
upplýsingatækni“ og skortur á
stuðningi.



Skipulagsheildum, þ.e.
sameiginlegt markmið



Öryggi- og samræmisgallar.
Ekki tilbúið í AI



Slæmt skipulag á gögnum og
úrelt uppbygging

Skilgreindu skýra AI-stefnu

- Samræmdu innleiðingu AI við markmið fyrirtækisins (t.d. framleiðni, nýsköpun, upplifun viðskiptavina).
- Settu mælanleg lykilárangursviðmið (KPI) til að fylgjast með ávinningi af verkfærum eins og Copilot.
- ***KPI** stendur fyrir **Lykilmælikvarði (Key Performance Indicator)**. Það er mælanlegt gildi sem sýnir hversu vel einstaklingur, teymi eða stofnun nær ákveðnu markmiði*

Stjórnun og öryggi

- Innleidd **gagnastjórnun** til að tryggja að viðkvæmar upplýsingar séu varðar.
- Notaðu Microsoft Purview og samræmisverkfæri til að stýra aðgangi og varðveislu gagna.
- Byggðu á **zero-trust öryggislíkani** til að tryggja örugga AI-vinnslu.

Stigvaxandi innleiðing Copilot

- Byrjaðu með tilraunahópum sem prófa Copilot í Word, Excel, PowerPoint, Outlook og Teams.
- Safnaðu endurgjöf, fínstilltu reglur og stækkaðu síðan smám saman.
- Tryggðu að leyfi og tæknileg aðstaða séu tilbúin áður en útbreiðsla hefst.

Hvað virkar vel

Einfaldleiki

Haltu flokkurastiginu einföldu

Prófa

Prófaðu fyrst, fínstilltu og þróaðu meira

Sjálfvirkni

Sjálfvirkni þar sem það hefur áhrif.

Taka þátt

Tengdu snemma saman hagsmunar aðila og notendur í verkefnið.

Starfsfólksþjálfun og valdefling

- Bjóða upp á **hagnýta þjálfun** svo starfsmenn skilji hvernig nota á AI á ábyrgan hátt.
- Hvetjið til tilrauna með Copilot fyrir uppkast, samantektir og greiningar.
- Deilið bestu starfsvenjum um jafnvægi sjálfvirkni og mannlegrar yfirferðar.

Gagnaundirbúningur

Mikilvæg atriði.

- Hreinsaðu og skipulegðu gögn í SharePoint, OneDrive og Teams til að hámarka nákvæmni AI.
- Tryggðu að lýsigögn og heimildir séu rétt stillt svo Copilot geti sótt viðeigandi efni.

Siðferðileg og ábyrgt AI-notkun

- Settu reglur um **ábyrga AI-notkun** (meðvitund um hlutdrægni, gagnsæi, ábyrgð).
- Upplýstu starfsmenn skýrt um hvað AI getur og getur ekki gert.
- Fylgstu með notkun til að koma í veg fyrir ofnotkun eða misnotkun.

Stöðug endurbót

- Uppfærðu reglulega AI-módel og Microsoft 365 forrit til að nýta nýja eiginleika.
- Safnaðu endurgjöf frá notendum til að betrumbæta vinnuflæði.
- Vertu upplýstur um þróunaráætlun Microsoft fyrir Copilot og tengd þjónustutól.

Dæmigerð innleiðingaráætlun

Fasi	Aðgerðir	Niðurstaða
1. Áætlanagerð	Skilgreindu markmið, stjórnun, samræmi	Skýr AI-rammi
2. Tilraun	Innleiðing hjá litlum hópi	Endurgjöf, betrubætur
3. Útbreiðsla	Stækkaðu yfir deildir	Aukinn árangur, örugg innleiðing
4. Hagræðing	Þjálfun og stöðugar uppfærslur	Sjálfbær AI-notkun

Niðurstaða:

✅ Bestu starfsvenjur fyrir AI í Microsoft 365 snúast ekki bara um að virkja Copilot—heldur um **stefnumótun, öryggi, þjálfun starfsfólks og stöðugar betrumbætur**. Rétt innleiðing gerir AI að traustum samstarfsaðila í framleiðni fyrirtækisins.

- **Mannleg yfirumsjón er lykilatriði** → Sjálfvirk kerfi verða að vera vöktuð og endurskoðuð.
- **Orðsporsáhætta er raunveruleg** → Ein mistök sem verða að netgríni geta eyðilagt traust í mörg ár.



Takk fyrir mig