



Kennissessie: Informatiebeveiliging, Privacy, AI en algoritmes

Andrea van Gent & Sander Brabander

Clint Reinders, Cemre Karso

DORDRECHT



Agenda

- **16.00 - 16.50:** Versterken lokale democratie in een digitale wereld
- **17.00 - 17.30:** Hoe gaan we om met kunstmatige intelligentie en algoritmes en welke ethische dilemma's zijn er?
- **17.30 - 17.45:** Toelichting nieuwe richtlijnen (addendum) apparaat gebruik Dordtse raad
- **Vanaf 17.45:** Uitloop en hulp bij veilig werken op de iPad



1. Versterken van de lokale democratie in een digitale wereld

(Digitale) beïnvloeding, informatiebeveiliging en sociale media-gebruik

DORDRECHT



Democratische principes onder druk door digitalisering

Digitalisering raakt alle vlakken van het maatschappelijke leven

Ontwikkelingen gaan steeds sneller

Overheden en burgers dreigen grip te verliezen

De macht van 'big data' en 'big tech'



Hoe advertenties op Sociale Media stemgedrag kunnen beïnvloeden

Casus: Brexit door Facebook?



Ebbw Vale - Wales

- Opvallend hoog percentage 'leave' stemmers
- 'Leave' campagne was rechts, Ebbw Vale is links
- Tientallen miljoenen EU geld geïnvesteerd
- Bevolking noemt angst voor immigranten en vluchtelingen als reden, die zijn er nauwelijks in Ebbw Vale
- Wat is er aan de hand?





Facebook maakt (gedwongen) advertenties openbaar

Britse burgers geconfronteerd met
nepnieuws advertenties over toetreding
Turkije tot de EU

Regelgeving doelbewust omzeilt door
tussenpartijen, toezicht schiet tekort

Hoe eerlijk zijn verkiezingen als mensen
hun stem baseren op nepnieuws?



Casus: Hack 72 Duitse gemeentes

Wat gebeurde er?

- 72 Duitse gemeentes raakten in november 2023 onbereikbaar na aanval op gemeentelijke IT-dienstverlener SIT
- Digitale dienstverlening kwam volledig tot stilstand
- 1,7 miljoen burgers (indirect) getroffen
- Twee maanden na de hack was de dienstverlening nog maar mondjesmaat opgestart



▲ Foto ter illustratie. © Archief

Vrees voor vloedgolf aan phishingmails door ChatGPT, mensen oplichten wordt kinderspel

EXPERTS BEZORGD Criminelen maken volop gebruik van ChatGPT om frauduleuze mails te schrijven die niet van echt te onderscheiden zijn. Experts vrezen de komende jaren voor een vloedgolf aan zogeheten phishingmails en stellen dat vooral kleine bedrijven en ouderen zonder digitale kennis hier onvoldoende tegen beschermd zijn. „Dit is een technologie die niet twee of drie keer sneller en slimmer wordt per jaar, maar een miljoen keer.”



▲ Een illustratieve weergave van de phishing van persoonsgegevens door een hack en phishing © Rob Engelaar

Bijna helft online fraudegevallen komt doordat slachtoffer direct handelt: 'Verkeerde beslissing door tijdsdruk'

Bijna de helft (44 procent) van de Nederlandse online fraudegevallen is te voorkomen, mits het slachtoffer maar niet direct tot handelen overgaat en zo de fraudeur in de kaart speelt. Dat blijkt uit onderzoek onder fraudeslachtoffers, uitgevoerd in opdracht van ABN Amro.



Een op de vijf Nederlandse bedrijven betaalt losgeld na aanval met gijzelsoftware

Door onze techredactie

22 feb 2024 om 10:31

Update: 5 dagen geleden



111 reacties



Delen

Criminelen hebben vorig jaar 147 succesvolle aanvallen met gijzelsoftware uitgevoerd op grote Nederlandse bedrijven. Van de getroffen bedrijven betaalde 18 procent losgeld, zodat ze weer toegang kregen tot hun systemen.



Grote maatschappelijke en economische impact

Dit raakt u ook!



▲ Publieksbalie in de centrale hal van het gemeentehuis in Hof van Twente. © Cees Elzenga / hetoog.nl

Gemeenteraad Hof van Twente steekt hand in eigen boezem na hack: 'Alles rondom beveiliging van onze informatie moet beter'

GOOR - De gemeenteraad van Hof van Twente steekt de hand in eigen boezem na de desastreuze cyberaanval van twee jaar geleden.



Wat de raad kan doen:

- Advies VNG: Organiseer het maatschappelijk debat
- Advies VNG: Verken weerbaarheid bij uw achterban (ondersteunde initiatieven)
- De raad wordt via de reguliere P&C cyclus en de jaarlijkse ENSIA* geïnformeerd

ENSIA


= Eenduidige Normatiek Single Information Audit

- Alle gemeenten verantwoordden zich over informatiebeveiliging middels ENSIA
- Verantwoording op basis van de 'Baseline Informatiebeveiliging Overheid' (BIO) en het gebruik van de Geo-basisregistraties
- ENSIA helpt gemeenten in één keer verantwoording af te leggen over informatieveiligheid
- Collegeverklaring inclusief 'oordeel' externe auditor bijlage bij Jaarrekening



Hoe kunt u zich weren?

- Herken 'phishing' (voorbeeld journalisten die raadsleden hadden gepakt via Twitter)
- Herken misinformatie en doe aan feitencontrole
- Gebruik uw mobiele en ICT apparatuur veilig



**Hoe gaan we om met
kunstmatige intelligentie
en algoritmes?
En welke ethische
dilemma's zijn er?**

DORDRECHT



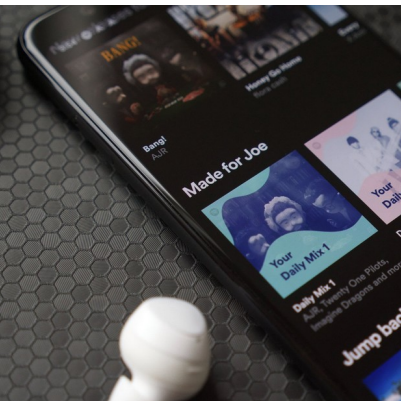
Wat is Kunstmatige Intelligentie?

- Software om taken uit te voeren of problemen op te lossen (**algoritmen**)
 - Bijv. Google/Amazon zoekresultaten, Facebook/LinkedIn berichten op je feed, advertenties die je op alle apps ziet, etc.
- Patronen herkennen en beslissingen ondersteunen en/of nemen(**machine learning**)
 - Bijv. Schaken tegen computers, spam filters, gezichtsherkenning, automatisering, etc.
- **Generatieve AI**; kan teksten, afbeeldingen, audio en andere content genereren (bv. Chat GPT)
- Door meer te oefenen werken ze steeds beter (**trainen**)



Bekende voorbeelden van Kunstmatige Intelligentie (AI)

- **Gepersonaliseerde aanbevelingen**
(bijv. Facebook, Spotify & Google)
- **Virtuele assistenten**
(bijv. Siri, Alexa & Google)
- **Slimme sensoren** van (zelfrijdende) auto's
(bijv. Tesla & Kia)





▲ Tim Hanssen krabde aan zijn oor, maar slimme camera denkt dat hij telefoon vasthoudt.

Tim krabde aan zijn oor en moet nu 380 euro betalen door fout van 'slimme' camera: 'Zie je een telefoon?'

Toen Tim aan zijn oor krabde, had hij niet verwacht daar een boete van 380 euro voor te krijgen. Een slimme camera dacht dat hij een telefoon vasthield op de snelweg, maar dat was toch echt een foutje. „Ik wil de boete aanvechten en denk dit zeker te kunnen winnen.”



▲ Supermarkteigenaar Nawin Harpal bij het scherm waarop alle beelden van 34 camera's in zijn winkel te zien zijn. © Ruud Voest

Supermarktondernemer Nawin heeft dé oplossing tegen winkeldiefstal: 'Ik raad dit iedere winkelier aan'

In de supermarkt van Nawin Harpal worden de laatste tijd opvallend veel winkeldieven betrapt. Hoe dat komt? Een half jaar geleden was het nog maar eens per week dat een winkeldief gepakt werd in de winkel in de Utrechtse binnenstad. Maar dankzij een superslimme oplossing zijn dat nu meerdere dieven per dag. „Ik raad dit iedere winkelier aan.”



Moeten we AI in de klas
verbieden of omarmen?

**Hoe het onderwijs zich voorbereidt op een
toekomst met kunstmatige intelligentie**

14 april 2023, Iza Omlo

→ **Educatie**

Robots voor de klas, een computer die je scriptie schrijft of een systeem dat dyslexie vroeg opspoot: de mogelijkheden op het gebied van AI (artificiële of kunstmatige intelligentie) lijken eindeloos. Hoe bereiden we docenten, studenten en leerlingen voor op een toekomst met AI? "Het vereist een bepaalde manier van denken om het beste uit AI te halen."



Fiscus gebruikte in toeslagenaffaire algoritmes die mensenrechten schenden

Door NU.nl

25 okt 2021 om 22:13

Update: 2 jaar geleden

 123 reacties

 Delen

De algoritmes die de Belastingdienst in de toeslagenaffaire gebruikte, schenden mensenrechten. Die conclusie trekt Amnesty International in een maandag verschenen rapport.



Één voorbeeld van AI en algoritmen in Dordt: Chatbot Gem

Mijn pagina

Contrast

Zoeken



Inwoners

Ondernemers

Bestuur

Onze stad

Contact



PARKEREN CENTRUM



BELASTINGEN



PASPOORT EN
IDENTITEITSKAART

Chat met Dordrecht

Welkom bij de livechat van Dordrecht.

Start gesprek met medewerker

Typ hier je vraag...

Of zoekt u

[Verhuizen](#)

[Afval van huishoudens](#)

[Parkeervergunning](#)

[Afspraak maken](#)

[Melding openbare ruimte](#)

[Uittreksel of afschrift](#)

[Trouwen / Partnerschap](#)

[Paspoort/ID-kaart kinderen](#)



Grote kansen, grote maatschappelijke risico's

- **AI Verordening:** EU werkt aan regelgeving
- **Rijksoverheid:** Commerciële AI's zoals ChatGPT verboden voor rijksambtenaren
- **GPT-NL:** Het Nederlandse taalmodel komt eraan (Overheid, TNO, NFI & SURF)

Forse ethische vraagstukken!

Dit raakt u ook

Ontwikkelingen gaan heel snel



Aantal voorbeelden van wat u kunt doen met AI

- Samenvatten beleidsstukken en agenda's voor raadsvergaderingen
- Vertalen van/naar Nederlands
- Teksten inkorten, herschrijven of controleren op (spel)fouten
- Teksten laten genereren/maken

Samenvatting raadsinformatiebrief (1)



ChatGPT

De raadsinformatiebrief informeert over de eerste resultaten van een onderzoek naar de aanwezigheid van PFAS in eieren van hobbykippen in de omgeving van Chemours. De gemeenten Dordrecht, Sliedrecht, Papendrecht en Molenlanden hebben het onderzoek uitgevoerd om te bepalen of het veilig is om eieren van hobbykippen uit deze omgeving te consumeren. De resultaten tonen aan dat er te hoge gehalten aan verschillende PFAS zijn aangetroffen in de eieren, zowel in gebieden rondom Chemours als in verder gelegen gebieden. Het advies van zowel het RIVM als de GGD is om voorlopig geen eieren van hobbykippen te consumeren, in afwachting van vervolgonderzoek. Eieren van professionele pluimveehouders zijn wel veilig. Het vervolgonderzoek, uitgevoerd door RIVM, Arcadis en WFSR, zal zich richten op het identificeren van de bron van de PFAS en de manier waarop deze in de eieren terechtkomen. Communicatie met betrokkenen, inclusief eigenaren van hobbykippen en media, is ingepland. De kosten van het onderzoek worden betaald uit een bodemsubsidie.

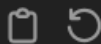


Samenvatting raadsinformatiebrief (2)



ChatGPT

- Een onderzoek door vier gemeenten in de omgeving van Chemours toont te hoge niveaus van verschillende PFAS aan in eieren van hobbykippen.
- Zowel het RIVM als de GGD adviseren om voorlopig geen eieren van hobbykippen te consumeren in afwachting van vervolgonderzoek.
- Eieren van professionele pluimveehouders worden als veilig beschouwd.
- Het vervolgonderzoek zal de bron van de PFAS en hun overdracht naar de eieren identificeren, uitgevoerd door RIVM, Arcadis en WFSR.
- Communicatie met belanghebbenden, waaronder eigenaren van hobbykippen en media, is gepland, en de kosten worden gedekt door een bodemsubsidie.





Wat zijn de risico's?

- Afhankelijkheid van een hulpmiddel waarvan de kwaliteit en feitelijke juistheid van het resultaat niet gegarandeerd wordt en kán worden
- Persoonlijke gegevens en vertrouwelijke informatie kunnen worden gebruikt om de systemen te trainen
 - Dit kan terug komen in de resultaten van andere gebruikers (datalekken)

Hoe maakt u verantwoord gebruik van AI?

- Gezien de nieuwigheid en snelheid van de ontwikkelingen zijn er nog weinig vertrouwde partijen
- Maak altijd een bewuste keuze of het gebruik van toegevoegde waarde is
- Verwerk, gebruik en voer géén persoonsgegevens of vertrouwelijke documenten in (Samsung datalekken)
- Controleer en verifieer altijd het resultaat!



3. Toelichting nieuwe richtlijnen apparaat gebruik

DORDRECHT




Veilig werken met de iPad (1)

- Zakelijk en privé altijd gescheiden houden op mobiele en ICT apparatuur
- Sociale media apps beveiligen
- Veilig mailen met Gmail of Proton
- Gebruik geen Chinese & Russische apps vanwege privacy en beveiligingsissues (bijv. TikTok, WeChat, AliExpress, VKontakte en CapCut).

Veilig werken met de iPad (2)

- Automatisch downloaden van de laatste iOS en apps updates
- Gebruik een wachtwoord of Face/Touch ID
- Automatisch vergrendelen
- Find My iPad
- App rechten beheren
- Verstandig gebruik maken van wifi (gebruik géén publieke wifi netwerken, en alleen eigen hotspots gebruiken)
- Gebruik Safari browser
- Back-ups via de iCloud



Dank u wel!
Zijn er vragen?

DORDRECHT

