AI: gevaar voor onze privacy?

De laatste tijd domineert *Artificial Intelligence* (AI) het nieuws. Denk aan programma's als ChatGPT, kunstgenerator DALL-E of andere AI-systemen die in staat zijn om nieuwe muziek uit te brengen waarbij niet kan worden onderscheiden of de muziek van de artiest zelf afkomstig is of niet. En wat te denken van gezichtsherkennings-software of *voice cloning* via stemimitatiesoftware?
Een van de zorgen over de inzet van AI is dat zich (grove) inbreuken op de privacy kunnen voordoen.Zoals in de Verenigde Staten (VS), bijvoorbeeld, waar de politie al gebruikmaakt van gezichtsherkenningssoftware. Begin dit jaar werd een acht maanden zwangere vrouw in Detroit gearresteerd omdat zij zou zijn "herkend". Ze bracht bijna anderhalve dag in hechtenis door, waarna bleek dat het gezichtsherkenningssysteem een fout had gemaakt. Ook *voice cloning* komt in de VS al veelvuldig voor: via stemimitatiesoftware lichten criminelen mensen op door aan de telefoon de stem van een familielid na te bootsen.
Naar aanleiding van genoemde voorbeelden dringt zich een aantal vragen op vanuit privacyperspectief. Mogen ontwikkelaars die AI-systemen met behulp van (stem)data trainen zomaar gebruikmaken van andermans stem of portret? Mag een organisatie dergelijke vormen van AI zonder meer inzetten bij bijvoorbeeld de opsporing? Voordat die vraag kan worden beantwoord, komt dan eerst de vraag hoe een stem juridisch moet worden gekwalificeerd. In rechtspraak is deze vraag al eens aan de orde geweest. Zo heeft de rechtbank Midden-Nederland op 9 januari 2020 (ECLI:NL:RBMNE:2020:24) geoordeeld dat de stem van een persoon een biometrisch persoonsgegeven is in de zin van artikel 9 van Algemene verordening gegevensbescherming (AVG). Het is daarmee een bijzonder persoonsgegeven waarvoor in principe een verbod op verwerking geldt. Dit verbod geldt behoudens enkele wettelijke uitzonderingen, bijvoorbeeld indien een betrokkene uitdrukkelijke toestemming geeft voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden.
Ook een portret dat gebruikt wordt voor

software volgens de AVG worden aangemerkt als verwerkingsverantwoordelijken voor de persoonsgegevens die zij – meestal in de vorm van trainingsdata – gebruiken. Zij moeten daarbij voldoen aan alle vereisten die voortvloeien uit de AVG. Dat blijkt ook uit het huidige voorstel voor de AI-verordening die nog in de maak is. Daarnaast volgen er nog veel meer verplichtingen die voortvloeien uit de op handen zijnde AI-verordening.
Vervolgens is het de vraag of organisaties gebruik kunnen maken van dergelijke AI-technologie. De besproken praktijkvoorbeelden laten zien dat (onjuist c.q. onethisch) gebruik kan leiden tot fouten en inbreuk op de privacy. Let wel: dit is slechts een van de vele privacyaspecten die hieraan kleven. Gelet op de vele risico's is het de vraag of de voordelen van de inzet van AI uiteindelijk opwegen tegen de nadelen hiervan. Mocht u AI-technologie willen inzetten, bedenk dan dat er eerst een gedegen risico-inventarisatie en privacy impact assessment moet plaatsvinden!

De advocaten en juristen van Elferink & Kortier Advocaten schrijven op deze plek regelmatig een column, waarin zij een praktisch probleem op het gebied van de AVG in relatie tot informatiebeheer behandelen. Heeft u een praktijkvraag die u behandeld wilt zien? Stuur deze naar Od@publiekdenken.nl.

Deel dit artikel

Inhoud