EU privacy and data protection law applied to AI: unveiling the legal problems for individuals

Häuselmann, A.N.

Samenvatting proefschrift 'EU-wetgeving inzake privacy en gegevensbescherming toegepast op AI: een analyse van de juridische problemen voor individuen'

Het is algemeen bekend dat elke baanbrekende technologie risico's en complexe beleidsuitdagingen met zich meebrengt. Dit geldt in het bijzonder voor AI en de fundamentele rechten op privacy en de bescherming van persoonsgegevens. Dit proefschrift analyseert deze uitdagingen en heeft als doel antwoord te geven op de vraag in hoeverre de ontwikkelingen op het gebied van AI een nieuw juridisch kader voor deze fundamentele rechten vereisen.

Hoofdstuk 1 introduceert de context en maatschappelijke relevantie van dit proefschrift, evenals de onderzoeksvraag, de gebruikte methodologie en de reikwijdte van het proefschrift.

Hoofdstuk 2 onderzoekt wat AI is. Allereerst worden de bestaande definities van AI besproken. Vervolgens wordt ingegaan op de AI-disciplines die in de context van fundamentele rechten op privacy en gegevensbescherming het meest problematisch zijn. Deze disciplines zijn onder meer machinaal leren, natuurlijke taalverwerking, computervisie, affectief computergebruik en geautomatiseerd redeneren. *Machinaal leren* (ML) is een belangrijke discipline van AI, en richt zich op computers die zichzelf programmeren op basis van ervaring. ML kan worden toegepast door middel van verschillende methoden, variërend van gesuperviseerd tot niet gesuperviseerd leren, tot versterkend leren. *Diep leren* (DL) is een zeer krachtige vorm van machinaal leren. De resultaten op dit gebied zijn bereikt met *kunstmatige neurale netwerken* (KNN), die, in vergelijking met de neurale netwerken in het menselijk brein, uit een verbazingwekkend klein aantal neuronen bestaan. Door middel van *natuurlijke taalverwerking* (NLP) zijn machines in staat menselijke taal te verwerken. Dit omvat zowel het genereren als het begrijpen van natuurlijke taal. NLP draagt aanzienlijk bij aan het verbeteren van interacties tussen machines en mensen. *Computervisie* (CV) bevordert geautomatiseerd begrip van visuele beelden, waardoor machines in staat zijn om "te zien". Gezichtsherkenning, een van de toepassingen van computervisie, zorgt ervoor dat machines de identiteit van mensen die zichtbaar zijn in afbeeldingen of video's kunnen identificeren of verifiëren op basis van biometrische gegevens. Omdat emoties een belangrijk element van menselijke intelligentie zijn en een grote rol spelen in het dagelijks leven, is *affectief computergebruik* (AC) erop gericht om machines emotionele capaciteiten te geven. AC-methoden waarmee emoties afgeleid worden uit gezichtsuitdrukkingen en spraak, kunnen eenvoudig worden toegepast en op grote schaal worden gebruikt. Werkwijzen op het gebied van *geautomatiseerd redeneren* (GR) zijn gericht op het automatisch uitvoeren van individuele redeneringen.

Hoofdstuk 3 introduceert het huidige EU-rechtskader met betrekking tot de fundamentele rechten op privacy en de bescherming van persoonsgegevens. Ook gaat het hoofdstuk in op relevante secundaire EU-wetgeving. In dit kader worden de Algemene Verordening Gegevensbescherming (AVG), het

belangrijkste secundaire EU-recht op het gebied van gegevensbescherming, en de ePrivacy-richtlijn (ePR) besproken. Bijzondere nadruk wordt gelegd op de beginselen en afdwingbare rechten in de AVG.

De hoofdstukken 4 en 5 gaan in op de juridische problemen die zich voordoen, of kunnen voordoen, wanneer de *beginselen* en *afdwingbare rechten* uit het huidige rechtskader worden toegepast op de in hoofdstuk 2 geïntroduceerde AI-disciplines. Drie categorieën juridische problemen worden besproken: (1) wettelijke bepalingen worden geschonden, (2) wettelijke bepalingen zijn niet handhaafbaar en (3) wettelijke bepalingen zijn ongeschikt om het fundamentele recht in kwestie te beschermen. Deze juridische problemen worden onderzocht vanuit het perspectief van natuurlijke personen (individuen).

Door de tekortkomingen in geautomatiseerd redeneren (GR) zijn AI-systemen niet in staat om de logica van systemen die werken met geautomatiseerde besluitvorming (GB) weer te geven. De redeneringen of criteria die ten grondslag liggen aan een geautomatiseerd besluit, zijn zodoende onduidelijk. AI-systemen die gebruikmaken van DL- en KNN-benaderingen van machinaal leren, produceren waarschijnlijk niet-interpreteerbare resultaten. Wanneer ze worden gebruikt in de context van GB, kunnen de verwerkingsverantwoordelijken geen zinvolle informatie over de logica achter de GB aan de betrokkenen verstrekken. Hierdoor schenden ze het transparantiebeginsel (Type 1).

AI-systemen kunnen persoonsgegevens verwerken op een manier die doorgaans als oneerlijk wordt beschouwd, bijvoorbeeld wanneer door machinaal leren gegenereerde waarschijnlijkheidsvoorspellingen als feiten worden beschouwd. De onduidelijke rol en betekenis van het behoorlijkheidsbeginsel verminderen de rechtszekerheid en maken het moeilijk voor betrokkenen om de eerlijkheid van een verwerking aan te vechten. Het behoorlijkheidsbeginsel is hierdoor lastig handhaafbaar (Type 2).

AI-systemen vergemakkelijken de geautomatiseerde verwerking van nieuwe soorten gevoelige gegevens, zoals emotiegegevens en mentale gegevens. Ondanks hun zeer gevoelige aard worden dergelijke gegevens in de AVG niet specifiek beschermd als bijzondere gegevens. Dit komt doordat ervoor is gekozen om alle bijzondere gegevens uitputtend op te sommen. Aangezien de ontwikkelingen op het gebied van AI niet zijn bij te houden, loopt de wetgever hierdoor achter de feiten aan. Als gevolg ontstaat een hiaat in de bescherming, waardoor de AVG niet geschikt is om het fundamentele recht op bescherming van persoonsgegevens te waarborgen (Type 3).

Machinaal leren, natuurlijke taalverwerking en affectief computergebruik faciliteren toezicht op de communicatie tussen mens en machine. Grote techbedrijven die mens-machine communicatiediensten (zoals virtuele assistenten) aanbieden, kunnen dergelijke communicatie gemakkelijk onderscheppen en op een andere manier verwerken. Met natuurlijke taalverwerking en machinaal leren kan

gevoelige informatie worden afgeleid uit menselijke spraak en andere akoestische elementen in opgenomen audio. Naast de inhoud van spraak, kunnen de stemkarakteristieken en uitdrukkingswijze van een spreker een breed scala aan persoonlijke informatie bevatten. Dit omvat aanwijzingen over de biometrische identiteit, persoonlijkheid, fysieke kenmerken, geografische herkomst, het niveau van dronkenschap/slaperigheid, leeftijd, geslacht, gezondheidstoestand en zelfs de sociaaleconomische status van de spreker. Aanbieders van mens-machine communicatiediensten vallen niet onder het strikte regime van Artikel 5 (1) ePR, dat de vertrouwelijkheid van communicatie regelt. Deze leemte in de wet geeft aan dat de ePR niet geschikt is om de vertrouwelijkheid van mens-machine communicatie te waarborgen (Type 3).

Betrokkenen moeten voldoen aan de objectieve controleerbaarheidsnorm om gegevens te laten rectificeren die gegenereerd zijn door systemen op het gebied van machinaal leren en affectief computergebruik. Persoonsgegevens die worden gegenereerd door middel van machinaal leren kunnen oncontroleerbaar zijn. Gegevens over emoties zijn van nature zeer subjectief. Betrokkenen kunnen hierdoor geen bewijs leveren dat voldoet aan de objectieve controleerbaarheidsnorm. Het recht op rectificatie is dus niet geschikt om het fundamentele recht op bescherming van persoonsgegevens te beschermen, aangezien de norm betrokkenen belemmert in de uitoefening van hun recht (Type 3).

Hoofdstuk 6 heeft als doel om antwoord te geven op de vraag hoe de tekortkomingen van het huidige wettelijke kader die in hoofdstuk 4 en 5 zijn geïdentificeerd, moeten worden aangepakt. Op basis van de selectiecriteria effectiviteit, urgentie en nieuwheid bespreek ik zes juridische problemen: onduidelijkheid, mentale data, communicatiesurveillance, bedrijfsgeheimen, controleerbaarheid en cumulatieproblemen. Hoofdstuk 6 onderzoekt geschikte juridische oplossingen voor deze juridische problemen. Juridische oplossingen zijn (i) nieuwe interpretaties van bestaande bepalingen, (ii) het wijzigen van bestaande bepalingen of (iii) het introduceren van nieuwe bepalingen als antwoord op de betreffende juridische problemen. Wat dit laatste betreft, worden twee specifieke instrumenten onderzocht: weerlegbare aannames en omkering van bewijs.

Hoofdstuk 7 bespreekt de conclusies van dit proefschrift en geeft antwoord op de vraag in hoeverre de ontwikkelingen in AI een nieuw juridisch kader voor de fundamentele rechten vereisen. De mate waarin aanpassingen nodig zijn hangt grotendeels af van (i) het soort juridisch probleem en (ii) de AI-discipline. Dit laatste wordt uitgedrukt door het totaal aantal Type 2 en Type 3 problemen per AI discipline.

Voor juridische problemen van Type 1 volstaat het huidige rechtskader. De oplossing voor deze problemen ligt voor de hand. Schendingen van bepalingen binnen het huidige rechtskader moeten gesanctioneerd worden door betrokkenen en/of vertegenwoordigende organen ("particuliere handhaving") en door toezichthoudende autoriteiten ("regelgevende handhaving"). Het huidige rechtskader

volstaat daarentegen niet voor juridische problemen van Type 2 en 3. Niet-handhaafbare en "ongeschikte" bepalingen zijn simpelweg niet toereikend om privacy en persoonsgegevens te beschermen. Deze twee soorten juridische problemen vereisen *aanpassingen in wetgeving* of nieuwe interpretaties van de huidige bepalingen. In het laatste geval zijn gerechtelijke maatregelen in plaats van wetgevende maatregelen nodig. Neem bijvoorbeeld het probleem onduidelijkheid. De onduidelijke rol en betekenis van het behoorlijkheidsbeginsel vermindert de rechtszekerheid en maakt het moeilijk voor betrokkenen om de eerlijkheid van verwerkingen door AI-systemen aan te vechten en het beginsel af te dwingen (Type 2). Wanneer dit beginsel door het HvJ-EU wordt geïnterpreteerd als zowel procedurele als materiële eerlijkheid, zou het potentiële schade voor betrokkenen als gevolg van de verwerking van persoonsgegevens door AI-systemen voorkomen. In andere gevallen zijn wetgevende maatregelen onvermijdelijk. De wetgever moet bepalingen binnen het huidige rechtskader aanpassen. Dit geldt bijvoorbeeld voor het probleem met communicatiesurveillance. Artikel 5 (1) ePR regelt de vertrouwelijkheid van communicatie, maar sluit mens-machine communicatiediensten gefaciliteerd door AI (bijv. virtuele assistenten) uit van het toepassingsgebied. Hierdoor ontstaat een aanzienlijk hiaat in de bescherming (Type 3). De wetgever zou nieuwe bepalingen in de toekomstige ePrivacy-verordening kunnen opnemen, en specifiek de vertrouwelijkheid van communicatie tussen mens en machine kunnen regelen.