Onderzoeksrapport

Algemene vergadering der MUNESCO 2022

“Het individuele recht op privacy beschermen in het digitale tijdperk.”



MUNESCO

Oostvaarderscollege te Almere

Introductie

In de laatste decennia, hebben grote technologische ontwikkeling ervoor gezorgd dat wij nu in het digitale tijdperk zitten. Dit heeft ervoor gezorgd dat zowel de productiviteit en ontwikkeling van de mens sneller is gegaan dan ooit tevoren. Desalniettemin, hebben deze ontwikkelingen gezorgd voor een tekort aan privacy bij de samenleving.

Definities van de kernbegrippen

Het digitale tijdperk:

> De tijdsperiode die strekt van toen de digitale technologie een doorslag maakte in de wereld, waardoor informatie sneller en makkelijker gedeeld kon worden, tot het heden.

Kunstmatige intelligentie:

> De simulatie van processen van het menselijk brein nagebootst door machines, zoals computers.

Toezicht van de staat:

> Het toezicht houden op dingen zoals activiteiten, om data van mensen te werven en zo de populatie proberen te stimuleren, beïnvloeden of te controleren.

Algemeen overzicht van de informatie

Nu wij dieper in het digitale tijdperk zitten, hebben ontwikkelingen in technologieën zoals kunstmatige intelligentie een digitale omgeving gecreëerd waarin de date van mensen kwetsbaarder is geworden voor het worden getrackt en geanalyseerd worden, door overheden en bedrijven.

Privacy wordt bestempeld als een mensenrecht in artikel 12 van De Universele Verklaring van de Rechten van de Mens, en nog vele andere verklaringen over de hele wereld. Daarom is het belangrijk dat het gebruik van kunstmatige intelligentie dit recht niet schendt, om zo de menselijke waardigheid en identiteit te beschermen.

De toenemende afhankelijkheid op persoonlijke data

Hoewel het digitale tijdperk relatief nieuw is, is de digitale voetprint van veel mensen exponentieel gegroeid, met mensen die bijna op alle technologieën die ze hebben worden getrackt, zonder dat ze dit vaak weten. Hier vallen biometrische gegevens, zoals gezichtsherkenning en vingerafdrukken, ook onder. Deze kunnen door zowel bedrijven als overheden gebruikt worden om toezicht te houden op het volk, en hen te kunnen identificeren. Sommige overheden zijn begonnen met grote projecten die biometrische gegevens omvatten, zonder dat er voldoende werd gedaan om deze data te beschermen.

Het is ook belangrijk dat veel van deze data wordt uitgewisseld tussen bedrijven en overheden. Dit maakt het bijna onmogelijk om te weten wie welke informatie heeft, en wiens informatie dit dan is. Dit zorgt ervoor dat het beschermen van privacy in het digitale tijdperk nog ingewikkelder wordt.

Doordat systemen gebruik maken van kunstmatige intelligentie en er veel data tegelijkertijd geanalyseerd kan worden, beschikken partijen die hierbij betrokken zijn over enorme hoeveelheden analytische kracht. Hierdoor kunnen zij veel data van mensen opslaan, en zo persoonlijke profielen creëren, om zo voorspellingen te doen over de fysieke en mentale eigenschappen van deze mensen. Dit zorgt voor een groot risico voor de maatschappij, omdat datalekken nu heel veel persoonlijke informatie in één keer kan lekken. Dit zou kunnen leiden tot fraude en de onthulling van kwetsbare en persoonlijke informatie.

Eerdere pogingen om dit probleem op te lossen

Pogingen om dit probleem aan te pakken begonnen in 2012, toen de VN de eerste resolutie die dit onderwerp besprak had gemaakt. De mensenrechtenraad van de Verenigde Naties heeft in 2019 een resolutie ingediend die ervoor heeft gezorgd dat mensen dezelfde rechten hebben als ze zich offline, dan wel online bevinden. Deze erkent ook het feit dat nog ontwikkelende technologieën, een grote impact kunnen hebben op mensenrechten en privacy. De resolutie doet een aantal aanbevelingen aangaande de toezicht van de staat en bedrijven.

Mogelijke oplossingen

Als we kijken naar mogelijke oplossingen, is het cruciaal om te kijken naar eerdere pogingen om dit te doen. Al helemaal in dit geval, aangezien veel

oplossingen dezelfde concrete ideeën zullen omvatten. Desalniettemin is het zeer belangrijk om te beseffen dat technologieën zich op een exponentiële wijze zullen blijven ontwikkelen en dat we eigenlijk niet kunnen voorspellen hoe data in de toekomst zal worden verzameld. Toch moeten wij te allen tijde de toekomst proberen te voorzien en zo concrete regels te creëren die concreet aangeven wat wel wordt toegestaan, en wat niet.

Naar: *research report HRC, LmunA 2022*