Tweede Kamer rondetafelgesprek tijdelijke commissie Digitale toekomst 'Wettelijk kader en toezicht'

prof.dr. Ronald Leenes
Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University

Ondanks snelle technologische en sociale ontwikkelingen lijkt het huidige reguleringskader in het licht van gevestigde grondrechten en rechterlijke toetsing vooralsnog toereikend. Wel is ontwikkeling van een toekomstvisie en aanscherping van handhaving van de bestaande kaders noodzakelijk.

De digitale technologieën waarop de tijdelijke commissie ziet hebben de afgelopen jaren kwalitatieve en kwantitatieve sprongen gemaakt. Door veranderingen in de technische aanpak, zoals in gezichtsherkenning, is de kwaliteit van de toepassingen significant verbeterd. Technieken gebaseerd op meting en vastlegging van afstanden tussen gedefinieerde punten in het gezicht (ogen, mond, neus) maken plaats voor deep learning algoritmen die op basis van voorbeelden in staat zijn gezichten van elkaar te onderscheiden om vervolgens gezichten te herkennen of identificeren.[1] Ook zijn in het detecteren van emoties in zowel beeld als spraak is sterke vooruitgang geboekt.

Door de enorme investeringen die wereldwijd in AI – en in het bijzonder in machine learning – plaatsvinden gaan de ontwikkelingen snel en komen toepassingen steeds meer laagdrempelig beschikbaar. Technologieën die een aantal jaren geleden slechts toegankelijk waren voor overheden, zijn dat nu ook voor bedrijven en burgers. Kostenverlaging en het feit dat allerlei diensten en producten gebaseerd op de verwerking van persoonsgegevens gemeengoed worden in de VS, levert ook in Nederland een opwaartse druk op om dergelijke producten en diensten in te zetten. Denk aan gezichtsherkenning dat nu ook door winkels wordt ingezet om bekende of verdachte winkeldieven te herkennen of toegangscontrole in voetbalstadions. Dit zelfde geldt voor technieken zoals automatische nummerplaat herkenning (ANPR). Ook deze technologie was lange tijd voorbehouden aan de overheid, terwijl nu in beginsel iedere – beetje technisch onderlegde – burger in staat is om een ANPR systeem te installeren in eigen straat of op eigen erf.

Naast de verbetering in kwaliteit en daling van kosten, is het verdwijnen van de technologie naar de achtergrond een factor van betekenis. Camera's die geschikt zijn voor gezichtsherkenning hoeven er niet als lompe camera's uit te zien, maar kunnen vrijwel onzichtbaar zijn ingebouwd in reclamezuilen, deurspionnen[2] en brievenbussen. Ook is technologie ontwikkeling op het gebied van het Internet of Things er expliciet op gericht om de interactie zo frictieloos mogelijk te maken. Geen veelheid aan knoppen en handleidingen, maar apparaten die eenmalig via een smartphone worden gekoppeld aan de achterliggende dienst en vervolgens reageren op spraak. Wie of wat er achter geavanceerde diensten en producten zitten wordt steeds intransparanter en de mogelijkheden voor de gebruiker om invloed uit te oefenen over wat er met haar

[1] Zie bijvoorbeeld E. Keymolen et al. Op het eerste gezicht, Den Haag, WODC, 2020.

[2] Zie bijvoorbeeld M. Galič, et al, 'Het gebruik van drones en spionageproducten door burgers: een verkenning van de privacyrisico's en reguleringsmogelijkheden', Den Haag, WODC, 2020.

persoonsgegevens (die bovendien veelal afgeleid worden uit gedrag in plaats van bewuste verstrekking) neemt af.

Het lijkt er op dat naast toenemende mogelijkheden voor de overheid om langs de verticale as inbreuk te maken op de privacy van burgers, dit ook op de horizontale as het geval is; burgers en bedrijven krijgen meer mogelijkheden om elkaar te monitoren, bespioneren en beïnvloeden.[3]

Een ontwikkeling die niet als zodanig wordt genoemd in de convocatie, maar die wel duidelijk verweven is met bovenstaande, is dat veel van de digitale ontwikkelingen worden aangedreven door de grote Amerikaanse (en in de nabije toekomst wellicht ook Chinese) technologiereuzen (Google, Facebook, Amazon, Microsoft, Apple). De thuisbasis van deze bedrijven is de VS met een totaal andere privacy cultuur dan de onze en een vrijwel ontbreken van regelgeving rond de verwerking van persoonsgegevens. Amerikaans partijen zullen zich wat betreft de Europese markt moeten schikken naar het Europese regelgevingskader, maar dat neemt niet weg dat hun bedrijfsmodellen zijn gebaseerd op de grootschalige verwerking van gegevens en dat ze een sterke, zo niet dominante positie hebben in de data economie.

Betekent dit alles dat wet- en regelgeving aanpassing behoeft?
In het algemeen zou ik deze vraag met nee beantwoorden.

De relatief recent in werking getreden Avg, opvolger van de meer dan 15 jaar oude Wbp die als centraal kader heeft gegolden voor gegevensverwerking in de informatiemaatschappij, bestrijkt een groot deel van nieuwe digitale toepassingen. Vrijwel alle digitale technologieën draaien op de verwerking van persoonsgegevens, zeker nu de grenzen van het begrip persoonsgegeven alsmaar worden opgerekt. Dit betekent dat het geactualiseerde gegevensverwerkingsregime (Avg, Wet Politiegegevens, op termijn de ePrivacy Regulation die de e-Privacy richtlijn zal vervangen) het centrale kader is. Gezichtsherkenning, geautomatiseerde besluitvorming op basis van AI (Machine Learning), Internet of Things, etc, allen vallen onder deze kaders en toepassing van die kaders levert geen grote verassingen op.

Wel valt op te merken dat de Avg vooral is ingestoken op de bescherming van rechten en vrijheden van het individu. Risico's van gegevensverwerking op groepsniveau en voor de maatschappij als geheel komen veel minder aan bod.[4] In een tijdperk waarin Big Data beslissingen en beleid voedt op basis van profielen en patronen worden belangen van groepen geraakt en verdienen die extra aandacht.

Naast het specieke gegevensbeschermingsregime moet niet vergeten worden dat we daarenboven de algemene grondrechten hebben, onder meer verankerd in onder meer het Europees Verdrag van de Rechten van de Mens (EVRM) en het Handvest van de Grondrechten

---

3 Zie het WODC onderzoek "Onderlinge privacy bescherming in het buitenland", 2020.

4 Zie hierover uitgebreid L. Taylor, L. Floridi and B. van der Sloot (eds), Group Privacy – New Challenges of Data Technologies, Springer, 2017.

van de Europese Unie, zoals het recht op privacy, het recht op gegevensbescherming en het discriminatieverbod. De invloed hiervan hebben we op 5 februari 2020 kunnen zien in de SyRI uitspraak van de Haagse rechtbank.

Het mededingingsrecht, vooral op Europees niveau zal een centrale positie moeten hebben in het kanaliseren van het gedrag van dominantie partijen in de data gedreven economie. We zien relatief voorzichtige eerste stappen in de toepassing van dit instrumentarium. Het gaat hier om toepassing van het mededingingsrecht op nieuwe vraagstukken, maar het instrumentarium op zich lijkt daarop toegerust. Gegevensbescherming en mededinging ontwikkelen zich hiermee als (de) twee centrale pijlers in de regulering van de data economie.

De algemene normen, gebaseerd op tamelijk algemeen erkende beginselen, zijn onverminderd relevant en van toepassing op huidige en voorzienbare digitale technologieën.

Functioneren de kaders zoals beoogd? Het antwoord op die vraag ligt genuanceerder.

In de eerste plaats lijkt het alsof de bestaande kaders niet voor iedereen even duidelijk zijn. De Avg biedt weliswaar normen waarbinnen de verwerking van persoonsgegevens plaats moet vinden en de vraag of een toepassing zoals gezichtsherkenning in een concreet geval binnen die kaders past lijkt doorgaans te beantwoorden (concreet: in veel gevallen zal toepassing van gezichtsherkenning niet mogen), maar die conclusie volgt niet voor iedereen klinkklaar uit de Avg, en zeker niet voor technologie-ontwikkelaars (denk aan start-ups) en het MKB waar juridische kennis relatief schaars is. Concretisering in de vorm van **handvatten** is een noodzakelijke manier om de kaders duidelijk te maken, zeker rond thema's zoals geautomatiseerde besluitvorming, uitleg van AI systemen, profiling en de betekenis van de Avg in concrete toepassingen zoals gezichtsherkenning en IoT.

Een tweede aspect dat aandacht behoeft is **handhaving**. De Wbp ontbeerde tanden om misstanden effectief aan te pakken. In het algemeen kan worden gesteld dat de compliance met de Wbp niet bijzonder groot was.[5] Gegeven de impact die sommige van de gememoreerde toepassingen (bijv. gezichtsherkenning) hebben op rechten en vrijheden van burgers, lijkt serieuze aandacht voor, en verscherping van, de handhaving noodzakelijk om de Avg een kans te geven om de geformuleerde wetgevingsdoelen te realiseren. Alhoewel hier de laatste jaren in is geïnvesteerd, valt er tegelijkertijd nog een wereld te winnen. Terwijl nieuwe technologische toepassingen vaak grote maatschappelijke gevolgen teweeg brengen is het huidige procesrecht en daarmee de mogelijkheid voor burgers om rechtsprincipes af te dwingen nog veelal gestoeld op de bescherming van individuele belangen.[6]

---

5 Dat verklaart ten dele waarom de Avg als *nieuw* werd onthaald.

6 B. van der Sloot & S. van Schendel, 'De Modernisering van het Nederlands Procesrecht in het licht van Big Data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving', WODC 2019.

Het derde, en misschien wel meest fundamentele punt is dat het nog **ontbreekt** aan **een duidelijke visie en positie**. Alvorens ten gronde te kunnen vaststellen of een wettelijk kader toereikend is en of dat al dan niet zou moeten worden aangepast, moet de vraag "in wat voor maatschappelijk willen wij eigenlijk leven?" worden beantwoord. Het antwoord op die vraag geeft niet alleen richting aan de voorliggende vraag of het kader sluitend is of niet maar is ook nodig om het maken van doordachte keuzes op de agenda te zetten.

Daarbij is het van belang dat Europa, in tegenstelling tot sommige andere werelddelen, een lange geschiedenis van rechtsbescherming kent. Dat betekent dat sommige ontwikkelingen worden ingekaderd en andere technieken en toepassingen simpelweg niet zijn toegestaan. Dat is geen kwestie van techniekscepsis of -angst, maar van realisme, geen kwestie van onbekend maakt onbemind, maar juist van een zeer goed begrip van technologieën en welke impact die op de samenleving en de rechtstaat kunnen hebben. Te vaak vervallen discussies in extreme posities en te vaak blijft het hangen in anekdotiek en de waan van de dag.

Het is duidelijk dat dat we naar een data-gedreven wereld toegaan, een wereld die er fundamenteel anders zal uitzien dan de onze. Maar hoe die samenleving er uit komt te zien, welke technieken daar een rol spelen en op welke wijze ze kunnen en mogen worden toegepast, daarop kunnen we wel degelijk invloed uitoefenen. We willen natuurlijk niet achterblijven in de technologische ontwikkelingen en zullen daarom veel technieken proactief moeten inzetten en ontwikkelen, maar we willen ook niet naar een Chinese samenleving, waarin burgers constant en overal in de gaten wordt gehouden, niet alleen door Grote Broer, maar door miljoenen kleine broertjes en zusjes.

Eén van die keuzemogelijkheden is het al dan niet tijdelijk verbieden van een technologische toepassing. Een pleidooi om dat te doen voor gezichtsherkenning wordt bijvoorbeeld gehouden in wetenschap[7] en beleid[8]. Technologie is niet neutraal en er zijn toepassingen die zo sterk inbreuk maken op rechten en vrijheden dat ze moeten worden verboden. Zitten we niet op een niet te stoppen rijdende trein en heeft een dergelijk verbod of moratorium wel zin? Het recente verbod op knalvuurwerk laat zien dat het wel degelijk mogelijk is om radicale koerswijzingen door te voeren op terreinen waar gebruiken onwrikbaar lijken. Zo'n discussie moet ook ten aanzien van digitale technieken plaatsvinden. Welke technieken willen we wel in de samenleving van de toekomst en welke gewoon niet.

Sapere aude, agere aude.

Tilburg, 10 februari 2020

---

7 Zie o.m. Woodrow Hartzog, The Inconsentability of Facial Surveillance," 65 Loyola Law Review 2019

8 https://www.theguardian.com/technology/2020/jan/17/eu-eyes-temporary-ban-on-facial-recognition-in-public-places