Gegevensbescherming, AI systemen en de digitale welvaartsstaat

Marvin van Bekkum

Inleiding

De Nederlandse overheid gaat steeds meer richting een digitale welvaartsstaat. De overheid zet AI in ter bestrijding van fraude of het goedkeuren van aanvragen. Dat heeft zowel voordelen als nadelen. Vanuit mensenrechtenperspectief heeft de burger recht op transparantie over de wijze waarop zij wordt geprofileerd. In de praktijk kunnen burgers niet altijd hun rechten uitoefenen. Denk aan de kindertoeslagenaffaire, die door een parlementaire onderzoekscommissie werd bestempeld als een falen van de trias politica.

De inzet van complexere algoritmen gaat hand in hand met het combineren en uitwisselen van bestaande datasets tussen bestuursorganen. In de zaak Systeem Risico Indicatie (SyRI) uit 2020 komt deze problematiek helder naar voren. In deze pitch bespreek ik de inzet van AI systemen in het licht van de zaak SyRI, de AVG en de nieuwe *AI Act*. Tijdens deze pitch behandel ik de vraag:

> Kunnen de AVG en AI Act burgers beschermen tegen de negatieve effecten van AI systemen, en wat is de rol van transparantie bij die bescherming?

Ik zal deze bijdragen baseren op eigen werk:

M. van Bekkum & F.Z. Borgesius, 'Digital welfare fraud detection and the Dutch *SyRI* judgment', *European Journal of Social Security* 2021/23, afl. 4, p. 323-340, https://journals.sagepub.com/doi/10.1177/13882627211031257, doi:10.1177/13882627211031257.

M. van Bekkum & F. Zuiderveen Borgesius, 'Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?', *Computer Law & Security Review* 2023/48, p. 105770, https://linkinghub.elsevier.com/retrieve/pii/S0267364922001133, doi:10.1016/j.clsr.2022.105770.

M. van Bekkum, *Using sensitive data to debias AI systems: Article 10(5) of the EU AI Act (preprint)*, 2024, https://arxiv.org/abs/2410.14501.

De SyRI-rechtszaak

In 2003 begonnen verschillende bestuursorganen met het uitwisselen van data om fraude te voorkomen. Dit systeem, de 'black box', was een voorouder van SyRI. Later is het systeem onder de naam Systeem Risico Indicatie in de Nederlandse wet verankerd. De feitelijke werking van SyRI was onbekend. Bekend was slechts dat samenwerkingsverbanden onderling data uitwisselden met een door het Ministerie opgerichte stichting genaamd het *inlichtingenbureau* en het Ministerie van Binnenlandse Zaken zelf. Deze datauitwisseling leidde tot lijsten met risico-gevallen geproduceerd door een (voor de burger) onbekend AI-systeem, en verder onderzoek door het Ministerie van die gevallen die het systeem als een *hit* beschouwde. De landsadvocaat hield de werking van het algoritme, informatie over de gebruikte data, en de risico-indicatoren voor de rechter geheim: de overheid was bang dat potentiële fraudeurs met deze informatie de dans konden ontspringen. De Nederlandse rechter oordeelde op basis van artikel 8 EVRM dat meer transparantie noodzakelijk was: zonder informatie over het algoritme zouden burgers niet weten of zij onderzocht worden voor fraude. Eventuele andere mensenrechteninbreuken, zoals het risico op discriminatie kon de Nederlandse rechter niet beoordelen: daarvoor was de overheid namelijk niet transparant genoeg over de eigenschappen van het systeem.

Uit de SyRI-zaak is duidelijk geworden dat de overheid enige transparantie over het gebruikte AI moet geven. Het enkel uitwisselen van gegevens is niet per definitie verboden. Het kabinet kwam zeer kort na de SyRI-zaak met een nieuw wetsvoorstel, het wetsvoorstel Gegevensverwerking Samenwerkingsverbanden. Privacy-activisten noemden dit wetsvoorstel ook wel *Super SyRI*. Enkele juristen spraken ook wel van ' oude wijn in nieuwe zakken'. Het wetvoorstel regelde het in abstracto uitwisselen van gegevens door samenwerkingsverbanden, zonder daarbij een specifiek systeem of doel aan te wijzen. Het wetsvoorstel is aangenomen door de tweedekamer. Omdat het wetsvoorstel geen specifieke gevallen regelt, lijkt het te voldoen aan de rechtsregel uit de SyRI-zaak.

Lessen uit de SyRI-zaak

Uit de SyRI-zaak wordt duidelijk dat de overheid transparant moet zijn richting de burger over het gebruik van AI-toepassingen. Door het geheim houden van AI-systemen is de overheid meer dan alleen ondoorzichtig: de burger kan andere rechten namelijk niet uitoefenen als de burger niet weet wat er achter de schermen gebeurt. De rechten die voorvloeien uit de AVG zijn dan ook minder nuttig zonder een transparante overheid.

Bij AI denkt men vaak aan machine learning-modellen, echter vallen ook beslisbomen onder het begrip. De overheid moet bij het combineren van datasets niet alleen nadenken over *wat* voor algoritme de overheid inzet, maar ook of het daadwerkelijk nodig is om de data te combineren en verder te analyseren. Zelfs de trias politica is niet bestand tegen een intransparante overheid.

De AVG

De AVG is van toepassing op elke verwerking van persoonsgegevens, ook die door AI. Door middel van gegevensbeschermingsbeginselen beschermt de AVG op een technologieneutrale manier de gegevens van burgers.

Met name heb beginselen van dataminimalisatie en doelbinding zijn belangrijk in het big data-tijdperk. Het combineren van en analyseren van grote datasets is noodzakelijk voor het trainen van AI systemen. Veel data-analisten richten zich echter ook op het bouwen van een 'minimaal' model: een model waarbij overbodige correlaties in de data niet worden gebruikt. Ook bestaan er technieken zoals 'power analysis', waarbij een data-analist kan beoordelen of met minder data het doel ook kan worden bereikt. De beginselen uit de AVG reguleren zo ook het gebruik van grote datasets met behulp van AI.

De AVG is risico-gebaseerd: Op basis van een contextgebonden beoordeling worden risico's voor de fundamentele rechten van het data subject gezocht, en steeds zijn passende maatregelen noodzakelijk. De AVG vereist die contextgevoelige beoordeling ook tijdens de ontwikkeling van het AI-systeem. In de praktijk werkt dit 'data protection by design' niet altijd: veel bedrijven doen aan zelfregulering.

De AI-verordening

De EU-wetgever heeft met de AI Act gekozen voor een andere weg dan zelfregulering. De AI Act onderscheidt verschillende risicoklassen. Voor elke klasse gelden specifieke productveiligheidsregels. Met Artikel 10 AI Act schrijft de wetgever datakwaliteitseisen voor die gelden voor het gebruik van Hoog Risico AI-systemen. Daarover heb ik een preprint van een artikel gepubliceerd (zie derde bron). De potentie van Artikel 10 is het gebruik van 'schonere' datasets, die minder vooringenomen zijn ten opzichte van bepaalde groepen. Of dat in de praktijk gaat werken, is nog maar de vraag: voor het verwijderen van bias in data zijn bijzondere persoonsgegevens nodig, en het verzamelen daarvan

brengt allerlei problemen. Nederlandse burgers met name lijkt zich ongemakkelijk te voelen bij het verzamelen van hun etniciteitsgegevens.

Of de AI Act van toepassing is op een bepaald AI-systeem, is niet altijd duidelijk. Artikel 3 AI Act bevat een complexe definitie, waar het onderscheid tussen regelgebaseerde systemen en complexere AI systemen soms vaag kan zijn. Kern van de definitie is het woord 'infer': leidt het systeem output af uit data? Het in nog onduidelijk wanneer daar wel of niet sprake van is. Ook is het de vraag of ook de losse *componenten* van systemen, of slechts het systeem dat een beslissing neemt, onder de definities van 'hoog risico' van de AI Act vallen.

Conclusie

Ik sluit deze korte pitch af met een kort overzicht. De zaak SyRI heeft ons geleerd dat burgers hun rechten niet kunnen uitoefenen zonder voldoende transparantie: als de specifieke techniek van een systeem, risico-indicatoren en de type data die achter de schermen gebruikt worden allemaal geheim zijn, dan kan een burger zijn rechten uit de AVG of de AI Act niet uitoefenen. Transparantie lijkt mij dus een praktische noodzaak voor democratische controle.

De AVG en AI Act leggen regels aan de overheid voor zowel het gebruik van gegevens als het gebruik van AI systemen. Daarmee is veel afgedekt: de regels zijn er. Dat die regels er zijn, betekent echter nog niet dat ze ook worden opgevolgd. De rechtspraktijk zal dat hopelijk verduidelijken.