Komt een fraude-opsporingssysteem bij de rechter

Çapkurt, F.; Schuurmans, Y.E.; Verboeket, L.W.; Brink, J.E. van den; Drahmann, A.; Jacobs, M.J.; Ortlep, R.

F. Çapkurt & Y.E. Schuurmans[1]

37 | Komt een fraude-opsporingssysteem bij de rechter

Rechtbank Den Haag
5 februari 2020, C-09-550982-HA ZA 18-388
(Mr. M.C. Ritsema van Eck-van Drempt, mr. J.S. Honée en mr. H.J. van Harten)
ECLI:NL:RBDHA:2020:865

Essentie

Nieuwe technologieën — waaronder digitale mogelijkheden om bestanden te koppelen en met behulp van algoritmen data te analyseren — bieden de overheid (meer) mogelijkheden om onderling gegevens uit te wisselen in het kader van hun wettelijke taak om fraude te voorkomen en te bestrijden. De rechtbank deelt het standpunt van de Staat dat die nieuwe technologische mogelijkheden ter voorkoming en bestrijding van fraude moeten worden benut. Zij is van oordeel dat de SyRI-wetgeving in het belang van het economisch welzijn is en daarmee een legitiem doel dient. Een adequate controle op de juistheid en de volledigheid van gegevens op basis waarvan aan burgers aanspraken worden verleend is immers van groot belang.

De ontwikkeling van nieuwe technologieën betekent echter óók dat in toenemende mate betekenis toekomt aan het recht op bescherming van persoonsgegevens. Het bestaan van adequate wettelijke privacybescherming bij de uitwisseling van persoonsgegevens door (overheids)instanties draagt bij aan het vertrouwen van de burger in de overheid, net zo zeer als het voorkomen en bestrijden van fraude dat doet. Zoals NJCM c.s. terecht stelt, is het aannemelijk dat bij het ontbreken van voldoende en transparante bescherming van het recht op respect voor het privéleven een 'chilling effect' optreedt. Zonder vertrouwen in voldoende privacybescherming zullen burgers minder snel gegevens willen verstrekken of zal daarvoor minder draagvlak bestaan.

Het transparantiebeginsel is het leidende hoofdbeginsel van gegevensbescherming dat ten grondslag ligt aan en is vastgelegd in het Handvest en de AVG (zie over de beginselen van gegevensbescherming hiervoor 6.27- 6.34). Dit beginsel is naar het oordeel van de rechtbank in de SyRI-wetgeving in het licht van artikel 8 lid 2 EVRM onvoldoende in acht genomen. De rechtbank stelt vast dat de SyRI-wetgeving op geen enkele manier voorziet in informatie over de feitelijke gegevens die de aanwezigheid van een bepaalde omstandigheid aannemelijk kunnen maken, oftewel welke ob-

---

[1] Fatma Çapkurt en Ymre Schuurmans zijn allebei verbonden aan de afdeling Staats- en bestuursrecht van de Universiteit Leiden. Fatma Çapkurt verricht promotieonderzoek naar de doorwerking van het Europees gegevensbeschermingsrecht naar het Nederlands bestuursrecht. Ymre Schuurmans is aan de afdeling verbonden als hoogleraar Staats- en bestuursrecht.

jectieve feitelijke gegevens gerechtvaardigd tot de conclusie kunnen leiden dat sprake is van een verhoogd risico.

Annotatie

1. Inleiding

Het afgelopen jaar sleepte een coalitie van burgerrechtenorganisaties een fraudeopsporingssysteem voor de rechter. Inzet van het geding was om de wetgeving die het Systeem Risico Indicatie (SyRI) van een wettelijke grondslag voorzag - de Wet SUWI en het Besluit SUWI (SyRI-wetgeving) - onverbindend te verklaren wegens strijd met hoger recht. De wetgever had dit systeem onder grote politieke druk in het leven geroepen om effectieve fraudebestrijding mogelijk te maken. Om dat doel te bereiken, koppelde en analyseerde dit systeem grote hoeveelheden persoonsgegevens die bestuursorganen voor andere doeleinden in bezit hadden. Uit data-analyse moest vervolgens blijken of een burger een verhoogd frauderisico zou vormen. Degene die uit deze analyse als potentiële fraudeur rolde, werd vervolgens gedurende twee jaar opgenomen in het Register Risicomeldingen. Van deze registratie werd een burger niet op de hoogte gebracht want dat zou een 'onevenredige inspanning' vergen van de overheid.[2]

Vrijwel alle cruciale elementen van SyRI waren geheim. Welke persoonsgegevens verwerkt het systeem? Op basis van welke indicatoren kan worden vastgesteld dat iemand een verhoogd frauderisico vormt? Welke exacte risicomodellen hanteert het systeem? Ondanks de grootschalige én ondoorzichtige wijze van persoonsgegevensverwerking werd de SyRI-wetgeving in 2013 geruisloos afgedaan als hamerstuk: zij werd door de wetgever als weinig controversieel gezien. Dit veranderde toen de coalitie jaren later de Staat over dit systeem dagvaardde. In een naar het Engelse vertaalde uitspraak die *viral* is gegaan[3] heeft de rechtbank Den Haag de SyRI-wetgeving onverbindend verklaard wegens strijd met artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM).[4] De wetgeving eerbiedigt volgens haar de persoonlijke levenssfeer van burgers

---

[2] *Kamerstukken II* 2012/13, 33 579, nr. 3, p. 23.

[3] Zie bijvoorbeeld: C. Metz & A. Satariano, *An Algorithm That Grants Freedom, or Takes It Away,* New York Times 7 februari 2020 en J. Henley & R. Booth, *Welfare surveillance system violates human rights, Dutch court rules,* The Guardian 5 februari 2020.

[4] Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, r.o. 6.5 (*SyRI*) *O&A* 2020/28, m.nt. T. Barkhuysen, N. Jak & S.R.P. Bastiaans; *NJ* 2020/386, m.nt. E.J. Dommering; *Computerrecht* 2020/87, m.nt. S. van Schendel; *AB* 2020/236, m.nt. H.B. van Kolfschooten; *TRA* 2020/49, m.nt. W.L. Roozendaal en *JB* 2020/63, m.nt. R.H.T. Jansen & M.D. Reijneveld.

onvoldoende, omdat zij geenszins transparant is over het risicomodel, de indicatoren en de analyseermethode die aan SyRI ten grondslag lagen.[5]

In deze annotatie analyseren wij de motivering en impact van deze uitspraak. Daarin staan wij in het bijzonder stil bij de wijze waarop de rechtbank het transparantiebeginsel uit de Algemene verordening gegevensbescherming (AVG) inleest in het tweede lid van artikel 8 EVRM. Hiervoor bestaan drie redenen. In de eerste plaats is de behandeling van het transparantiebeginsel vanuit het perspectief van rechtsontwikkeling een van de meest vernieuwende elementen van de *SyRI*-uitspraak. Bij de toetsing aan artikel 8 EVRM beoordeelt de rechter de noodzakelijkheid van de inbreuk doorgaans aan de hand van maatstaven die zijn neergelegd in het tweede lid van dit artikel: is de inbreuk evenredig en subsidiair in relatie tot het beoogde doel? Rechters doen echter zelden een direct beroep op het Unierecht, om deze toetsing handen en voeten te geven.[6] In de *SyRI*-uitspraak doet de rechtbank daarentegen een expliciet beroep op het Unierecht om de toetsing aan artikel 8 EVRM te operationaliseren. Dit geldt in het bijzonder voor het transparantiebeginsel dat in artikel 5 AVG is neergelegd.

In de tweede plaats verstevigt deze uitspraak de positie van het gegevensbeschermingsrechtelijke transparantiebeginsel dat door de voortschrijdende digitalisering aan belang wint. Nu is het transparantiebeginsel als zodanig allerminst een nieuw beginsel.[7] Zo heeft Prechal al jaren geleden gesignaleerd dat dit beginsel de neiging heeft om op de meest uiteenlopende deelterreinen van het Europees recht op te duiken.[8] Op nationaal niveau heeft dit beginsel onder invloed van het Unierecht een belangrijke positie ingenomen in het financieel bestuursrecht. Dat geldt in het bijzonder voor het aanbestedingsrecht en voor de verdeling van schaarse rechten.[9] Het gegevensbeschermingsrechtelijke transparantiebeginsel daarentegen - dat al ruim een kwart eeuw is gecodificeerd in het Unierecht – is echter opmerkelijk onderbelicht gebleven. Dat transparantiebeginsel vergt dat voor natuurlijke personen transparant dient te zijn welke hen betreffende persoonsgegevens worden verzameld, gebruikt, geraadpleegd

---

[5] Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, r.o. 6.87 (*SyRI*).

[6] L.F.M. Verhey & M.W. Raijmakers, 'Artikel 8 EVRM: proportionaliteit en verwerking van persoonsgegevens', *Regelmaat* 2013(28) 3, p. 189-190.

[7] A.W.G.J. Buijze, *The Principle of Transparency in EU Law* (diss. Utrecht), Utrecht: Utrecht University 2013.

[8] S. Prechal, 'De emancipatie van het algemene transparantiebeginsel', *SEW* 2008/9, p. 316.

[9] A.W.G.J. Buijze, 'Het transparantiebeginsel naar Nederlands recht: een visie geïnspireerd op het EU-recht', *JBplus* 2016(4), A. Drahmann, *Transparante en eerlijke verdeling van schaarse besluiten: een onderzoek naar de toegevoegde waarde van een transparantieverplichting bij de verdeling van schaarse besluiten in het Nederlandse bestuursrecht* (diss. Leiden), Deventer: Kluwer 2015 en Conclusie van A-G Widdershoven 25 mei 2016, ECLI:NL:RVS:2016:1421, punt 6.13 e.v.

of anderszins verwerkt, opdat zij hun informatierechten kunnen uitoefenen.[10] Deze dimensie van het transparantiebeginsel vindt haar grondslag in menselijke waardigheid, die vergt dat mensen kennis moeten hebben van hen betreffende persoonsgegevens om autonome keuzes te kunnen maken, bijvoorbeeld om voor hun belangen bij bestuur of rechter op te kunnen komen.[11] De *SyRI*-uitspraak geeft aan de ontwikkeling van het gegevensbeschermingsrechtelijke transparantiebeginsel een belangrijke stimulans.

Tot slot menen wij dat het thema van deze annotatie goed past in een afscheidsbundel voor Willemien den Ouden. Fraudeopsporing en risicoanalyse zijn bij uitstek in het financieel bestuursrecht tot ontwikkeling gekomen. Als lid van de Adviescommissie uitvoering toeslagen (commissie Donner), die onderzoek heeft verricht naar de kinderopvangtoeslagenaffaire, heeft ze van dichtbij de grote impact van risicoprofilering ervaren.[12] Bovendien valt de invalshoek van het transparantiebeginsel binnen haar bijzondere interesse voor de doorwerking van Europese rechtsbeginselen in het Nederlandse bestuursrecht.

De opbouw van deze annotatie is als volgt. Eerst lichten wij de politieke totstandkomingsgeschiedenis van de SyRI-wetgeving toe, waaronder de beperkte mate van aandacht voor de gegevensbeschermingsrechtelijke impact van SyRI (paragraaf 2). Daarna zetten wij uiteen hoe de rechtbank de SyRI-wetgeving toetst aan artikel 8 lid 2 EVRM en het gegevensbeschermingsrechtelijke transparantiebeginsel (paragaaf 3). Vervolgens analyseren wij hoe zij de toetsing aan het EVRM inkleurt aan de hand van het Unierechtelijk gegevensbeschermingsrecht en wat de toegevoegde waarde hiervan is (paragraaf 4). Hierna bespreken wij hoe de *SyRI*-uitspraak kan worden vertaald naar een kader voor de normering van risicosystemen in het bestuursrechtelijk domein (paragraaf 5). Daarop doordenken wij de bredere implicaties van het gegevensbeschermingsrechtelijke transparantiebeginsel voor het bestuursrechtelijke bewijsrecht (paragraaf 6). Teneinde de bevindingen in context te plaatsen vergelijken we SyRI met een ander, buitenwettelijk, risicosysteem dat in de nasleep van de kinderopvangtoeslagenaffaire het nieuws heeft gehaald: de Fraude Signalering Voorziening (paragraaf 7). Wij sluiten af met een slotbeschouwing (paragraaf 8).

---

[10] Zie overweging (39) van de considerans van de AVG.

[11] Buijze 2013, p. 255-259.

[12] Adviescommissie uitvoering toeslagen, *Omzien in verwondering 2*, eindadvies van 12 maart 2020 en Adviescommissie uitvoering toeslagen, *Omzien in verwondering,* interim-advies van 14 november 2019.

2. Transparantie in de SyRI-wetgeving: de politieke voorgeschiedenis

Voor het uitvoeren van wetgeving zijn persoonsgegevens onmisbaar: zonder deze gegevens kunnen bestuursorgaan geen besluiten nemen. Tegelijkertijd vormt de verwerking van persoonsgegevens een potentiële bedreiging voor de persoonlijke levenssfeer van burgers. Daarom moet de wetgever het vervaardigen van wetgeving nagaan of deze de toets van artikel 8 EVRM kan doorstaan.[13] Ook de ontwerpwetgeving die SyRI van een wettelijke grondslag voorzag, werd onderworpen aan een dergelijke toets.

Al in de ontwerpfase had de Afdeling advisering van de Raad van State (de Afdeling advisering) fundamentele bezwaren tegen dit wetsontwerp. Het eerste betrof de omvang van de gegevensverwerking. De wettelijke grondslag om persoonsgegevens te verzamelen en koppelen was volgens de Afdeling advisering zo ruim, dat er nagenoeg geen gegevens te bedenken waren die niet voor verwerking in aanmerking kwamen.[14] Dit leverde volgens haar spanningen op met het dataminimalisatiebeginsel, dat vereist dat niet meer gegevens worden verwerkt dan nodig is om het beoogde doel te bereiken. Het tweede bezwaar zag op de risicomodellen en indicatoren die door de Minister van Sociale Zaken en Werkgelegenheid (de Minister) werden vervaardigd. De Afdeling advisering benadrukte dat deze voorafgaand aan de verwerking transparant zouden moeten zijn. Anders kan een verwerking mogelijk leiden tot een '*fishing expedition*'. Om dat te voorkomen, zou het '*select before you collect*' principe moeten worden toegepast bij het opstellen van risicomodellen. De gegevens zouden volgens dit principe vooraf, op basis van objectieve indicatoren moeten worden geselecteerd. De toenmalige toezichthouder, het College Bescherming Persoonsgegevens (CBP), liet zich in zijn advies eveneens kritisch uit. Zijn bezwaren kwamen grotendeels overeen met die van de Afdeling advisering. Het zette vraagtekens bij de proportionaliteit van de gegevensverwerking en adviseerde de Minister om de SYRI-wetgeving niet in te dienen.[15]

Terwijl de Afdeling advisering en het CBP voornamelijk oog hadden voor het privacy-bedreigende karakter van de SyRI-wetgeving, maakte het parlement zich vooral zorgen om de staatskas: zouden de kosten van de wet hoger of lager

---

[13] Ook moet de verwerkingsverantwoordelijke op grond van artikel 35 AVG een beoordeling maken van de effecten van een grootschalige gegevensverwerking, in het bijzonder wanneer nieuwe technologieën worden toegepast (een zogenaamde *privacy impact assessment*).

[14] Afdeling advisering van de Raad van State, *Ontwerpbesluit houdende regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens (Besluit SyRI), met nota van toelichting, Stcrt.* 2014, nr. 26306.

[15] College Bescherming Persoonsgegevens, *Advies conceptbesluit SyRI,* Den Haag, 18 februari 2014.

uitvallen dan de boeteopbrengst?[16] De fundamentele bezwaren van de Afdeling advisering en het CBP pareerde de toenmalig Minister van Sociale Zaken, Lodewijk Asscher, met het argument dat de SyRI-wetgeving wel degelijk voldoende gegevensbeschermingsrechtelijke waarborgen bevatte omdat zij de te koppelen persoonsgegevens limitatief opsomde en de deelnemende overheidsinstanties verplichtte de noodzakelijkheid van de gegevensverwerking voorafgaand aan elk project te toetsen.[17]

Pas jaren later vond de kritiek van de Afdeling advisering en de toezichthouder gehoor in de Tweede Kamer en verzochten Kamerleden de regering om de databestanden, algoritmes en analyseermethoden die aan SyRI ten grondslag lagen te openbaren.[18] Kort daarvoor had een coalitie bestaande uit verschillende burgerrechtenorganisaties zoals het Nederlands Juristen Comité voor de Mensenrechten, het Platform Bescherming Burgerrechten en Privacy First, al de krachten gebundeld om via de Wet openbaarheid van bestuur (Wob) deze informatie boven water te halen.[19] Beide pogingen om meer transparantie af te dwingen waren tevergeefs. Telkens wees de Minister op het gevaar van '*gaming the system*'. De gevraagde openbaarmaking zou de modus-operandi van het systeem te veel blootleggen, waardoor (potentiële) fraudeurs het zouden kunnen omzeilen.[20] Daarmee gaf hij een zeer duidelijke boodschap af: transparantie en fraudeopsporing zijn volgens de Minister geen natuurlijke bondgenoten.

3. Transparantie in de SyRI-wetgeving: de rechterlijke toets

De rechtbank Den Haag ziet de verhouding tussen transparantie en fraudeopsporing heel anders. Zij verklaart de SyRI-wetgeving onverbindend omdat het transparantiebeginsel onvoldoende in acht is genomen.[21] De rechtbank stelt vast dat de SyRI-wetgeving op geen enkele manier voorziet in informatie over de gehanteerde risicomodellen of risicoanalyses. Daardoor is onduidelijk gebleven welke objectieve feitelijke gegevens gerechtvaardigd tot de conclusie kunnen leiden dat sprake is van een verhoogd frauderisico.[22] Ook tijdens de procedure heeft de Staat nagelaten de rechtbank hierin inzicht te bieden. Als gevolg heeft de rechter op geen enkele manier kunnen controleren hoe de 'eenvoudige beslis-

---

[16] H. Kaal & C. Hoetink, *Doordacht digitalisering. Digitalisering doordacht. Resultaten van een onderzoek naar het parlementaire debat over digitaliseringsvraagstukken,* Nijmegen: Radboud Universiteit 2020, p. 53.

[17] Nader rapport bij advies van de Afdeling advisering.

[18] *Kamerstukken II* 2017/18, 32761, nr. 118 (*motie Verhoeven-Buitenweg*) en *Kamerstukken II* 2017/19, 32761, nr. 112.

[19] Zie voor het Wob-verzoek https://bijvoorbaatverdacht.nl/wob-verzoek/.

[20] *Kamerstukken II* 2017/18, 32 761, nr. 122.

[21] Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, r.o. 6.87 (*SyRI*).

[22] Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, r.o. 6.87 (*SyRI*).

boom' waar de Staat over spreekt, daadwerkelijk functioneert. Daaruit concludeert hij dat de SyRI-wetgeving onvoldoende waarborgen bevat om op grond van artikel 8 lid 2 EVRM te kunnen spreken van een gerechtvaardigde inbreuk op het privéleven.

Dit gebrek aan openheid creëert volgens de rechter twee fundamentele problemen. Allereerst kunnen burgers zich hierdoor onmogelijk verdedigen tegen een risicomelding. Dat geldt ook voor burgers wiens gegevens wel in SyRI zijn verwerkt, maar die niet hebben geleid tot een risicomelding. Voor beide categorieën burgers is het onmogelijk te achterhalen of hun persoonsgegevens op juiste gronden zijn verwerkt, waardoor zij beperkt worden in hun recht om hun persoonsgegevens te volgen. De rechtbank acht dit onacceptabel. Het feit dat de overheid door de ontwikkeling van nieuwe technologieën meer mogelijkheden heeft om gegevens over burgers te verzamelen en deze met behulp van algoritmen te analyseren, brengt een bijzondere verantwoordelijkheid voor de wetgever met zich mee. Want, zo overweegt de rechtbank, "het verzamelen en analyseren van gegevens met behulp van die nieuwe technologieën kan diep ingrijpen op het privéleven van degenen op wie die gegevens betrekking hebben." Daarom zou de wetgever zich juist méér moeten inspannen om voor de burger inzichtelijk te maken wat het effect van een instrument zoals SyRI op zijn privéleven is.[23]

Ten tweede ligt het gevaar van stigmatisering op de loer. Omdat zowel het risicomodel alsook de gehanteerde risico-indicatoren tijdens het proces geheim zijn gebleven, heeft de rechtbank niet kunnen controleren of deze (onbedoeld) discriminatoir zijn. Toch is voor haar wel aannemelijk dat de inzet van SyRI mogelijk een stigmatiserend en discriminerend effect heeft. Aangezien het systeem alleen in probleemwijken is ingezet, bestaat het risico dat onbedoeld verbanden worden gelegd op grond van bias zoals een lagere sociaal economische status of een immigratieachtergrond.[24] Eisers hebben op dit punt ook bijval gekregen uit Wenen. Philip Alston, rapporteur bij de Verenigde Naties op het gebied van extreme armoede en mensenrechten, heeft zich gewend tot de rechtbank Den Haag om zijn zorgen te uiten over deze 'digitale stigmatisering' van hulpbehoevende en kwetsbare burgers.[25] De rechtbank Den Haag laat er in de *SyRI* uitspraak geen twijfel over bestaan: transparantie en fraudeopsporing zijn wel degelijk verenigbaar. Sterker nog, ze *moeten* daadwerkelijk met elkaar worden verenigd om data-gedreven fraudeopsporing binnen de grenzen van de wet te houden.

---

[23] Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, r.o. 6.85 (*SyRI*).

[24] Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, r.o. 6.85 (*SyRI*).

[25] Brief by the United Nations Special Rapporteur on extreme poverty and human rights as *Amicus Curiae* in the case of NJCM/De Staat der Nederlanden (SyRI) before the District Court of The Hague, case number C/09/5509/82, HA ZA 18//388.

4. De verbinding tussen artikel 8 EVRM en het transparantiebeginsel

De rechtbank Den Haag presenteert de toetsing aan het Unierechtelijke transparantiebeginsel op grond van artikel 8 EVRM als een vaststaand gegeven. De vraag is echter of dat daadwerkelijk zo is. Om te kunnen spreken van een gerechtvaardigde inmenging in het privéleven, vereist het tweede lid van artikel 8 EVRM dat die een wettelijke grondslag dient te hebben, noodzakelijk is in een democratische rechtsorde en proportioneel en subsidiair is in relatie tot het beoogde doel. Dat laatste is het geval indien er een *fair balance* bestaat tussen de maatschappelijke belangen die de wetgeving beoogt te beschermen en de inbreuk op het privéleven die zij eveneens oplevert. Het transparantiebeginsel komt dus als zelfstandige waarborg niet voor in het EVRM. Hoe kan de rechtbank dit Unierechtelijke beginsel dan toch inlezen in artikel 8 EVRM?

In de *SyRI*-uitspraak legt de rechtbank de verbinding tussen het Unierechtelijk gegevensbeschermingsrecht en het EVRM aan de hand van drie stappen.[26] Eerst overweegt de rechtbank dat het EVRM voorziet in een minimumbescherming van het fundamentele recht op de eerbiediging van de persoonlijke levenssfeer. Daarna stelt zij dat de reikwijdte van de bescherming die wordt geboden door de grondrechten in het EU-Grondrechtenhandvest, vergelijkbaar is met de daarmee corresponderende EVRM-rechten. Tot slot constateert de rechtbank dat het Europees recht, op grond van artikel 52 lid 3 van het EU-Grondrechtenhandvest, een ruimere bescherming kan bieden dan het EVRM. Ten aanzien van gegevensbescherming stelt zij dat de normen uit het Unierecht, de AVG en artikel 8 van het EU-Grondrechtenhandvest, een ruimere bescherming bieden dan artikel 8 EVRM. Uit deze drie punten destilleert de rechtbank dat "de minimumbescherming van artikel 8 EVRM mede inhoudt dat de SyRI-wetgeving moet voldoen aan de hiervoor genoemde algemene beginselen van gegevensbescherming die Unierechtelijk zijn vastgelegd in het Handvest en de AVG, zoals het transparantiebeginsel".[27] Zo geeft de rechtbank een ruimere uitleg aan artikel 8 EVRM. Daarmee versterkt zij de feitelijke bescherming die deze bepaling biedt. Dit valt vanuit het perspectief van rechtsbescherming toe te juichen.

Toch roept de redenering van de rechtbank de vraag op waarom zij het noodzakelijk achtte om normen uit de AVG in te lezen in artikel 8 lid 2 EVRM. Die noodzaak lijkt te schuilen in de meerwaarde die de verordening heeft ten opzichte van het EVRM. De AVG biedt op een hele andere manier bescherming aan persoonsgegevens. In tegenstelling tot het EVRM, formuleert zij concrete, gedetailleerde rechtsnormen waar instanties die persoonsgegevens verwerken – zogenaamde verwerkingsverantwoordelijken – vooraf aantoonbaar aan moeten

---

[26] Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, r.o. 6.37 (*SyRI*).
[27] Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, r.o. 6.40 (*SyRI).*

voldoen. Elke gegevensverwerking moet volgens artikel 5 AVG ten minste voldoen aan 1) het beginsel van rechtmatigheid, behoorlijkheid en transparantie, 2) het doelbindingsbeginsel, 3) het data-minimalisatiebeginsel, 4) het beginsel van opslagbeperking en 5) het beginsel van integriteit en vertrouwelijkheid. Daarnaast kent het Europees gegevensbeschermingsrecht burgers verschillende specifieke informatierechten toe waarmee zij controle kunnen uitoefenen over hun persoonsgegevens, zoals het inzagerecht, correctierecht en verwijderingsrecht.

Nu is het zo dat het EHRM een aantal van deze Unierechtelijke beginselen voor behoorlijke gegevensverwerking en informatierechten in zijn jurisprudentie ook erkent. Die erkenning baseert het Hof echter niet op het Unierecht, maar op het Dataprotectieverdrag van de Raad van Europa uit 1981.[28] Dit verdrag heeft grote invloed gehad op de rechtspraak van het EHRM.[29] Bij zijn toetsing aan artikel 8 EVRM heeft het Straatsburgse Hof regelmatig verwezen naar de beginselen voor behoorlijke gegevensverwerking uit het Dataprotectieverdrag. Op de Unierechtelijke gegevensbeschermingsregels doet het zelden een beroep. Dat is een gemiste kans. Want de beginselen voor behoorlijke gegevensverwerking uit het Dataprotectieverdrag zijn minder gedetailleerd dan die van de AVG. Zo kent dit verdrag het transparantiebeginsel niet als gegevensbeschermingsbeginsel. Daar waar de beginselen uit Verdrag 108 en de AVG wel overlappen, zijn die van de verordening doorgaans meer gedetailleerd. Dit geldt onder andere voor het doelbindingsbeginsel.[30]

5. Een transparant wettelijk kader voor risicosystemen

De *SyRI*-uitspraak leidt niet tot een kant-en-klaar raamwerk waaraan risicosystemen, waarin grote hoeveelheden persoonsgegevens worden verwerkt, moeten voldoen. Dat had ook niet gekund; de controlerende rechter zegt vooral waar de grens van de rechtmatigheid wordt overschreden en hoeft geen uitspraken te doen over mogelijke systemen die de toets wel zouden doorstaan. Bovendien zal de Staat veel meer informatie moeten ontsluiten over de programmering, uitwerking en periodieke controle op het systeem, wil een rechterlijke uitspraak meer houvast kunnen geven ten aanzien van de vraag of het risicomodel voldoet. En dat is de meest belangrijke les van deze uitspraak: zonder de nodige transparantie over de gehanteerde risicomodellen en indicatoren kan een rechter on-

---

[28] Verdrag van de Raad van Europa tot bescherming van personen in verband met de automatische verwerking van persoonsgegevens, Straatsburg 18 januari 1981, ETS 108, Trb. 1988, nr. 7.

[29] H.R. Kranenborg & L.F.M. Verhey, *De Algemene Verordening Gegevensbescherming in Europees en Nederlands perspectief,* Deventer: Wolters Kluwer 2018, p. 23.

[30] Verhey & Raijmakers, 2013, p. 196.

mogelijk toetsen of een '*fair balance'* is bereikt.[31] Ook belangrijk is dat men inziet dat het enkele ontwerp van een systeem niet alles bepalend is of een risicomodel de toets aan artikel 8 lid 2 EVRM of de AVG doorstaat. Hoe groot de inbreuk op het privéleven is, is ook afhankelijk van de wijze waarop vervolgens op de werkvloer (of in de *cloud)* met de gegevensverwerking en –analyse wordt omgegaan. Belangrijk is dat in wetgeving waarborgen zijn getroffen om misbruik in het gebruik te voorkomen, bijvoorbeeld door regulering van werkprocessen en periodieke controlesystemen. Wij geven vanuit een bestuursrechtelijke context enige handvaten die we aan de rechtspraak ontlenen, die wetgever en bestuur moeten doordenken ten behoeve van een rechtmatig risicoprofileringssysteem:[32]

5.1 Over het ontwerp van het systeem

- Creëer een wettelijke grondslag voor risicoanalyses en de waarborgen die daarbij in acht moeten worden genomen, zoals de termijnen voor bewaring en vernietiging van de verzamelde persoonsgegevens, de opslag en het gebruik van de verkregen gegevens, toegang van derden tot de vergaarde gegevens en procedures voor de borging van de integriteit en vertrouwelijkheid van de gegevens.[33]
- Bij geheime onderzoekshandelingen in de privésfeer biedt 'de wettelijke grondslag' van een bevoegdheid echter beperkt houvast. Het EHRM heeft er bijzondere aandacht voor of voldoende waarborgen zijn getroffen om willekeur en misbruik te doen voorkomen.[34] De risico's op misbruik kunnen met zowel juridische (zoals wie autoriseert onder welke voorwaarden)[35]

---

[31] Vgl. B. van der Sloot & S. van Schendel, 'De juridische randvoorwaarden voor een data-gedreven samenleving', *NJB* 2019/2776, par. 4 en de noot van Van Schendel in *Computerrecht* 2020/87.

[32] De Minister van Rechtsbescherming heeft in een brief van 8 oktober 2019 waarborgen geduid waaraan risicoanalyses binnen de overheid moeten voldoen, in het bijzonder wanneer persoonsgegevens worden verwerkt, *Kamerstukken II* 2019-20, 26 643, nr. 641. Het kabinet streeft ernaar deze richtlijnen uiteindelijk in wettelijke regels neer te leggen.

[33] EHRM 4 december 2008, nr. 30562/04 en 30566/04, *NJ* 2009/410 m.nt. E.A. Alkema (*S en Marper/Verenigd Koninkrijk*).

[34] Zie o.a. EHRM 4 december 2008, nrs. 30562/04 en 30566/04 (*S. en Marper tegen het Verenigd Koninkrijk*); EHRM 18 oktober 2016, nr. 61838/10 (Vukota-Bojic tegen Zwitserland), *AB* 2017/418 m.nt. Y.E Schuurmans & J. Uzman.

[35] Zo nam de rechtbank mee dat SyRI geen voorafgaande integrale afweging van de noodzakelijkheid van de gegevensverwerking door een onafhankelijke derde bevatte, zie r.o. 6.99.

als met technische instrumenten (zoals informatiebeveiliging)[36] worden geminimaliseerd.
- Verantwoord de selectie van categorieën gegevens[37]/ type bestanden die worden gekoppeld.[38]
- Maak duidelijk of die categorieën enkel gestructureerde of ook ongestructureerde gegevens bevatten.[39]
- Leg het ontwerp van het systeem goed vast en maak deze voor burgers inzichtelijk. Het moet evident zijn welke keuzes zijn gemaakt (o.a. welke gegevenskoppeling), welke feitelijke aannames het systeem bevat (een groot gevaar bestaat als waarde x wordt overschreden) en aan de hand van welk type algoritme de verzamelde gegevens worden geanalyseerd. Het ontwerp op papier is echter niet alles bepalend, de uitkomsten van het ontwerp moeten worden geverifieerd en gevalideerd (hoe werkt het feitelijk uit als we het ontwerp op verschillende datasets loslaten?).[40]
- Algoritmes die een beslisboom volgen, zijn het gemakkelijkst uitlegbaar en transparant te maken. Voor eenvoudige overheidstaken verdienen die de voorkeur, omdat ze op fouten controleerbaar zijn en dus controle op het bestuur mogelijk maken. Uiteraard moet een bestuursorgaan dan wel inzicht geven in die beslisbomen, wat de Minister in de SyRI-zaak juist stelselmatig weigerde. Complexe taken met een grote impact op het algemeen belang (bijv. maatregel x betekent y voor de instandhouding van deze beschermde diersoort) vragen eerder om de inzet van *artificial intelligence*. Daar waar de menselijke intelligentie er niet meer bij kan, bestaat behoefte aan kunstmatige intelligentie.[41] *Case based algorithms* en *deep learning* toepassingen

---

[36] Zie o.a. M.S. Bargh, R. Meijer & M. Vink, *On statistical disclosure control technologies. For enabling personal data protection in open data settings*, Den Haag: WODC Cahier 2018-20.

[37] Met de term 'gegevens' doelen we op persoonsgegevens en niet-persoonsgegevens.

[38] Vgl. ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259, *AB* 2017/313 m.nt. P. Mendelts; *M&R* 2017/84, m.nt. M.M. Kaajan; *Computerrecht* 2017/256, m.nt. B.M.A. van Eck en *Gst.* 2017/170, m.nt. B. Assink.

[39] Vgl. S. van Schendel in de noot in *Computerrecht* 2020/87.

[40] Vgl. r.o. 6.89 van de SyRI-uitspraak.

[41] Het kabinet geeft zich laten inspireren door Frankrijk en neemt als beleidsmatig uitgangspunt dat overheidsorganisaties geen algoritmes mogen hanteren die te complex zijn om redelijkerwijs te kunnen worden uitgelegd, *Kamerstukken II* 2019/20, 26 643, nr. 641, p. 7.

zijn niet bij voorbaat onrechtmatig, maar moeten van uitleg- en auditsystemen worden voorzien, opdat controle op het bestuur mogelijk blijft.[42]

5.2 Over de gegevensanalyse

- Besteed aandacht aan de beginselen voor gegevensverwerking uit artikel 5 van de AVG. Houd daarbij in het bijzonder rekening met het doelbindingsvereiste en het dataminimalisatiebeginsel. Maar ook het privacy-aspect vergt soberheid. Hoe meer persoonsgegevens een bestuursorgaan koppelt, hoe eerder het een bepaald aspect van het privéleven structureel en indringend in kaart brengt, en dus hoe forser de inmenging is in de zin van artikel 8 EVRM.[43] In het algemeen is het juridisch slim om eerst met een vrij sober risicosysteem te werken; blijkt dat ontwerp onvoldoende voor zinvolle risicoselectie, dan is het gemakkelijker uit te leggen dat een bredere gegevensvergaring noodzakelijk is om het doel van fraudeopsporing te bereiken. De proportionaliteitstoets kan dan beter worden gemotiveerd.
- Naast zorgen over de privacy-inmenging bestaan grote zorgen over het mogelijk discriminerende effect van risicoanalyses. Tussen het recht op de persoonlijk levenssfeer, het ontwikkelen van een persoonlijke identiteit én het recht gevrijwaard te blijven van discriminatie, stereotypering en stigmatisering bestaat een nauwe band.[44] Om zorgen rond discriminatie weg te kunnen nemen, moet je weten op welke factoren wordt geselecteerd. Die factoren doen alarmbellen rinkelen als zij verwijzen naar bijvoorbeeld nationaliteit, leeftijd, of geslacht.[45] Een direct onderscheid naar deze factoren is verdacht en moet door het bestuursorgaan zeer overtuigend worden gemotiveerd. Een toets op direct onderscheid is echter niet voldoende, ook een ongerechtvaardigd indirect onderscheid moet worden opgemerkt. En dat vaststellen kan niet zonder de *uitwerking* van het risicosysteem aan een analyse te onderwerpen. Wie bijvoorbeeld bezit van een huisdier selecteert als een contra-indicatie voor fraude (aanname van een zorgzaam persoon), moet zich realiseren dat die factor leidt tot een ondervertegenwoordiging van personen met een migratieachtergrond in de verzameling

---

[42] Zie o.a. N.H. van Amerongen & Y.E. Schuurmans, 'Advies van een deskundige of algoritme? De toetsing van black-box besluiten door de bestuursrechter', in: P.J. Huisman, A.R. Neerhof & F.J. van Ommeren (red.), *Verwant met verband: ruimte, recht en wetenschap*, Den Haag: IBR 2019, p. 175-196; C.J. Wolswinkel, *Willekeur of algoritme? Laveren tussen analoog en digitaal bestuursrecht* (oratie Tilburg), Tilburg: Tilburg University 2020, i.h.b. par. 3.3 en 3.4.

[43] EHRM 22 september 2010, ECLI:NL:XX:2010:BQ2953 nr. 35623 (*Uzun/Duitsland*).

[44] Zie ook r.o. 6.24 van de SyRI-uitspraak.

[45] Of een van de andere factoren uit artikel 14 EVRM en artikel 1 GW.

contra-indicaties, omdat zij gemiddeld minder vaak een huisdier hebben.[46] Een methode is om bij het ontwerp wél relevante bijzondere persoonsgegevens te verwerken, zodat elementen in de profilering die tot vooroordelen leiden, kunnen worden geëlimineerd.[47]

- Worden persoonsgegevens van burgers opgenomen in het systeem, informeer hen dan over de verwerking, zodat zij zich ervan kunnen vergewissen dat de verwerking op juiste gronden plaatsvindt en zich daartegen eventueel in rechte kunnen verdedigen.[48]

6. Het transparantiebeginsel in het bestuursrechtelijk bewijsrecht

Transparantie moet niet alleen in *het ontwerp* van een risicosysteem zijn ingebouwd, het moet ook een leidende waarde zijn bij de uitvoering op basis van het systeem. Deels kan het gegevensbeschermingsrechtelijke transparantiebeginsel worden ingelezen in het bestuursrechtelijke bewijsrecht, deels heeft het een eigenstandige waarde. Veel bewijsregels hebben tot doel waarheidsvinding te bevorderen. Als uitgangspunt zal het transparantiebeginsel ruimhartig worden omarmd in het bestuursrechtelijke bewijsrecht, omdat het waarheidsvinding bevordert. Toch hebben gegevensbeschermingsrechtelijke en bewijsrechtelijke transparantie een ander doel en ratio. In het gegevensbeschermingsrecht moet het transparantiebeginsel bestuursorganen verantwoording laten afleggen over de verwerking en de burger in staat stellen zijn rechten uit te oefenen, bijvoorbeeld opdat hij zijn geïnformeerde toestemming tot gegevensverwerking kan intrekken. Met die strekking duikt het transparantiebeginsel op vele momenten in de verwerkingscyclus op, maar ver hoeft de uitleg van de verwerkingsverantwoordelijke niet te gaan. Zo legt artikel 12 AVG vast dat communicatie in verband met de verwerking in beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal dient te geschieden.[49] Bewijsrechtelijke transparantie vergt dat feitelijke stellingen concreet en verifieerbaar zijn, zodat de wederpartij tegenbewijs kan leveren en de rechter uiteindelijk tot een beredeneerde overtuiging kan komen. Die vorm van transparantie duikt op minder momenten op (alleen bij feitelijke stellingen die tot de omvang van het

---

[46] Of zie het voorbeeld in de noot van Bastiaans, Barkhuysen & Jak: inwoners in Amsterdam-Zuid blijken beter te klagen dan inwoners van Amsterdam-Noord, omdat het systeem voor klachtafhandeling meer gewicht toekent aan het woord 'klacht' dan aan het woord 'teringzooi', *O&A* 2020/28.

[47] Zie *Kamerstukken II* 2019/20, 26 643, nr. 641, p. 11 en H. Lammerant, P. Blok & P. de Hert, Big data besluitvormingsprocessen en sluipwegen van discriminatie, *NTM/NJCM-bull.* 2018/1, p. 10–11.

[48] SyRI-uitspraak r.o. 6.90.

[49] Artikel 12 AVG. Zie ook Groep gegevensbescherming artikel 29, Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679.

geding behoren), maar gaat wel een stuk verder. Ten behoeve van de waarheidsvinding moet de communicatie eerder plaatsvinden in uitgebreide, precieze en zo nodig met expertise onderbouwde vorm. Kortom, gegevensbeschermingsrechtelijke transparantie kan bewijslevering bevorderen, maar zal vanuit bewijsrechtelijk oogpunt niet ver genoeg gaan. Aan de andere kant versterkt het brede gegevensbeschermingsrechtelijke transparantiebeginsel de informatiepositie van de burger. Hij krijgt nu informatie over wie op welk moment aan de hand van welke persoonsgegevens onderzoek naar hem verricht. Daardoor krijgen burgers meer zicht op het feitelijke onderzoek, wat het juridische debat meer richting de rechtmatigheid van de wijze van bewijsverkrijging trekt. Wij vermoeden dat het gegevensbeschermingsrecht de komende jaren een prominente rol gaat spelen in de verdere ontwikkeling van het leerstuk van onrechtmatig verkregen bewijs.

Deze ontwikkeling sluit aan bij een van onze eerdere observaties: in het bestuursrecht zal meer aandacht voor feitelijke handelingen moeten bestaan, omdat in een gedataficeerde samenleving het Awb-besluit niet langer het ultieme moment van machtsuitoefening is.[50] Niet alleen besluiten, maar ook feitelijke gegevensregistraties kunnen een grote, langdurige en deels onvoorziene impact hebben op het leven van een burger.[51] Dat is ook wat de rechtbank in de SyRI-uitspraak benadrukt. Hoewel er geen publiekrechtelijke rechtshandeling plaatsvindt – en het bestuur dus niet uit is op een bepaald rechtsgevolg – heeft de risicomelding wel degelijk aanmerkelijk effect op het privéleven van degene ten aanzien van wie een melding is gedaan.[52] Hij kan twee jaar lang met een verhoogd frauderisico bij bestuur, politie en Openbaar Ministerie te boek staan. Wie alleen vanuit de rechtshandeling denkt, ziet wellicht weinig schade; de burger worden immers nog geen rechten afgenomen. Maar de impact op het verdere verloop van het fraudeonderzoek kan groot zijn. Vanuit de rechtspsychologie is duidelijk dat *framing* van informatie van grote invloed is op de waardering van bewijsmateriaal. Degene die bewijsmateriaal gaat waarderen, start niet bij nul. De eerste informatie die hij tot zich neemt, vult het denkraam, waarna hij bij de beoordeling van volgende bewijsstukken steeds zal moeten beredeneren of hij zijn aanvankelijke beeld moet bijstellen.[53] Bij degene die aangevinkt staat als fraudegevoelig persoon, is dát het frame waarin bewijsmateriaal wordt gewaardeerd. De kans dat het bestuursorgaan actief op zoek gaat naar ontlastend be-

---

[50] F. Çapkurt & Y.E. Schuurmans, 'Blinde vlek in de Awb: data', in: T. Barkhuysen e.a. (red.), *25 jaar Awb. In eenheid en verscheidenheid*, Deventer: Wolters Kluwer 2019, p. 253-265.

[51] F. Çapkurt, 'Het bestuursrecht en gegevensbeschermingsrecht: de ontmoeting van twee rechtsgebieden in historisch perspectief', *RMThemis* 2020-4, p. 186.

[52] R.o. 6.59 van de SyRI-uitspraak.

[53] Zie o.a. D.H.J. Wigboldus, 'Psychologisch aspecten bij bewijslevering', in: *Bewijsrecht* (procesrechtelijke reeks NVvP), Den Haag: Bju 2010, p. 46-55.

wijsmateriaal en het toetsen van alternatieve hypothesen, is daarmee aanzienlijk verkleind.

7. De toeslagenaffaire: SyRI 2.0?

De Staat heeft besloten om niet in hoger beroep te gaan tegen de uitspraak van de rechtbank Den Haag. Daarmee is het SyRI hoofdstuk in beginsel afgesloten. In beginsel, want SyRI is niet het enige profileringssysteem dat het afgelopen jaar veel stof heeft doen opwaaien. Ook andere profileringssystemen van de overheid haalden het nieuws. Een daarvan was de Fraude Signalering Voorziening (FSV) van de Belastingdienst, een van de hoofdrolspelers in de kinderopvangtoeslagenaffaire.[54] De Belastingdienst heeft in dit systeem jarenlang signalementen van fraude vastgelegd. Tot zover de overeenkomsten tussen SyRI en de FSV. De verschillen tussen deze twee fraude-opsporingssystemen zijn namelijk nog groter. Het eerste verschil heeft betrekking op transparantie. SyRI was weliswaar ondoorzichtig en daardoor oncontroleerbaar voor zowel burger als rechter, maar men wist wel dát het bestond; het systeem was zelfs verankerd in de wet. Bij de FSV was dit geenszins het geval. Dit systeem opereerde volledig in de schaduw van de rechtsstaat: op de Belastingdienst na, wist niemand af van het bestaan ervan. Pas na de onthulling van de kinderopvangtoeslagenaffaire kwam het aan het licht. De FSV was geen *black box* maar een *unknown box*.

Het tweede verschil ziet op rechtsbescherming. De gegevensregistratie in SyRI had geen directe rechtsgevolgen. Na het signalement ging het betrokken bestuursorgaan over tot heronderzoek en pas na aannemelijk gemaakte fraude kon een uitkering worden ingetrokken of gekort. Registratie in de FSV had daarentegen wél direct grote gevolgen voor de rechtspositie van burgers. Werd je als fraudeur met de indicatie 'opzet/grove schuld' in het systeem geregistreerd – wat de Dienst Toeslagen regelmatig deed zonder feitenonderzoek te verrichten -[55] dan werd je onder verzwaard bestuurlijk toezicht geplaatst: je toeslag werd van de ene op de andere dag stopgezet en het recht op een persoonlijke betalingsregeling werd je ontnomen.[56] Alle ruimte voor het bieden van maatwerk verviel hiermee: ongeacht de betalingscapaciteit van de burger, moest hij de reeds ont-

---

[54] P. Klein, 'Geheime zwarte lijst Belastingdienst over 'verdachte' burgers', *RTL Nieuws* 17 april 2020 en KPMG, *Rapportage verwerking risicosignalen toezicht Belastingdienst,* bijlage bij de brief van de Staatssecretarissen van Financiën van 10 juli 2020, 2020-0000130507. Dit systeem is per februari 2020 uit de lucht gehaald.

[55] KPMG, *Rapportage verwerking risicosignalen toezicht Belastingdienst,* bijlage bij de brief van de Staatssecretarissen van Financiën van 10 juli 2020, 2020-0000130507, p. 4.

[56] KPMG, *Rapportage verwerking risicosignalen toezicht Belastingdienst,* bijlage bij de brief van de Staatssecretarissen van Financiën van 10 juli 2020, 2020-0000130507, p. 34 e.v.

vangen toeslagen in één keer terugbetalen.[57] Dat heeft in de toeslagenaffaire uiteindelijk duizenden families in de problemen gebracht.

De registratie in de FSV had dus grote gevolgen voor de positie van burgers. Tegelijkertijd was de opzet, inrichting en werking van het systeem allesbehalve behoorlijk en rechtmatig. Meer dan vijfduizend medewerkers van de Belastingdienst hadden toegang tot de FSV.[58] Zij konden ongecontroleerd persoonsgegevens kopiëren, wijzigen of wissen. De gegevens werden, volledig in strijd met de beginselen voor behoorlijke gegevensverwerking uit de AVG, jarenlang bewaard en vormden de basis voor toekomstige, voor de burger onvoorzienbare rechtshandelingen, zoals de terugvordering van de kinderopvangtoeslag.[59] Dit leidde tot een kafkaëske situatie: de registratie bepaalde de facto hoe de burger werd behandeld door Toeslagen/de Belastingdienst en werd hem het recht op een persoonlijke betalingsregeling ontnomen, maar de burger kon zich tegen de registratie op geen enkele manier verdedigen omdat hij hiervan niet op de hoogte was.

Met de *SyRI*-uitspraak heeft de rechtbank Den Haag een belangrijke stap gezet richting de normering van data-gedreven fraudeonderzoek. Toch is het maar de vraag in hoeverre de concrete normen die uit deze rechtspraak voortkomen, erin zullen slagen om grip te krijgen op de risicoprofileringspraktijk in de publieke sector. Dat kan alleen als bestuursorganen vooraf meer openheid geven, waarvoor enige dwang van wetgever en rechter nodig lijken.

8. Conclusie

Naarmate gegevensregistraties bepalender zijn voor de positie van de burger ten opzichte van de overheid - en de aanleiding vormen voor het nemen van ingrijpende besluiten - zal ook het bestuursrecht meer oog moeten krijgen voor de rechtmatigheid van de verwerking van persoonsgegevens. In de *SyRI*-uitspraak heeft de rechtbank belangrijke lijnen uitgezet voor de normering van fraudeonderzoek door overheidsinstanties in het digitale tijdperk. De klassieke waarborgen van artikel 8 EVRM heeft zij versterkt door deze een Unierechtelijke tintje te geven, met een prominente rol voor het transparantiebeginsel. Zonder transparantie over ontwerp én werking

---

[57] Artikel 7 lid 6 Awir.

[58] Gegevensbeschermingseffectbeoordeling Rijksdienst, *FSV (Fraude Signalering Voorziening)*, geactualiseerde versie 1.2, november 2019, p. 17.

[59] Recent kwam aan het licht dat de aanwezigheid van een tweede nationaliteit reden kon zijn voor Toeslagen om toeslagenontvangers te onderwerpen aan extra controle. De registratie van de dubbele nationaliteit van toeslagaanvragers was volgens de Autoriteit Persoonsgegevens echter onrechtmatig, discriminerend en daarmee in strijd met de AVG. Zie Belastingdienst/Toeslagen, *De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag*, Onderzoeksrapport | z2018-22445.

van het systeem kan de rechter niet beoordelen hoeveel informatie over personen wordt geanalyseerd, hoe groot de privacy-inbreuk is, noch wat de discriminerende effecten zijn.

De *SyRI*-uitspraak zien wij als een eerste maar belangrijke stap in een ontwikkeling naar een ruimhartige toepassing van het gegevensbeschermingsrechtelijke transparantiebeginsel in het bestuursrecht, waarbij steeds meer aandacht uitgaat naar de wijze waarop met gegevens, in het bijzonder persoonsgegevens, wordt omgegaan. Deze uitspraak maakt geen einde aan frauderisicoanalyses, maar vraagt wel om meer waarborgen. Buitenwettelijke, geheime risicoprofileringssystemen kunnen niet aan die eisen voldoen. Hoe de uitspraak een vervolg gaat krijgen, is nog gissen. De Minister voor Rechtsbescherming onderkent inmiddels dat transparantie het leidende beginsel is bij algoritmische data-analyses door de overheid, maar ziet tegelijk dat uitzonderingen nodig zijn om *'gaming the system'* te voorkomen.[60] Hopelijk hebben de *SyRI*-uitspraak én de maatschappelijke ophef over de kinderopvangtoeslagaffaire geïllustreerd dat die uitzondering zeer spaarzaam en selectief moet worden ingezet.

---

[60] *Kamerstukken II* 2019/20, 26 643, nr. 641.