Positie Amnesty 'Kwaliteitskader Big Data' van het OM en de Nederlandse politie

Mei 2021

1. Benoem mensenrechtenstandaarden

Het kwaliteitskader is een beschrijvings- en toetsingskader, waarmee de politie inzichtelijk wil maken hoe een Big Data project is opgezet, wordt uitgevoerd en welke 'checks and balances' aanwezig zijn.[1] Het bevat overwegingen die relevant zijn voor mensenrechten, maar overweegt mensenrechten niet als bindende normen waaraan moet worden voldaan en verwijst niet naar mensenrechtenverdragen of jurisprudentie. Het kwaliteitskader is vrijblijvend: er zijn "geen goede of foute antwoorden".[2] Toch wordt het als toetsingskader ingezet. Het kader kan in de huidige vorm om twee redenen niet als mensenrechtenwaarborg worden gezien:

i. Een toetsing moet uitgevoerd worden door een rechter of een andere onafhankelijke en onpartijdige partij. Hoewel de OvJ gebonden is aan integriteitseisen, is hij/zij een 'partij' die belangen verdedigt. De OvJ kan moeilijk gezien worden als voldoende objectief en onafhankelijk om de noodzakelijke afweging tussen conflicterende belangen te maken.[3]
ii. Voor een toetsing moeten duidelijke criteria worden gehanteerd, waaronder de vraag of een minder ingrijpende maatregel kan volstaan om de vastgestelde dwingende publieke belangen te dienen. De verschillende risico's en belangen moeten voorafgaand worden gewogen.[4] Dergelijke criteria ontbreken in het kwaliteitskader.

Kortom, zonder criteria is het Kwaliteitskader niet geschikt voor risico-inschatting en toetsing. Amnesty raadt aan om in het Kwaliteitskader duidelijke criteria op te nemen waaraan getoetst kan worden. Alleen dan kan het Kwaliteitskader de politie en het OM helpen om de mensenrechtenrisico's van gegevensverwerkingen te beoordelen en schendingen te voorkomen. De volgende punten geven hiertoe een eerste aanzet.

[1] OM en Politie, Kwaliteitskader Big Data, Versie 1.0, 11 mei 2020, https://www.rijksoverheid.nl/documenten/rapporten/2020/05/29/tk-bijlage-2-kwaliteitskader-big-data, p. 3.
[2] OM en Politie, Kwaliteitskader Big Data, Versie 1.0, 11 mei 2020, p. 3.
[3] EHRM 14 september 2010, nr. 38224/03 (*Canoma Uitgevers B.V. t. Nederland*) para. 93.
[4] EHRM 14 september 2010, nr. 38224/03 (*Canoma Uitgevers B.V. t. Nederland*) para. 92.

2. Stel beperkingen aan het gebruik van artikel 3 Politiewet

Gegevensverwerkingen door de politie vormen een inmenging op het recht op privacy.[5] Een inmenging moet een legitiem doel dienen, gebaseerd zijn op een wettelijke grondslag en noodzakelijk zijn in een democratische samenleving.[6] Het kwaliteitskader overweegt dat het vereiste van een wettelijke grondslag *"dwingt om kritisch te kijken naar de grenzen van artikel 3 Politiewet en aanpalende wetgeving waar Politie bevoegdheid uit ontleent".*[7]

Amnesty onderschrijft deze noodzaak en raadt aan om het gebruik van artikel 3 Politiewet duidelijk te begrenzen in het kwaliteitskader, conform mensenrechten. Artikel 3 Politiewet is een wet met een laag niveau van nauwkeurigheid die kan worden gebruikt voor een 'geringe inbreuk', bijvoorbeeld surveillance door middel van een politieauto. Politiesystemen die gebruik maken van sensoren en/of geautomatiseerde verwerking van persoonsgegevens brengen een ernstigere inbreuk op het recht op privacy met zich mee. Artikel 3 Politiewet volstaat in zulke gevallen niet als voldoende specifieke wettelijke basis.[8]

3. Formuleer de verplichting tot het uitvoeren van een gegevensbeschermings-effectbeoordeling (GEB) conform EU-recht

Het recht op gegevensbescherming vereist dat gegevensverwerkingen gebaseerd zijn op een wettelijke basis en een specifiek en legitiem doel dienen. Gegevensverwerkingen moeten ook proportioneel zijn. Dit betekent onder meer dat zij moeten voldoen aan het principe van dataminimalisatie: de data moet relevant zijn voor het doel van de verwerking. Het recht op gegevensbescherming verplicht tot het uitvoeren van een gegevensbeschermingseffectbeoordeling (GEB) bij gegevensverwerkingen met een hoog risico voor de rechten en vrijheden van betrokkenen.[9]

Het kwaliteitskader beperkt de GEB-verplichting tot de inzet van nieuwe technologieën met een risico voor de rechten van betrokkenen. Richtlijn 2016/680 bevat een bredere verplichting: een GEB is verplicht wanneer een verwerking "*gelet op de aard, de reikwijdte, de context of de doeleinden daarvan, waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen oplevert."*[10] Het gebruik van nieuwe technologieën kan wijzen op een dergelijk hoog risico, maar ook andere factoren kunnen nopen tot een GEB (zie

[5] Artikel 12 Universele Verklaring van de Rechten van de Mens (UVRM), artikel 17 Internationaal Verdrag inzake burgerrechten en politieke Rechten (IVBPR), artikel 8 Europese Verdrag voor de Rechten van de Mens (EVRM) en artikel 7 Handvest van de Grondrechten van de EU (EU-Handvest). Amnesty International, *We Sense Trouble,* 2020*,* hoofdstuk 2.1, p. 15-16.

[6] Amnesty International, *We Sense Trouble,* 2020, https://www.amnesty.org/download/Documents/EUR3529712020ENGLISH.PDF, hoofdstuk 2.2, p. 17-19.

[7] OM en Politie, Kwaliteitskader Big Data, Versie 1.0, 11 mei 2020, p. 5.

[8] Amnesty's International, *We Sense Trouble,* 2020*,* hoofdstuk 4.4, p. 33-34.

[9] Het EVRM erkent het fundamentele belang van gegevensbescherming onder het recht op privacy. In de EU is het recht op gegevensbescherming opgenomen in artikel 8 van het EU-Handvest. Zie Amnesty International, *We Sense Trouble,* 2020*,* hoofdstuk 2.3, p. 19-21.

[10] EU-Richtlijn 2016/680, artikel 27, lid 1.

bijlage voor een overzicht).[11] Daarbij moet de verwijzing naar “de rechten en vrijheden” breder worden opgevat dan enkel het recht op gegevensbescherming:

> “Zoals aangegeven in de Verklaring van de Groep gegevensbescherming artikel29 over de rol van een risicogebaseerde benadering in rechtskaders inzake gegevensbescherming, heeft de verwijzing naar "de rechten en vrijheden" van betrokkenen voornamelijk betrekking op de rechten op gegevensbescherming en privacy, maar kan ze ook andere grondrechten betreffen zoals vrijheid van meningsuiting, vrijheid van gedachte, vrijheid van verkeer, discriminatieverbod, recht op vrijheid, en vrijheid van geweten en godsdienst.”[12]

De GEB-verplichting is daarmee breder dan de verplichting tot het uitvoeren van een security audit. Als verwerkingsverantwoordelijke moet de politie de risico's voortdurend beoordelen om te kunnen vaststellen wanneer een soort verwerking waarschijnlijk een hoog risico inhoudt.[13] Amnesty raadt aan om deze criteria op te nemen in het kwaliteitskader. Daarnaast raadt Amnesty aan om ook de consultatieverplichting op te nemen in het Kwaliteitskader. De Autoriteit Persoonsgegevens dient geraadpleegd te worden wanneer een gegevensverwerking een hoog risico voor de rechten en vrijheden van betrokkenen met zich meebrengt.[14]

4. Voorkom discriminatie: gebruik geen beschermde gronden in profielen en risicomodellen

Mensen hebben het recht om niet gediscrimineerd te worden.[15] Data en algoritmes zijn niet objectief, en het gebruik daarvan kan op verschillende manieren leiden tot discriminatie.[16] Het kwaliteitskader overweegt terecht dat:

> *“Het (…) belangrijk [is] dat bij elke stap in het proces er bewustwording op het risico van bias aanwezig is”.*[17]

Om discriminatie te voorkomen, moet de politie systemen niet inzetten voor stereotypen criminaliteit, die specifieke gemeenschappen raken, en afzien van het gebruik van beschermde gronden, zoals etniciteit, nationaliteit of proxy’s daarvoor, in profielen en

[11] Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking “waarschijnlijk een hoog risico inhoudt” in de zin van Verordening 2016/679, 17/NL WP 248 rev.01, https://edpb.europa.eu/our-work-tools/our-documents/guideline/data-protection-impact-assessments-high-risk-processing_nl.

[12] Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking “waarschijnlijk een hoog risico inhoudt” in de zin van Verordening 2016/679, p. 7.

[13] Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking “waarschijnlijk een hoog risico inhoudt” in de zin van Verordening 2016/679, p. 7.

[14] Richtlijn gegevensbescherming opsporing en vervolging (EU) 2016/680, art. 28 lid 1, sub b. Zie ook Aanbeveling betreffende het gebruik van persoonsgegevens in de politiesector (1987), p. 1.3. De verplichting is geïmplementeerd in Wet politiegegevens, art. 33b lid 1, sub a.

[15] Artikel 7 UVRM, artikel 26 IVBPR, artikel 14 EVRM en artikel 21 EU-Handvest. Het EU-recht bevat daarnaast een specifiek verbod op discriminatie op grond van nationaliteit in artikel 18 van het Verdrag betreffende de werking van de EU. Zie Amnesty International, *We Sense Trouble*, 2020, hoofdstuk 2.4, p. 21-24.

[16] Zie Amnesty International, *We Sense Trouble,* 2020*,* hoofdstuk 5, p. 37-42.

[17] OM en Politie, Kwaliteitskader Big Data, Versie 1.0, 11 mei 2020, p. 10.

risicomodellen.[18] Amnesty raadt aan om risicomodellen te evalueren om te beoordelen of zij tot discriminatie leiden. Ook wordt aanbevolen om experts, waaronder non-discriminatie-experts en getroffen gemeenschappen, te consulteren in het ontwerp en de evaluatie van risicomodellen.[19]

5. Betrek mensenrechtenexperts bij Big Data projecten

Het kwaliteitskader erkent het belang van een multidisciplinair team:

> *"Het is van groot belang dat materiedeskundigen evenals privacy deskundigen al aan de tekentafel betrokken worden. Het streven is met een multidisciplinair team te werken aan een plan van aanpak".*[20]

Amnesty raadt aan om mensenrechtenexperts te consulteren voorafgaand en gedurende projecten die gebruik maken van risicomodellen en nieuwe vormen van surveillance.[21]

6. Benoem in het Kwaliteitskader dat ook proeftuinen, experimenten en pilots in lijn moeten zijn met mensenrechten

Mensenrechten zijn overal van toepassing en gelden ook wanneer de politie experimenteert met nieuwe technologieën of methoden. Sterker nog: er moet dan strenger worden toegezien op de naleving van mensenrechten.[22]

7. Formuleer transparantieverplichtingen

Transparantie wordt in het kwaliteitskader maar liefst veertien keer genoemd onder 'te beschermen waarden', maar zonder normstelling of verplichting. Amnesty raadt aan om transparantieverplichtingen te formuleren die publieke controle en toezicht door de Autoriteit Persoonsgegevens mogelijk maken.[23]

[18] Amnesty International, *We Sense Trouble, 2020,* hoofdstuk 5.2, p. 40-41 en Recommendations, p. 43, onder 4.
[19] Amnesty International, *We Sense Trouble, 2020,* hoofdstuk 5.2, p. 40-41 en Recommendations, p. 43, onder 5.
[20] OM en Politie, Kwaliteitskader Big Data, Versie 1.0, 11 mei 2020, p. 7.
[21] Amnesty International, *We Sense Trouble,* 2020*,* Recommendations, p. 43 onder 5 en 6.
[22] Amnesty International, *We Sense Trouble,* 2020*,* hoofdstuk 4.1, p. 29-30.
[23] Amnesty International, *We Sense Trouble,* 2020*,* Recommendations, p. 43 onder 8.

Bijlage: Richtsnoeren voor gegevensbeschermingseffectbeoordelingen

De volgende negen criteria moeten in aanmerking worden genomen bij het bepalen of een verwerking een hoog risico inhoudt:[24]

1. *Evaluatie of scoretoekennig*
   Een voorbeeld hiervan is een databank die wordt ingezet in de strijd tegen witwaspraktijken en terrorismefinanciering, of het verzamelen van openbare socialemediagegevens met het oog op het genereren van profielen.[25]

2. *Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg*
   Een verwerking die gericht is op het nemen van beslissingen met betrekking tot betrokkenen "waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden" of die "de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen". De verwerking kan bijvoorbeeld leiden tot uitsluiting of discriminatie van natuurlijke personen. Verwerking met weinig of geen gevolg voor natuurlijke personen voldoet niet aan dit specifieke criterium.

3. *Stelselmatige monitoring*
   Verwerking die wordt gebruikt voor het observeren, monitoren of controleren van betrokkenen, inclusief via netwerken verzamelde gegevens of stelselmatige monitoring van openbaar toegankelijke ruimten.

4. *Gevoelige gegevens of gegevens van zeer persoonlijke aard*
   Hieronder vallen onder meer locatiegegevens en persoonsgegevens met betrekking tot strafrechtelijke veroordelingen of strafbare feiten.

5. *Op grote schaal verwerkte gegevens*
   Factoren hierbij zijn het aantal betrokkenen, het volume van de gegevens, de duur of het permanente karakter van de gegevensverwerking en de geografische omvang van de verwerking.

6. *Matching of samenvoeging van datasets*
   Bijvoorbeeld datasets die voortkomen uit twee of meer gegevensverwerkingen die voor verschillende doeleinden zijn uitgevoerd en/of door verschillende verwerkingsverantwoordelijken zijn uitgevoerd op een wijze die de redelijke verwachtingen van de betrokkene zou overschrijden.

7. *Gegevens met betrekking tot kwetsbare betrokkenen*

[24] Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking “waarschijnlijk een hoog risico inhoudt” in de zin van Verordening 2016/679, p. 10-13.
[25] Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking “waarschijnlijk een hoog risico inhoudt” in de zin van Verordening 2016/679, p. 13.

De verwerking van dit soort gegevens is een criterium vanwege de toegenomen machtsongelijkheid tussen de betrokkenen en de verwerkingsverantwoordelijke. Kwetsbare betrokkenen zijn bijvoorbeeld werknemers, kinderen, geesteszieken of asielzoekers.

8. *Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen*
   In de AVG wordt duidelijk gesteld dat het gebruik van een nieuwe technologie aanleiding kan geven tot de noodzaak om een GEB uit te voeren. Ook innovatieve toepassing kan tot een hoog risico leiden: bijvoorbeeld het gebruik van een intelligent video-analysesysteem om auto's te onderscheiden en nummerplaten automatisch te herkennen.[26]

9. *Wanneer als gevolg van de verwerking zelf betrokkenen een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of overeenkomst*
   Dit omvat verwerkingen die erop gericht zijn de toegang van betrokkenen tot een dienst of de mogelijkheid van betrokkenen om een overeenkomst aan te gaan toe te staan, te wijzigen of te verwijderen.

In de meeste gevallen zal voor een verwerking die aan twee criteria voldoet een GEB moeten worden uitgevoerd. In sommige gevallen kan een verwerkingsverantwoordelijke oordelen dat een verwerking die aan slechts een van deze criteria voldoet een GEB vereist.[27]

[26] Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679, p. 13.
[27] Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679, p. 13.