Zitting d.d. 12 maart 2024 te Rechtbank Den Haag

Inzake

STICHTING PRIVACY FIRST, gevestigd en kantoorhoudende te Amsterdam,

Eiseres,

Advocaten: mrs. L.J. Böhmer & S.E.J.P. van den Berg

tegen

DE STAAT DER NEDERLANDEN, zetelende te Den Haag,

Gedaagde,

Advocaten: mrs. C. Bitter en T. Gillhaus

1. ALGEMENE LIJN EUROPESE JURISPRUDENTIE

1.1 Zowel het Hof van Justitie als het EHRM hebben de afgelopen jaren in hun jurisprudentie enkele duidelijke vereisten geformuleerd wat betreft de inbreuk op grondrechten die zijn vervat in de artikelen 7 en 8 van het Europees Handvest en in artikel 8 van het EVRM in verband met opsporingsactiviteiten, namelijk de principes dat sprake moet zijn van een proportionele inbreuk en dat voldoende waarborgen, inclusief onafhankelijk toezicht, moeten bestaan om de inbreuk tot het strikt noodzakelijke te beperken. In dit kader noemen we in het bijzonder de door het EHRM gestelde eis van end-to-end safeguards. Wanneer artikel 126jj Sv en de wijze waarop de Staat hier uitvoering aan geeft langs deze maatstaven worden gelegd blijkt dat sprake is van schending van deze vereisten, met als gevolg dat artikel 126jj onverbindend is wegens strijd met het EVRM en het Europees Handvest. Op grond van deze regeling wordt namelijk op grote schaal gegevens vergaard, ongeacht of sprake is van enige connectie met misdaad, en zonder enig betekenisvol onafhankelijk toezicht op de verzameling en het gebruik van de gegevens.

1.2 Hoewel de Staat een 'margin of appreciation' heeft in het maken van een afweging tussen het publieke belang en het individuele belang betekent dit niet dat deze vrijheid van de Staat grenzeloos is. Uit rechtspraak van het EHRM volgt dat de 'margin of appreciation' grenzen kent, zowel bij het beoordelen of een maatregel daadwerkelijk proportioneel is als bij het vaststellen of voldoende waarborgen zijn ingericht om de inbreuk die een maatregel oplevert te beperken. Uit Big Brother Watch/VK[1] volgt in dat opzicht dat de beoordelingsruimte van een staat met betrekking tot het gebruik van een bulk-interceptiesysteem beperkt is, en dat bepaalde waarborgen bij een dergelijk systeem vereist zijn.

1.3 Voor we in meer detail zullen ingaan op de vereiste proportionaliteit en waarborgen, en de wijzen waarop de regeling niet voldoet, zullen we echter kort reageren op het standpunt van de Staat ten aanzien van de door Privacy First aangehaalde jurisprudentie. In het algemeen stelt de Staat in haar conclusie van antwoord dat deze jurisprudentie betrekking heeft op andere soorten gegevens en daarom minder relevant zou zijn. De jurisprudentie ziet met name op telecommunicatiegegevens, en in het bijzonder verkeers- en locatiegegevens zoals gedefinieerd in de e-privacyrichtlijn.

1.4 De Staat stelt terecht dat de ANPR-wetgeving niet onder de e-privacyrichtlijn valt en dat verzameling en gebruik van telecommunicatiegegevens niet aan de orde is. De e-privacyrichtlijn betreft echter gedeeltelijk een codificatie van vereisten met betrekking tot de bescherming van grondrechten die volgen uit het Handvest en

[1] R.o. 347.

jurisprudentie van het HvJ en EHRM, zoals mede blijkt uit considerans 2 van de richtlijn die expliciet verwijst naar de te respecteren grondrechten zoals opgenomen in het Handvest, artikel 7 en 8 in het bijzonder. Het standpunt dat de vereisten die gecodificeerd zijn in de e-privacyrichtlijn en die zijn geformuleerd in jurisprudentie over telecommunicatiegegevens enkel toepassing zouden vinden wanneer het gaat over het massaal verzamelen en gebruiken van telecommunicatiegegevens – en niet andere soorten gegevens – leidt tot een onbedoelde en onacceptabele inperking van de reikwijdte van deze vereisten. De in de aangehaalde jurisprudentie getrokken conclusies zijn daarom ook van toepassing op het massaal verzamelen, bewaren en gebruiken van andere soorten gegevens die in grote mate inzage kunnen geven in de levens van de personen die die gegevens betreffen.

1.5 Dat de gegevens die door de ANPR-camera's worden opgenomen een dergelijke grote mate van inzage kunnen opleveren moge duidelijk zijn. In haar betoog dat "kentekengegevens […] geen zeer nauwkeurige aanwijzingen [kunnen] verschaffen over het privéleven van degenen wier kentekengegevens […] worden bewaard"[2] miskent de Staat dat in een heel aanzienlijk aantal gevallen door de grote hoeveelheid camerabeelden wel degelijk in heel behoorlijke mate zal kunnen worden vastgesteld waar personen zich van dag tot dag begeven, zeker wanneer die personen, zoals ongeveer de helft van de Nederlandse bevolking, in de Randstad wonen. De inbreuk is des te ingrijpender nu veruit de meeste mensen die gefotografeerd worden hier niet van op de hoogte zullen zijn, en niet zullen weten dat deze foto's voor een langere periode in een centrale database worden opgeslagen. Dat de camera's zichtbaar zijn betekent niet dat voor iedereen die de camera's passeert duidelijk is wat er met die camera's precies gedaan wordt. Het cameraplan is weliswaar publiekelijk toegankelijk, maar is voor de gemiddelde Nederlander niet bekend en ziet enkel op de vaste camera's, niet de mobiele.

1.6 Op de gemaakte foto's zijn personen herkenbaar, en naast de foto zelf wordt ook de locatie waar de foto is genomen, het tijdstip en de datum opgeslagen. Ondanks dat op basis van alleen de gemaakte foto's personen meestal niet bij naam geïdentificeerd zullen kunnen worden, zal dit in de praktijk in het grootste deel van de gevallen heel gemakkelijk te doen zijn door na te gaan op wiens naam de auto waarin de gefotografeerde persoon zich bevindt geregistreerd is. Hoewel de Staat aangeeft dat inmiddels gebruik wordt gemaakt van geautomatiseerde blindering die inzittenden van voertuigen onherkenbaar zou moeten maken, wijst alles erop dat dit pas gebeurt op het moment dat de foto's daadwerkelijk worden opgevraagd, en niet op het

[2] Conclusie van Antwoord, rn. 4.4.5.

moment dat ze gemaakt of opgeslagen worden.[3] Daarnaast ziet deze blindering enkel op de personen die zich in het voertuig bevinden, en niet op eventuele anderen die zichtbaar zijn op de foto's.

1.7 Ook gaat de Staat eraan voorbij dat de inbreuk die op grond van de Wet ANPR plaatsvindt in sommige opzichten zelfs ingrijpender is dan de in de jurisprudentie besproken verzameling en bewaring van telecommunicatiegegevens. Daar ging het namelijk om gegevens die nog opgevraagd moesten worden door de overheid, en die tot die tijd werden opgeslagen door aanbieders van telecommunicatiediensten en -netwerken. In dit geval is de Staat echter niet alleen de partij die om inzage van de gegevens verzoekt, maar ook de partij die de gegevens bewaart voordat ooit een opvraag wordt gedaan. In dit opzicht verwijst Privacy First ook naar jurisprudentie van het EHRM, waaronder Rotaru/Roemenië[4] en Amann/Zwitserland[5] waaruit blijkt dat het enkele feit dat een overheid gegevens over een persoon bewaart, ongeacht of die gegevens vervolgens ook door die overheid worden gebruikt, al leidt tot een inbreuk van artikel 8 EVRM.

1.8 Enige maatregelen die ertoe zouden dienen om toegang door de overheid te beperken zijn kunstmatig. De overheid, specifiek de politie die belast is met een opsporingstaak, legt maatregelen aan zichzelf op en kan ervoor kiezen om die maatregelen niet na te leven, zonder dat enige andere partij dit door hoeft te hebben. De Staat geeft zelf in haar conclusie aan dat de inzet van ANPR-gegevens veelal een ondersteunend middel is, en vaak niet als bewijsmiddel wordt ingebracht. Dit leidt ertoe dat de inzet van ANPR-gegevens slechts in beperkte mate voor toetsing door een rechter in aanmerking zal komen, met een groter risico op misbruik tot gevolg.

1.9 Dat de Hoge Raad in 2014 al geoordeeld zou hebben dat het voor 7 dagen bewaren van ANPR-gegevens die zowel 'hits' als 'no-hits' bevatten toelaatbaar is, zoals de Staat stelt in haar Conclusie,[6] klopt niet. In het betreffende arrest[7] overweegt de Hoge Raad niet of de regeling van het bewaren van ANPR-gegevens in zijn geheel door

---

[3] Zie bijvoorbeeld kst-33542-O (Eerste Kamer, vergaderjaar 2022-2023), pagina 5: "Een voorbeeld van een verbeterpunt dat inmiddels is gerealiseerd is het gebruik van een algoritme dat op de ANPR-foto's de voorruiten van de voertuigen automatisch blindeert, zodat inzittenden niet meer zichtbaar zijn op de foto's die aan het Openbaar Ministerie worden verstrekt. Het blinderen was voorheen een handmatige handeling." Hieruit blijkt dat het automatisch blinderen in de plaats komt van het handmatig blinderen, dat pas plaatsvond bij raadpleging van de beelden, niet bij het verzamelen. Ook wordt aangegeven dat inzittenden niet meer zichtbaar zijn op de foto's die aan het OM worden verstrekt, niet op alle foto's. Zie in dit opzicht ook pagina 2 van de brief van de politie aan de Minister d.d. 22/11/2023 (Productie 1) (onderstreping advocaat): "De te verstrekken foto's worden sinds medio oktober 2022 geautomatiseerd geblindeerd."

[4] Case no. 28341/95, ro 46.

[5] Case no. 27798/95, ro 69.

[6] Rn. 3.1.2.

[7] ECLI:NL:HR:2014:3142.

de beugel kan, maar of door het gebruik van de ANPR-gegevens in het kader van een strafzaak sprake was van een onherstelbaar vormverzuim in de zin van artikel 359a Sv. Hierbij heeft de Hoge Raad enkel een toets uitgevoerd met het oog op de specifieke verdachte. In onderhavige zaak hebben we het echter niet over een specifiek geval waar de inbreuk op de rechten van een verdachte moeten worden afgewogen tegen het belang van de opsporing, maar over een landsbrede toepassing van een camerasysteem waarmee jan en alleman op dagelijkse basis gefotografeerd worden. Het arrest van de Hoge Raad is daarom niet relevant bij de beoordeling of dit systeem in zijn geheel toelaatbaar is. Zij heeft immers niet getoetst aan de verschillende vereisten die gelden voor een inbreuk middels een regeling zoals artikel 126jj, die ik nu in meer detail zal bespreken.

2. PROPORTIONALITEIT/NOODZAKELIJKHEID

2.1 Ten eerste stellen het HvJ en het EHRM[8] de eis dat de inbreuk proportioneel moet zijn en beperkt blijft tot het strikt noodzakelijke. Privacy First wijst in het bijzonder op de uitspraken van het HvJ in Digital Rights/Ierland en Tele2/Zweden, waarin het Hof onder meer overwoog dat het enkele algemene belang van publieke veiligheid onvoldoende is om de massale opslag van persoonsgegevens te rechtvaardigen.[9] Ook stelt het HvJ dat van belang is dat de verzameling en opslag van gegevens zoveel als mogelijk beperkt blijft tot personen die daadwerkelijk op enige wijze betrokken zijn bij illegale activiteit.[10]

2.2 In deze beide opzichten voldoet artikel 126jj niet. Op grond van dit artikel worden op massale schaal foto's gemaakt van personen in of rondom voertuigen die zich bevinden op de wegen waar camera's zijn geplaatst. Uit het in 2021 gepubliceerde WODC rapport blijkt dat destijds sprake was van 461 126jj-locaties, waar 919 vaste 126jj-camera's geplaatst waren[11], dus ruwweg 2 camera's per locatie. In het meest recent gepubliceerde cameraplan voor Q1 van 2024 worden omstreeks 900 locaties benoemd.

2.3 Volstrekt onduidelijk is hoeveel camera's daadwerkelijk geplaatst zijn, maar als we de in het WODC-rapport gepubliceerde cijfers als richtlijn kunnen nemen zijn naar verwachting 1800 vaste camera's geplaatst die dagelijks continu foto's maken van iedere auto die langskomt. Onduidelijk is nog hoeveel mobiele camera's in 2023 geplaatst zijn geweest, omdat dit nog niet publiekelijk bekend is gemaakt. Uit de

---

[8] Het algemene criterium dat volgens het EHRM een inbreuk op de grondrechten van artikel 8 EVRM proportioneel en strikt noodzakelijk in een democratische maatschappij moet zijn is onlangs wederom bevestigd in haar uitspraak in Podchasov/Rusland (13 februari 2024, Case no. 33696/19).

[9] ECLI:EU:C:2014:238 (Digital Rights/Ireland), ro 51; Joined Cases C-203/15 en C-698/15 (Tele2/Sverige), ro 103.

[10] Digital Rights/Ireland, ro 58 – 59; Tele2/Sverige, ro 105.

[11] WODC, Evaluatie ANPR-wetgeving 126jj Wetboek van Strafvordering, Cahier 2021-19, p. 9 (Productie 1 van de Staat).

over mobiele camera's gepubliceerde informatie blijkt echter dat het aantal locaties waar dergelijke camera's geplaatst zijn tussen 2021 en 2022 meer dan verdubbeld is, van 20 locaties in 2021 naar 47 in 2022.

2.4 Als deze trend zich in 2023 en 2024 heeft voortgezet, en met het oog op de kennelijke toename van het aantal geplaatste vaste camera's over de afgelopen jaren, is het aantal foto's dat gemaakt wordt van weggebruikers in Nederland sinds Privacy First haar dagvaarding heeft ingediend nog eens behoorlijk toegenomen. Hoeveel foto's precies gemaakt worden is onduidelijk, maar gezien de conclusie van het WODC dat in 2020 gemiddeld 5 miljoen passages per dag werden gefotografeerd en met inachtneming van de enorme toename van het aantal camera's sinds dat meetmoment moet het gaan om vele miljoenen foto's per dag. Er kan geen twijfel over bestaan dat hiermee sprake is van het massaal vergaren en opslaan van persoonsgegevens. De bewaartermijn van 4 weken doet hier niet aan af, nu er zo veel foto's gemaakt worden dat 4 weken ruim voldoende is om een enorme hoeveelheid te verzamelen. Het enkele feit dat publieke veiligheid van algemeen belang is rechtvaardigt een dergelijke massale inbreuk op de grondrechten van de vele mensen die door deze regeling worden gefotografeerd niet.

2.5 Uit de keuzes die gemaakt zijn bij het plaatsen van de camera's blijkt ook dat de Staat helemaal niet voor ogen heeft om te voorkomen dat zo weinig mogelijk personen die niks te maken hebben met eventuele te onderzoeken misdrijven worden gefotografeerd. Sterker nog, één van de drie redenen die de Staat volgens artikel 126jj kan aandragen om een camera te plaatsen is juist dat er zo veel mogelijk mensen passeren. Hieruit blijkt dat de regeling niet gericht is op het verzamelen van informatie die daadwerkelijk van concreet belang is voor opsporing, maar dat het doel van de regeling is om zoveel mogelijk gegevens te verzamelen, zonder acht te slaan op de mate van waarschijnlijkheid dat deze inbreuk enig nut heeft.

2.6 Dat de regeling in zijn algemeenheid voldoende nut heeft om de massale inbreuk op privacyrechten te rechtvaardigen blijkt allerminst. In haar conclusie van antwoord probeert de Staat weliswaar door middel van enkele voorbeelden een dergelijk nut aan te tonen, maar dat is ook waar het bij blijft: voorbeelden. Informatie over de daadwerkelijke mate waarin art. 126jj leidt tot effectievere opsporing blijft uit. Ter onderbouwing van het nut van de regeling haalt de Staat onder meer het inmiddels behoorlijk gedateerde WODC-onderzoek uit 2021 aan. Opmerking verdient dat de politie zelf een belangrijke rol speelde in de selectie van de zaken die het WODC heeft onderzocht. Uit de toelichting op de zaakselectie blijkt dat 1 op de 3 door het

WODC onderzochte zaken zijn aangedragen door de politie zelf.[12] Ook hebben in meerdere gevallen waarin het WODC zelf zaken wilde selecteren op basis van een aselecte steekproef betrokkenen geweigerd om mee te werken met het onderzoek. Een vertekenend effect op enige positieve resultaten van het onderzoek valt hierdoor niet uit te sluiten.

2.7 De conclusies van het onderzoek zijn overigens wat minder rooskleurig dan door de Staat geschetst. Volgens het onderzoek wordt de via 126jj verkregen informatie veelal "gebruikt als 'plusje' om verder richting te geven aan een onderzoek".[13] Het WODC concludeert verder dat de bevoegdheid slechts "in enkele gevallen" doorslaggevende informatie opleverde. Dat de regeling in een zodanig beperkte mate daadwerkelijk wat oplevert maakt dat de massale inbreuk op privacyrechten niet gerechtvaardigd wordt.

3. ONAFHANKELIJKE TOETSING

3.1 Als onderdeel van de vereisten op het vlak van proportionaliteit en noodzakelijkheid in het algemeen zijn in de jurisprudentie van het HvJ en het EHRM ook eisen gesteld aan de waarborgen die nodig zijn om te verzekeren dat bij ieder afzonderlijk gebruik van een bevoegdheid de inbreuk beperkt blijft tot het strikt noodzakelijke. Dergelijke waarborgen moeten in het nationaal recht verankerd zijn. In o.a. het Prokuratuur-arrest[14] is in dit kader bevestigd dat toegang van de bevoegde nationale instanties tot verkeers- en locatiegegevens wordt onderworpen aan voorafgaande toetsing door een rechterlijke instantie of een onafhankelijke bestuurlijke entiteit. De 126jj-regeling voldoet in dit opzicht niet.

3.2 Zoals al eerder uiteengezet is Privacy First van mening dat het op grote schaal maken en opslaan van foto's middels ANPR-camera's een inbreuk van een vergelijkbare orde is. Hierbij geldt ook dat voor de eerste door de Staat begane inbreuk ten aanzien van de gemaakte foto's, namelijk het zelf opslaan en bewaren hiervan, überhaupt geen vorm van controle bestaat. Pas op het moment dat de tweede inbreuk, namelijk de raadpleging van de foto's, plaatsvindt, is sprake van enige toetsing, namelijk door een OvJ.

3.3 Het Hof overweegt in Prokuratuur dat een openbaar ministerie dat betrokken is bij het onderzoek en optreedt als openbaar aanklager niet kan functioneren als een

[12] Uit pagina 26 e.v. valt op te maken dat in totaal 7 door het WODC onderzochte zaken zijn aangedragen door de politie. 4 zaken zijn door het WODC geselecteerd uit 10 door politie-eenheden aangedragen zaken. 2 zaken zijn "spontaan aangedragen' tijdens interviews met functionarissen van de politie". In 1 geval is door de politie een alternatieve zaak voorgesteld (en gebruikt) nadat in een door het WODC zelf geselecteerde zaak medewerking werd geweigerd. Uit bijlage 5 bij het onderzoek blijkt dat 21 zaken zijn onderzocht door het WODC.

[13] Evaluatie ANPR-wetgeving 126jj Wetboek van Strafvordering, Cahier 2021-19, WODC, p. 83.

[14] Zie ook Digital Rights/Ireland, ro 62; Tele2/Sverige, ro 120

onafhankelijke partij in het kader van de vereiste toetsing.[15] Dat het gebruikelijk is in het Nederlandse strafrecht dat een officier van justitie, en niet een rechter, in veel gevallen toetst of een bepaalde bevoegdheid ingezet mag worden doet niet af aan de conclusies van het Hof dat waar het gaat om ingrijpende inbreuken een onafhankelijke toets nodig is, en dat het openbaar ministerie deze niet kan uitvoeren. Dat kritisch gekeken moet worden naar de mate waarin het OM in staat moet worden geacht om een effectieve toets uit te voeren is recentelijk gebleken in de zaken omtrent Box Consultants[16] en Weski[17], waar in beide gevallen het OM een flinke tik op de vingers kreeg vanwege het schenden van het verschoningsrecht.

3.4 In het kader van het standpunt van de Staat dat een officier van justitie die niet is betrokken bij het betreffende strafrechtelijke onderzoek zou kunnen fungeren als een onafhankelijke bestuurlijke entiteit wijst Privacy First op het feit dat uit de Box-zaak is gebleken dat precies zo een constructie niet werkt, en dat ook een zogenaamd onafhankelijke officier van justitie vatbaar is voor beïnvloeding door collega's die wel belast zijn met het strafrechtelijke onderzoek.[18] Dit bevestigt dat een officier van justitie vanwege de aard van haar functie en de positie waarin zij verkeert nooit echt, zoals genoemd in het Commissioner arrest van het Hof van Justitie, "neutraal […] ten opzichte van de partijen in de strafprocedure" kan zijn.[19]

3.5 Ook de Raad van State heeft in haar advies over de vaststelling van het nieuwe Wetboek van Strafvordering gesignaleerd dat het Prokuratuur-arrest bredere implicaties heeft dan alleen ten aanzien van de vordering van telecommunicatiegegevens. De Raad van State stelt vast dat voor het vorderen van locatie- en verkeersgegevens naar aanleiding van dit arrest een rechterlijke machtiging vereist is, waar op grond van zowel het huidige als het toekomstige Wetboek van Strafvordering voor inbreuken die vergelijkbaar of meer ingrijpend zijn een bevel van een officier van justitie nog volstaat. De Raad van State adviseert de Staat daarom om te overwegen in hoeverre het Prokuratuur-arrest zou moeten leiden tot een herijking van de normering van opsporingsbevoegdheden.[20] Kortom: de stelling dat het vereiste van onafhankelijke voorafgaande toetsing alleen van toepassing zou zijn op verkeers- en locatiegegevens gaat niet op.

---

[15] C-746/18 (Prokuratuur), ro. 55

[16] ECLI:NL:GHDHA:2023:298

[17] ECLI:NL:RBDHA:2023:10541

[18] Zie voor meer context bijvoorbeeld het artikel van NRC d.d. 14 januari 2022 – 'Strafzaak tegen vermogensbeheerder kantelt: hoe fout zat opsporing zelf?' (https://www.nrc.nl/nieuws/2022/01/14/staatsspeurders-naar-fraude-nu-opeens-zelf-aangeklaagd-a4079332#photo=LTE1NDk)

[19] HvJ 5 april 2022, C-140/20 (Commissioner), ro. 108.

[20] Kamerstukken II 2022/23, 36327, nr. 4, Deeladvies C onder 3 (c).

3.6 Het standpunt van de Staat dat onafhankelijk toezicht door de Autoriteit Persoonsgegevens en de Inspectie Justitie en Veiligheid plaats zou vinden snijdt ook geen hout. Het betreffen slechts zeer algemene toezichtstaken die niet gericht zijn op de specifieke uitvoering van artikel 126jj. Dit blijkt mede uit het WODC-rapport, waarin wordt aangegeven dat beide toezichthouders "126jj niet als specifiek onderwerp behandelen in hun onderzoeksprogramma's".[21] De toezichthouders geven richting het WODC aan geen signalen te hebben ontvangen die gericht onderzoek naar de werkwijze van 126jj volgens hen nodig maken. Het WODC concludeert dat er een kans bestaat dat mogelijke problemen niet worden opgemerkt die wel zouden opduiken bij gericht toezicht. Voor zover Privacy First bekend hebben de toezichthouders ook in de nog nader te bespreken afkeurende KPMG-audits geen noodzaak gezien om enigszins gericht toezicht te houden. Van enig consistent en inhoudelijk toezicht is dan ook geen sprake.

4. END-TO-END SAFEGUARDS

4.1 Onafhankelijke toetsing is slechts 1 van de waarborgen die volgens jurisprudentie van het HvJ en het EHRM worden vereist. In o.a. Privacy International benadrukt het Hof van Justitie nog eens dat het belang van waarborgen die in het recht verankerd zijn extra groot is waar het geautomatiseerde verwerking van gegevens betreft, omdat er bij dergelijke verwerkingen een groter risico bestaat op ongeautoriseerde toegang.[22] In Big Brother Watch and Others/VK en Centrum för Rättvisa/Zweden[23] zet het EHRM uiteen welke waarborgen in de wet opgenomen moeten zijn in geval van de massale ongedifferentieerde preventieve interceptie van gegevens. Het EHRM stelt de eis dat end-to-end safeguards worden geïmplementeerd. In brede zin betekent dit dat ieder onderdeel van een systeem wordt beoordeeld op subsidiariteit en proportionaliteit, en dat de interceptie vanaf het begin onderworpen is aan onafhankelijke autorisatie en onafhankelijk toezicht.

4.2 We hebben reeds besproken dat geen sprake is van onafhankelijk toezicht in het kader van de toegang van de overheid tot de gegevens en dat de massale verzameling van gegevens niet proportioneel is. Ook in andere opzichten voldoet 126jj en de onderliggende regelgeving niet, waaronder de specifieke vereisten dat de interceptie in duur beperkt is, dat de maatregel beperkt wordt tot specifieke categorieën personen, en dat procedures worden vastgesteld voor het onderzoek, gebruik en de opslag van de gegevens.[24] De interceptie is niet in duur beperkt, want de inzet van de

[21] WODC, Evaluatie ANPR-wetgeving 126jj Wetboek van Strafvordering, Cahier 2021-19, p. 92 (Productie 1 van de Staat).

[22] C-623/17 (Privacy International), ro. 68.

[23] Big Brother Watch and Others/VK, case nos. 58170/13, 62322/14 en 24969/15; Centrum för Rättvisa/Zweden, case no. 35252/08

[24] Zie Big Brother and Others/VK, ro. 349.

vaste camera's is niet tijdsgebonden. De maatregel is niet beperkt tot specifieke categorieën personen, maar treft in potentie iedereen in Nederland. En procedures over de opslag en het gebruik van de gegevens zijn in slechts zeer beperkte mate vastgelegd in artikel 126jj en de onderliggende regelgeving.

4.3 Zo wordt in het Besluit[25] weliswaar genoemd dat de toegang tot Argus beperkt moet zijn tot enkel geautoriseerde opsporingsambtenaren die niet bij het onderzoek betrokken zijn. De controle hierop schiet echter tekort, zo blijkt uit de auditrapporten van KPMG over 2021[26] en over 2022[27]. Toegang tot het systeem wordt weliswaar gelogd, maar die logging wordt vervolgens niet daadwerkelijk gemonitord, waardoor ongeautoriseerde toegang niet wordt opgemerkt. Ook blijkt uit de audits dat deze logging muteerbaar is, en daarmee geen betrouwbaar beeld geeft van wie toegang heeft verkregen.

4.4 Verdere enigszins specifieke eisen aan de beveiliging zijn niet vastgelegd in enig besluit of regeling. De Staat verwijst naar waarborgen die zijn opgenomen in de Wpg en de Politiewet, zoals het vereiste dat bij de verwerking van politiegegevens passende technische en organisatorische maatregelen worden genomen. Onduidelijk is overigens op welk moment de door ANPR-camera's gemaakte foto's precies binnen het bereik van de Wpg vallen doordat zij politiegegevens worden, in plaats van de gebruikelijke persoonsgegevens in de zin van de AVG. Zo lang als de foto's enkel opgeslagen zijn en niet zijn opgevraagd in het kader van een opsporingsonderzoek is het immers de vraag of zij worden verwerkt in het kader van de uitvoering van de politietaak. Privacy First is benieuwd hoe uw rechtbank hier tegenaan kijkt.

4.5 Effectief toezicht op de inhoud en naleving van de door de Wpg vereiste technische en organisatorische maatregelen ontbreekt hoe dan ook. In de zojuist al aangehaalde door KPMG uitgevoerde audits wordt niet getoetst aan een onafhankelijk ontwikkelde en internationaal erkende standaard, maar aan het door de politie zelf opgestelde 'Privacy Control Framework 126jj'. Het framework ziet alleen op Argus zelf. Er wordt met geen woord gerept over hoe risico's op ongeautoriseerde toegang tot de ANPR-camera's zelf en het pad dat de foto's afleggen om via die camera's in Argus opgeslagen te worden, worden afgedekt. In dit opzicht blijft Privacy First in het duister tasten.

---

[25] Besluit vaststelling nadere regels vastleggen en bewaren kentekengegevens ex artikel 126jj Wetboek van Strafvordering door politie.

[26] Productie 2 bij de Conclusie van Antwoord van de Staat.

[27] Productie 1 van Privacy First.

4.6 Het framework bevat qua beveiliging van Argus zelf niet bepaald vergaande eisen. Zo stelt de politie in het framework onder meer de volgende eis: "alle wijzigingen in apparatuur, software of procedures die de beveiliging van de gegevens en informatie kunnen beïnvloeden zijn bekend en beoordeeld door of namens de verwerkingsverantwoordelijke als zijnde aanvaardbaar"[28]. De verwerkingsverantwoordelijke bij de politie is volgens artikel 1 van het Besluit de korpschef van de politie. Met andere woorden: de politie moet op de hoogte zijn van de wijzigingen die de beveiliging kunnen beïnvloeden die door de politie zelf zijn uitgevoerd, en de politie beoordeelt vervolgens of deze wijzigingen aanvaardbaar zijn.

4.7 Zelfs nu de politie zelf bepaalt aan welke maatstaven getoetst wordt, is zij er nog niet in geslaagd om een audit positief af te sluiten. In zowel 2021 als in 2022 heeft KPMG een afkeurend oordeel gegeven. Gesignaleerde tekortkomingen over 2022 betreffen de eerder genoemde gebrekkige controle en beveiliging van ongeautoriseerde toegang, de verstrekking van foto's waarop kenmerken onvoldoende onherkenbaar zijn gemaakt, de verstrekking van foto's die niet voldoen aan de daadwerkelijke zoekvraag, het niet binnen 3 dagen opvolgen van een telefonisch bevel met een schriftelijk bevel, en het niet juist documenteren van een zoekvraag en de hierbij gevonden resultaten. Ook zijn wijzigingen in de Argus-programmatuur die de beveiliging van gegevens en informatie kunnen beïnvloeden niet voldoende vastgelegd.

4.8 De Staat heeft in haar Conclusie allerlei beloften gedaan over in te voeren maatregelen, maar het feit dat een externe auditor op basis van een niet bijzonder strenge toets 2 jaar op rij heeft moeten concluderen dat het systeem niet voldoet stemt weinig hoopvol. Ook blijkt uit een verslag voor de Eerste Kamer dat verdere audits niet zullen worden uitgevoerd door een externe auditor zoals KPMG, maar door de afdeling concernaudit van de politie zelf.[29] Er zal dus geen enkele onafhankelijke controle meer plaatsvinden ten aanzien van de implementatie van deze beloofde verbeteringen.

4.9 Ter samenvatting: de politie stelt slechts voor een deel van de keten waarin door ANPR-camera's gemaakte foto's worden verwerkt eisen aan de technische en organisatorische maatregelen voor beveiliging. De politie stelt zelf de eisen waarop gecontroleerd wordt, en legt de lat hierbij laag. Desondanks is de politie er de afgelopen jaren niet in geslaagd om te voldoen aan de door haar zelf gestelde minimumvereisten. Voor zover verdere verbetermaatregelen beloofd zijn geldt dat

[28] Productie 1 van Privacy First, p. 13 onder CHM.02.

[29] Kst-33542-O (Eerste Kamer, vergaderjaar 2022-2023), pagina 11.

hierover geen enkele vorm van onafhankelijke controle zal plaatsvinden, nu de Staat heeft besloten om - naast het uitvoeren van de regeling en het stellen van de eisen aan deze uitvoering - ook de toekomstige audits bij de politie te beleggen. Een duidelijker voorbeeld van het adagium 'de slager keurt zijn eigen vlees' is lastig te bedenken.

5. OPMERKINGEN STAAT MBT FORMULERING VORDERINGEN

5.1 Naast haar inhoudelijke verweren heeft de Staat ook enkele opmerkingen gemaakt ten aanzien van de formulering van de vorderingen van Privacy First. Ten eerste geeft de Staat aan dat onvoldoende duidelijk is welke bepalingen uit de bij of krachtens artikel 126jj Sv gestelde regels met welk eenieder verbindende bepaling van hoger recht onverenigbaar zou zijn. Privacy First is van mening dat artikel 126jj Sv en de daarop gebaseerde regelingen in het geheel onverenigbaar zijn met artikel 8 van het EVRM en artikel 7 en 8 van het Europees Handvest. Het is namelijk het geheel van het systeem dat volgt uit artikel 126jj en de daarop gebaseerde regelingen, zowel de bevoegdheden als de gestelde waarborgen, dat niet voldoet aan de op grond van deze artikelen gestelde eisen.

5.2 Ook stelt de Staat dat zowel de primaire als subsidiaire vorderingen te algemeen omschreven zouden zijn omdat gebruik is gemaakt van de woorden "en/of". Privacy First is van mening dat het gebruik van en/of normaal taalgebruik betreft en dat voor eenieder, inclusief de rechtbank, duidelijk is dat Privacy First hiermee aangeeft dat zij de rechtbank verzoekt om bij voorkeur alle vorderingen, en anders een deel daarvan, toe te wijzen.

5.3 Daarnaast geeft de Staat ten aanzien van de primaire vordering aan dat onvoldoende duidelijk zou zijn wat Privacy First bedoelt met "enig gegeven toevoegen aan het databastand (of databestanden) die zijn gebaseerd op artikel 126jj Sv en daarop gebaseerde besluiten en regelingen". Voor zover nodig verduidelijkt Privacy First bij deze graag dat hiermee wordt gedoeld op enig databestand, zoals Argus, waar de gegevens die volgens artikel 2 van de Regeling[30] worden verzameld worden opgeslagen, en niet op enige logging die wordt bijgehouden in verband met beveiligingsmaatregelen.

5.4 Ten slotte stelt de Staat dat zowel de primaire als subsidiaire vorderingen gedeeltelijk zien op bevoegdheden die worden uitgevoerd door de politie, namelijk het verzamelen van gegevens en het toevoegen van gegevens aan databestanden. In dat kader wenst Privacy First te verduidelijken dat de politie weliswaar een afzonderlijke rechtspersoon is, maar dat de politie desalniettemin onder het rechtstreekse gezag

[30] Regeling technische vereisten ANPR-camera's en het centrale opslagsysteem

van de Staat valt. Dit blijkt onder meer uit artikel 27 van de Politiewet, waarin wordt aangegeven dat de korpschef – die belast is met de leiding en het beheer van de politie, en tevens als verwerkingsverantwoordelijke is aangemerkt met betrekking tot de verwerkingen van gegevens in het kader van de inzet van 126jj – over de uitoefening van zijn taken en bevoegdheden verantwoording aflegt aan de Minister van Justitie en Veiligheid. Ook blijkt uit artikel 31 Pw dat de Minister de korpschef algemene en bijzondere aanwijzingen kan geven met betrekking tot de uitoefening van diens taken en bevoegdheden. Voor zover uw rechtbank van mening is dat het verbieden van de Staat om enige handelingen uit te voeren die specifiek worden uitgevoerd door de politie niet kan leiden tot een effectief verbod op die handelingen verzoekt Privacy First uw rechtbank om de vorderingen zo te lezen dat de Staat geboden wordt om een dergelijk verbod feitelijk in effect te brengen door middel van haar gezag over de politie.

6. SLOT

6.1 Het voorgaande leidt tot de volgende conclusie: Artikel 126jj en de onderliggende regelgeving is inherent in strijd met de door het Unierecht en het EVRM beschermde grondrechten, en is daarom onverbindend. De inbreuk vindt plaats op een zodanig massale schaal dat deze niet goed te praten is. Het gaat over miljoenen foto's op dagelijkse basis, zonder dat enig onderscheid wordt gemaakt tussen de surveillance van criminelen en van burgers die toevallig langs komen rijden, fietsen of lopen. Dit alles ten behoeve van een opbrengst die op zijn zachtst gezegd mager is, zeker wanneer men overweegt dat de betrouwbaarheid van de bronnen waarop de Staat zich ter onderbouwing van het beweerdelijke nut van de regeling baseert twijfelachtig is.

6.2 Een zodanig massale inbreuk valt eigenlijk al niet meer te rechtvaardigen, maar zelfs als dat had gekund is gebleken dat de getroffen waarborgen om te verzekeren dat de inbreuk zoveel als mogelijk beperkt blijft ernstig tekort schieten. Voor zover in de wetgeving überhaupt waarborgen te vinden zijn is gebleken dat op geen enkel punt sprake is van effectief onafhankelijk toezicht. En zelfs nu de politie zelf de eisen heeft mogen stellen aan de technische en organisatorische maatregelen ter beveiliging van de gevoelige gegevens slaagt zij er niet in om aan deze eisen te voldoen.

6.3 In het licht van het voorgaande verzoekt Privacy First uw rechtbank primair om artikel 126jj Sv en de daarop gebaseerde regelgeving onverbindend te verklaren. Subsidiair verzoekt Privacy First uw rechtbank om de Staat te verbieden om nog verder kentekengegevens te verzamelen of om deze nog verder te raadplegen totdat het systeem voldoet aan de door het EVRM en Handvest gestelde eisen.

28 februari 2024

Behandeld door	: S. E. J. P. van den Berg
Correspondentie	: 94700, NL-1090 GS Amsterdam
Telefoon	: +31 20 301 63 51
Fax	: +31 20 301 63 33
E-mail	: fietje.vandenberg@cms-dsb.com
Referentie	: SEJPvdB/2024/0035