DAGVAARDING COLLECTIEVE ACTIE

Heden, de …… tweeduizend drieëntwintig , ten verzoeke van de **Stichting Privacy First**, hierna te noemen: "**Privacy First**", gevestigd en kantoorhoudende te Nieuwe Herengracht 49 (1011 RN) Amsterdam, in deze zaak woonplaats kiezende te Amsterdam aan de Parnassusweg 737 (1077) DG Amsterdam), op het kantoor van de naamloze vennootschap CMS Derks Star Busmann N.V. van welk kantoor mr. L.J. Böhmer als advocaat wordt gesteld en als zodanig zal optreden met het recht van substitutie;

Heb ik,

GEDAGVAARD:

De Staat der Nederlanden (het Ministerie van Justitie en Veiligheid), hierna te noemen: "**De Staat**", zetelende te (2511 DP) Den Haag aan de Turfmarkt 147, ex art. 48 Rv mijn exploot doende aan het parket van de Procureur-Generaal bij de Hoge Raad der Nederlanden, (2511 EK) aan de Korte Voorhout 8 en aldaar afschrift dezes latende aan:

OM:

Op tweeduizend drieëntwintig, om niet in persoon, maar vertegenwoordigd door een advocaat te verschijnen voor de rechtbank Den Haag, sector civiel, welke zitting alsdan aldaar wordt gehouden in één der zalen van het Paleis van Justitie aan de Prins Clauslaan 60, 2595 AJ te Den Haag;

MET AANZEGGING:

(1) dat indien gedaagde niet vertegenwoordigd door een advocaat op de terechtzitting verschijnt en de voorgeschreven termijnen en formaliteiten in acht zijn genomen, de rechter verstek tegen gedaagde zal verlenen en de hierna omschreven vordering zal toewijzen, tenzij deze hem onrechtmatig of ongegrond voorkomt;

(2) dat bij verschijning in het geding van gedaagde een griffierecht zal worden geheven, te voldoen binnen vier weken te rekenen vanaf het tijdstip van verschijning;

(3) dat de hoogte van de griffierechten is vermeld in de meest recente bijlage behorend met locatie en tijdgegevens bij de Wet griffierechten burgerlijke zaken, die onder meer is te vinden op de website: www.kbvg.nl/griffierechtentabel;

(4) dat van een persoon die onvermogend is, een bij of krachtens de wet vastgesteld griffierecht voor onvermogenden wordt geheven, indien hij op het tijdstip waarop het griffierecht wordt geheven heeft overgelegd:

   (a) een afschrift van het besluit tot toevoeging, bedoeld in artikel 29 van de Wet op de rechtsbijstand, of indien dit niet mogelijk is ten gevolge van omstandigheden die redelijkerwijs niet aan hem zijn toe te rekenen, een afschrift van de aanvraag, bedoeld in artikel 24, tweede lid, van de Wet op de rechtsbijstand, dan wel

   (b) een verklaring van het bestuur van de raad voor rechtsbijstand, bedoeld in artikel 7, derde lid, onderdeel e, van de Wet op de rechtsbijstand waaruit blijkt dat zijn inkomen niet meer bedraagt dan de inkomens bedoeld in de algemene maatregel van bestuur krachtens artikel 35, tweede lid, van die wet;

(5) dat Privacy First op straffe van niet-ontvankelijkheid verplicht is deze dagvaarding aan te tekenen in het centraal register voor collectieve acties als bedoeld in artikel 305a, zevende lid, van Boek 3 van het Burgerlijk Wetboek;

(6) dat deze aantekening tot gevolg heeft dat – tenzij de rechtbank Privacy First aanstonds niet ontvankelijk verklaart – de rechtbank de zaak aanhoudt totdat een termijn van drie maanden na de aantekening in het centraal register is verstreken;

(7) dat na het verstrijken van deze termijn de behandeling van de zaak wordt voortgezet in de stand waarin zij zich bevindt, tenzij ingevolge artikel 1018d, tweede lid, Rv deze termijn is verlengd of een andere collectieve vordering voor dezelfde gebeurtenis is ingesteld; dat de in artikel 128, tweede lid, Rv bedoelde roldatum voor het nemen van de conclusie van antwoord door de rechtbank zal worden bepaald op een termijn van zes weken nadat de in artikel 1018c, derde lid, Rv bedoelde termijn is verstreken;

1. SAMENVATTING: ARTIKEL 126 JJ STRAFVORDERING (SV) KENNELIJK ONVERBINDEND WEGENS STRIJD MET EUROPEES RECHT

1.1 De per 1 januari 2019 in werking getreden wet inzake de invoering van artikel 126 JJ Sv en de daarop gebaseerde regelgeving vormt de basis voor een databestand van miljoenen verzamelde en opgeslagen (digitale) foto's van onder meer kentekenplaten met vermelding van tijd en plaats in Nederland. Doel van deze regelgeving: het opsporen van voortvluchtige personen en van ernstige strafbare feiten.

1.2 De gegevens zijn voornamelijk afkomstig van camera's van de politie en van de Koninklijke Marechaussee. De camera's zijn onder te verdelen in vaste camera's en mobiele camera's.

1.3 In theorie worden de gegevens 4 weken in het databestand bewaard. De opsporingsdiensten mogen zonder enige onafhankelijke toetsing het databestand raadplegen via een verzoek aan een aantal geselecteerde agenten. Die agenten beoordelen of het raadplegingsverzoek voldoet aan een aantal vormvereisten. Vervolgens verstrekken de agenten de gevraagde gegevens, als de gegevens in het databestand voorkomen. In theorie worden de gegevens na 4 weken (automatisch) verwijderd, tenzij een gegeven geraakt is door een raadplegingsverzoek.

1.4 Het systeem omvat vier fasen:

1.4.1 Verzamelen van de foto's (miljoenen per maand)

1.4.2 Het opslaan van de foto's in een digitaal bestand (4 weken)

1.4.3 Het bewerken van de foto's ("blurren"/bewerken en linken met datum en tijd en locatie)

1.4.4 Het "automatisch" verwijderen van de informatie uit het databestand.

1.5 Ieder van de vier fasen bestaat uit een volstrekt ondoorgrondelijk en ongecontroleerd proces waarbij op geen enkele kenbare wijze de veiligheid, de rechtmatigheid of de mensenrechten zijn geborgd.

1.6 Recente perspublicaties en bevindingen van het WODC in rapportages[1] melden misbruik en misstanden bij het gebruik van de foto's en de informatie.

1.7 Zo verhaalt het NRC op 11 augustus 2021 naar aanleiding van het WODC-rapport van september 2020 dat het OM in strijd met de wet gebruik probeert te maken van "onbewerkte" foto's[2]

1.8 Inmiddels heeft de politie in 2021 juist gepleit voor meer gebruik van de onbewerkte foto's (in strijd met de wet).[3]

1.9 Sinds 2019 heeft het gebruik van systeem nog niet een keer geleid tot opsporing en aanhouding van een voortvluchtige of oplossing van een ernstig misdrijf.

---

[11] WODC rapport Cahier 2020-13 "Het gebruik van bewaarde kentekengegevens in de opsporing de wet 'vastleggen en bewaren van kentekengegevens door de politie' een jaar in werking en Cahier 2021-19 Evaluatie ANPR-wetgeving 126jj Wetboek van Strafvordering.

[2] NRC 11 augustus 2021 "OM vroeg foto's passagiers op zonder wettelijke ruimte"

[3] NRC 30 augustus 2021 Politie wil kentekenfoto gebruiken voor opsporing"

1.10 Het systeem van artikel 126 JJ Sv is om meerdere redenen kennelijk onverbindend wegens strijd met:

- artikelen 16, 21, 67 VWEU,
- artikelen 7 en 8 van het Europees Handvest en
- artikel 8 van het Europees Verdrag voor de rechten van de mens (EVRM).

1.11 Vanwege onder meer de volgende elementen:

- Schending van het noodzakelijkheidsvereiste
- Schending van het proportionaliteitsvereiste
- Onvoldoende bescherming tegen het inherente risico van misbruik
- Ontbreken van onafhankelijke toetsing op de werking van het systeem als geheel en op de raadplegingsaanvraag van/namens de officier van justitie
- De status van de originele digitale foto's en de bewerkingen van de foto's voor opslag is niet geregeld, hetgeen misbruik in de hand werkt (hetgeen ook al is gebeurd)[4]
- Geen enkele controle op de beweerde vernietiging van de opgeslagen data na afloop van de vier weken
- Geen onafhankelijke evaluatie van (de werking van) het systeem van foto tot vernietiging
- De gepubliceerde cameraplannen voldoen niet aan de wettelijke vereisten, waardoor de controle op het gebruik wordt gereduceerd.
- Effectiviteit nul/ geen meerwaarde aangetoond na drie jaar werking
- Schending van het vereiste van "End-to-End Safeguards" zoals omschreven in de jurisprudentie van het Hof
- Schending van het vereiste van voorzienbaarheid en legaliteit

[4] Pagina 84 WODC rapport Cahier 2020-13 "Het gebruik van bewaarde kentekengegevens in de opsporing" De wet 'vastleggen en bewaren van kentekengegevens door de politie' een jaar in werking : *Vanuit de opsporing bestaat er dus een wens om in bepaalde gevallen gebruik te kunnen maken van de oorspronkelijke (ongeblurde) foto 's. Doordat de foto 's pas in een later stadium onherkenbaar worden gemaakt leidt dit soms tot dilemma's. Sommige zaken zijn zo ernstig dat vanuit politie en OM toch wordt geprobeerd de oorspronkelijke foto 's te krijgen. Er zijn enkele voorbeelden waarbij een foto, die mogelijk tot de dader zou kunnen leiden, geblurd werd aangeleverd. Verschillende respondenten geven aan dat dit tot discussie leidde met de officier van justitie die de originele foto 's wilde ontvangen. In sommige gevallen werd geprobeerd de foto 's via andere BOB-middelen te vorderen zoals 126nd Sv. In één zaak zijn ook daadwerkelijk de originele foto 's verkregen.*
Voor een ander geval van misbruik zie beschrijving in paragraaf 8.6.1 van rapport: *Vervolgens is handmatig in deze beelden gezocht naar het model en type voertuig.*

1.12 Privacy First vordert in essentie primair buiten werkingstelling van de per 1 januari 2019 in werking gestelde artikel 126 JJ Sv ("de wet") en verwijdering van de op grond van de wet verzamelde gegevens.

1.13 Subsidiair vordert Privacy First opschorting van de mogelijkheid tot raadpleging van de gegevens door een opsporingsambtenaar.

2. HET SYSTEEM VAN ARTIKEL 126 JJ SV: VERZAMELING, BEWARING EN RAADPLEGING VAN ANPR PERSOONSGEGEVENS

2.1 Een kenteken wordt aangemerkt als een persoonsgegeven. Een (bewerkte) foto van een (auto met) kentekenplaat met vermelding van locatie, tijd en plaats (“ANPR") geldt zeker als een persoonsgegeven. De gegevens zijn herleidbaar tot de bestuurder van de auto (en tot de andere personen op de foto).

2.2 Doel van artikel 126 JJ Sv is het verzamelen van miljoenen foto's per dag in een databestand, dat de opsporingsdiensten zonder enige onafhankelijke toetsing kunnen raadplegen om te achterhalen welke persoon op enig moment op welke plaats was.

2.3 Het systeem van artikel 126 JJ bestaat uit het wetsartikel, een aantal besluiten waaronder het besluit van 5 december 2018 tot vaststelling tot nadere regels voor het vastleggen en bewaren van kentekengegevens op grond van artikel 126 JJ Sv door politie in werking getreden[5] ('het besluit') en diverse regelingen.

2.4 Naast de wet en het besluit heeft de minister bij besluit autorisatie raadplegen kentekengegevens een beperkt aantal opsporingsambtenaren geautoriseerd (hierna: "de agenten') om de centrale opslag te raadplegen.

2.5 De minister heeft het cameraplan van de nationale politie ten behoeve van artikel 126 JJ wetboek van Strafvordering gepubliceerd.

2.6 Verder heeft de minister op 21 december 2018 een regeling gepubliceerd met de technische vereisten voor de camera's en het centrale opslagsysteem[6].

2.7 Overzicht van de structuur van de regeling van artikel 126 JJ Sv:

(a) Wet;

(b) Besluit vastleggen en bewaren:

(c) Besluit cameraplan

(d) Besluit geautoriseerde agenten

5 *Stb.* 2018, 472

6 Staatscourant 2018 nr.72191, d.d. 21 december 2018

(e) Regeling

2.8 Doel van het systeem is officieel:

- het opsporen van voortvluchtige personen, en
- het opsporen en vervolgen van ernstige strafbare feiten.

2.9 Deze doelen moeten worden behaald door het verzamelen, bewaren en raadplegen van ANPR-gegevens, foto's van auto's met kentekens, die de politie en de Koninklijke Marechaussee elke dag verzamelen via vaste en mobiele camera's.

2.10 Per dag verzamelt men tussen de 4 en de 5 miljoen foto's. Dat zijn 28-35 miljoen foto's per week, en 108-130 miljoen foto's per maand.[7] Het betreft hier gewone onbewerkte foto's.

2.11 De foto's worden zonder adequate basis onbewerkt opgeslagen Die ANPR-gegevens worden in een gezamenlijk databestand van politie en Koninklijke Marechaussee opgeslagen, De verantwoordelijken voor het systeem zijn de minister van Justitie en Veiligheid en de commandant van de Koninklijke Marechaussee. In de praktijk beheert Justitie en Veiligheid het databestand en heeft de Koninklijke Marechaussee alleen in formele zin enige band met het bestand.

2.12 Volgens het systeem mag de Officier van Justitie via een bepaald formulier gegevens opvragen aan een aantal daartoe speciaal benoemde agenten. Die agenten controleren of de aanvraag voldoet aan de wettelijke vereisten. Voldoet de aanvraag aan de eisen, dan checkt de agent of de aanvraag een zogenaamde "hit" oplevert: een hit ontstaat als het gevraagde kenteken inderdaad in het systeem voorkomt.

2.13 In ongedefinieerde spoedgevallen kan een Officier ook telefonisch een raadplegingsverzoek doen, op voorwaarde dat hij dat verzoek binnen drie dagen alsnog via het formulier indient. Er bestaat geen controle of de officier dat verzoek ook binnen de termijn indient. Op termijnoverschrijding staat geen enkele sanctie.

2.14 Bij een hit verstrekt de agent een kopie vanuit het bestand aan de Officier van Justitie, nadat men de onbewerkte foto heeft bewerkt ("geblurred"). Blurren is een handmatige bewerking van de foto waarbij de op foto aanwezige personen onherkenbaar worden gemaakt. Het is de bedoeling dat de politie in 2023 gebruik gaat maken van ongecertificeerde en ongeverifieerde software waarbij "de voorruit automatisch zwart wordt gemaakt". De originele onbewerkte foto blijft in het databestand opgeslagen. De gegevens die geraakt zijn door een hit worden bewaard. Alle overige gegevens uit het bestand worden na 4 weken automatisch vernietigd.

[7] WODC-rapport pagina 45

Het systeem in de praktijk

2.15 Dagelijks verzamelt een aantal overheidsinstanties miljoenen (foto-) registraties van auto's met kentekenplaten en plaats en tijd in heel Nederland. Naast Politie en Koninklijke Marechaussee is ook de Belastingdienst actief met honderden camera's.

2.16 Deze wet is beperkt tot het verzamelen van gegevens met behulp van zogenaamde artikel 126 JJ Sv camera's. De wet stelt eisen aan de plaatsing van vaste camera's. Artikel 126 JJ lid 1 Sv bepaalt dat de aanwezigheid van camera's op duidelijke wijze kenbaar worden gemaakt.

2.17 Hiertoe wordt de plaatsing van vaste camera's bekend gemaakt in een bij besluit gepubliceerd cameraplan. De vaste camera's worden ook alleen ingezet conform het cameraplan.

2.18 Het cameraplan bevat[8] een overzicht van:

(i) De locaties waar de vaste camera's zijn geplaatst of zullen worden geplaatst;

(ii) De locaties van vaste camera's van andere instanties wanneer daarvan structureel gebruik wordt gemaakt; en

(iii) Het aantal mobiele camera's dat kan worden ingezet en het soort locaties waar die mobiele camera's kunnen worden ingezet

(iv) Een motivering[9].

2.19 Het cameraplan is door de Minister gepubliceerd in de Staatscourant[10]. Het gepubliceerde cameraplan voldoet niet aan de vereisten van artikel 2 lid 2 van het besluit:

(a) het plan bevat geen beschrijving van de exacte locaties van vaste camera's van andere instanties als bedoeld in artikel 2 lid 2 sub (b);

(b) het cameraplan vermeldt niet het aantal mobiele camera's dat kan worden gebruikt als bedoeld in artikel 2 lid 2 sub (c).

(c) De vereiste motivering van artikel 2 lid 3 Besluit ontbreekt geheel.

2.20 Verder moet de minister achteraf een overzicht publiceren van mobiele camera's die gebruikt zijn voor de verzameling van de gegevens in het kader van deze wet.

[8] Artikel 2 lid 2 besluit

[9] Artikel 2 lid 3 besluit

[10] Meest recent op 12 februari 2021 Staatscourant 2021,7001.

2.21 Op 15 januari 2020 is het tweede cameraplan gepubliceerd in de Staatscourant (Cameraplan ANPR Nationale Politie 2020). In het eerste cameraplan is alleen een overzicht van de cameralocaties opgenomen en geen motivatie van de locaties.

2.22 In het tweede cameraplan is de volgende passage opgenomen (Cameraplan ANPR Nationale Politie, p. 1):

'Criteria bedoeld in artikel 3, tweede lid:

Camera's worden slechts overeenkomstig het cameraplan geplaatst en ingezet op locaties:

- die vanwege de specifieke aard daarvan een bepaald risico in zich hebben,

- die gekenmerkt worden door intensieve verkeersstromen of een specifieke waarvan bekend is dat bepaalde strafbare feiten op dergelijke locaties worden gepleegd.

De camera's worden afzonderlijk per locatie benoemd en van elke locatie is een afzonderlijk document waarin onder andere de motivatie zoals bedoeld in artikel 3, tweede lid van het besluit staat. De formulieren zijn ondertekend door een Officier van Justitie van de specifieke eenheid. Door ondertekening van dit plan door de Korpschef van de Nationale Politie (NP), als beheerder als verantwoordelijke wordt bekrachtigd'.

2.23 De afzonderlijke documenten waarin de motivatie voor de plaatsing van de camera's per locatie is opgenomen is niet openbaar beschikbaar. Deze cameraplanpraktijken strijden met de eis uit artikel 2 lid 3 van het Besluit, dat stelt dat de motivatie deel uitmaakt van het cameraplan.[11]

2.24 De cameraplannen van 2021 en 2022[12] bevatten dezelfde mankementen, ondanks de herhaaldelijke constateringen van de mankementen[13]. Privacy First neemt aan dat de mankementen bewust niet worden hersteld.

2.25 Privacy First heeft weinig vertrouwen in de accuratesse van het overzicht van mobiele camera's die gegevens verzamelen voor dit centrale opslagsysteem. De toetsing op naleving is zo goed als onmogelijk.

---

[11] Zie pagina 42-43 WODC rapport

[12] Cameraplan ANPR Nationale Politie 2021, Staatscourant 2021, 7001 Cameraplan ANPR Nationale Politie 2022, Nr. 51016, 30 december 2021

[13] Onder meer schending wettelijke eis van motivatie van de locatiekeuze

2.26 De camera's maken digitale foto's. De foto is afhankelijk van de instelling van de camera. Het besluit bevat dan ook een aantal technische eisen voor de camera's en een aantal handvatten voor de plaatsing van de camera's.

2.27 Maar het eindresultaat is en blijft een digitale foto. Op de foto staat alles wat de camera registreert, zoals omstanders, andere weggebruikers, alles wat voor de lens staat op het moment van de foto. Het beeld van die foto is dus niet beperkt tot de volgens de wet te bewaren en te raadplegen gegevens. De foto bevat veel meer gegevens[14].

2.28 De camera legt per voertuig één registratie vast in het centrale opslagsysteem die de volgende gegevens bevat:

a) een overzichtsfoto;

b) een uitsnede van het kenteken uit de overzichtsfoto;

c) het erkende kenteken;

d) de coördinaten van de locatie (…);

e) de datum en tijdvelden die zijn opgemaakt (…);

f) een unieke identificatiecode van de camera.

2.29 Hoe de camera deze additionele gegevens naast de foto registreert is volkomen onduidelijk. Niet duidelijk is of de cameraregistratie de onder a) tot en met f) hierboven gemelde gegevens bevat, of dat iemand of iets deze gegevens na registratie toevoegt. Verder is onduidelijk of de foto's via een beveiligde verbinding worden verzonden naar een centraal opslagsysteem of dat encryptie wordt toegepast tijdens het verzenden ervan. Privacy First begrijpt dat op dit moment geen sprake is van verzending van encrypted bestanden.

2.30 Volstrekt onduidelijk en onhelder is de logistiek tussen het moment van registratie door de camera en opslag in het centrale opslagsysteem. Tussen het moment van de digitale foto en het moment van opslag van de bewerkte foto in het databestand vinden bewerkingen plaats van de originele digitale foto. De bewerking van de foto's is niet wettelijk geregeld. Controle op die bewerking(en) door een onafhankelijke autoriteit ontbreekt.

2.31 Verder is onduidelijk wat de overheid doet met de originele digitale foto's. Op die foto staan ook personen, voorbijgangers, andere verkeersdeelnemers. Al die andere gegevens mag men niet verzamelen of bewaren of gebruiken. De status en het

14 Of, als de weersomstandigheden tegen zitten, veel minder gegevens, want de foto's kunnen door mist, sneeuw, regen, hagel, reflectie en andere invloeden onbruikbaar worden.

gebruik van de originele digitale foto's is niet wettelijk geregeld. Nergens in de wet- of regelgeving is geregeld wat de bewerkers moeten doen met de gegevens van de digitale foto die NIET als ANPR gegeven worden bewaard.

2.32 Officieren van justitie achten het ironisch dat juist die overige gegevens van de foto, met daarop bestuurders, passagiers en omstanders niet mogen worden bewaard. Want het gaat de officier van justitie en de agent tenslotte juist om de vraag wie op dat moment in of bij de gefotografeerde auto aanwezig was. En juist die gegevens worden officieel niet bewaard. Overigens is gebleken dat de officier van justitie in een aantal gevallen wel de beschikking heeft gekregen over die onbewerkte foto's[15]. Hoe dat kan, is onduidelijk.

2.33 Digitale gegevens verdwijnen niet automatisch. Men kan digitale gegevens niet weggooien alsof het een uniek papieren document is. Digitale informatie wordt hooguit ontoegankelijk gemaakt door het bestand te "overschrijven" met andere gegevens. Maar die overschrijving kan technisch worden teruggedraaid. Het is een illusie om te veronderstellen dat digitaal opgeslagen informatie wordt vernietigd; de informatie wordt hooguit ontoegankelijk gemaakt. Maar die ontoegankelijkheid is terug te draaien.

2.34 Over het tijdpad tussen het maken van de foto en de opslag van de gegevens in het centrale opslagsysteem is niets bekend. Wat het logistieke traject is, hoeveel bewerkingen de foto en/of de registratie ondergaan tussen het maken en de opslag is onbekend. Evenzeer is onbekend hoeveel personen in dat traject toegang hebben tot de informatie op de foto en de locatie en tijdvermeldingen. Geen woord over de (mate van) beveiliging van het systeem.

2.35 De verantwoordelijken voor het centrale opslagsysteem zijn de korpschef bij de politie en de Minister van Defensie bij de Koninklijke Marechaussee. Over de rolverdeling is verder niets gepubliceerd. Hoe zij hun verantwoordelijkheden invullen en uitvoeren evenmin. Het is Privacy First gebleken dat de Koninklijke Marechaussee weinig tot geen bemoeienis heeft met de uitvoering van het systeem. Bij vragen verwijst de Koninklijke Marechaussee altijd naar het ministerie van Justitie en Veiligheid.

2.36 De wet, het besluit en de regeling geven aan dat opgeslagen gegevens automatisch 4 weken na opslag automatisch worden gewist.

2.37 Door de gebrekkige en weinig transparante regelgeving en het totale gebrek aan enige onafhankelijke controle of verantwoording wordt niet gecontroleerd of de verantwoordelijke instanties de verzamelde gegevens (zowel de wettelijk

[15] Zie Pagina 84 en 85 WODC rapport.

omschreven gegevens als de overige overige) ook daadwerkelijk blijvend verwijderen.

2.38 De tussenconclusie is dan ook dat de daadwerkelijke gang van zaken tussen het maken van de digitale foto met specifiek aangewezen camera's en de opslag van al dan niet bewerkte persoonsgegevens in het databestand krakkemikkig en onvolledig is geregeld.

2.39 Onafhankelijke controle op de gang van zaken ontbreekt geheel. Van enige transparante verifieerbare verantwoording achteraf is geen sprake.

Raadpleging van het bestand: een gatenkaas

2.40 De in het centraal opslagsysteem opgeslagen gegevens worden volgens de wet uitsluitend geraadpleegd:

- In geval van verdenking van een misdrijf omschreven in artikel 67 Sv (grof gezegd, misdrijven met een straf van ten minste 4 jaar en bijzondere specifieke misdrijven),
- Ter aanhouding van een voortvluchtige als bedoeld in art 546 Sv (een veroordeelde of iemand van wie de vrijheidsbeneming is gelast).

2.41 De raadpleging geschiedt in beginsel als volgt: een opsporingsambtenaar doet langs geautomatiseerde weg een verzoek aan de geautoriseerde ambtenaar, een daartoe benoemde agent, om verstrekking van gegevens. Daarbij zendt de verzoeker een bevel van de officier (OvJ) op de voet van artikel 126 JJ lid 4 Sv.

2.42 De officier van justitie geeft via een standaardformulier een bevel tot raadpleging aan agenten die zijn geautoriseerd door de Minister van Justitie en Veiligheid. Bij dringende noodzaak mag de officier het bevel mondeling geven mits de officier binnen 3 dagen het bevel op schrift stelt.[16][17]

2.43 Nergens in de wet- of regelgeving staat dat het verzoek of het bevel een volledig kenteken moet bevatten. De zoekvraag kan ook een deel van een kenteken bevatten: "begint met AA.". Komt het kenteken op de foto niet overeen met het kenteken in het systeem, dan verstrekt de geautoriseerde agent de gegevens niet. Maar deze regel geldt alleen als de verzoeker om een specifiek kenteken verzoekt.

2.44 De zoekvraag en het bevel hoeven zelfs helemaal geen kenteken te bevatten. Artikel 126 JJ lid 3 sub e Sv stelt dat het bevel bevat: het tijdstip, de locatie en, voor zo ver

[16] Artikel 126 JJ lid 4 Sv.

[17] Onduidelijk is overigens hoe de verzoeker een mondeling bevel van de OvJ via geautomatiseerde weg aan de geautoriseerde agent zendt.

bekend, het kenteken of anders een zo nauwkeurig mogelijke aanduiding van het voertuig waarvan de gegevens worden geraadpleegd.

2.45 Het bevel kan dus de omschrijving bevatten: *"een zwarte VW Golf op donderdagmiddag tussen 1700 uur en 18 uur op de A4 naar Amsterdam" Of "alle voertuigen op locatie X op tijdstip (of in tijdsperiode) Y*". In dat geval moet de geautoriseerde agent naar waarheid duidelijk aangeven dat de kentekennummers niet overeenkomen. Maar de agent moet in dat geval wel de foto en de gegevens verstrekken.

2.46 De minister heeft 17 agenten als geautoriseerde opsporingsambtenaren benoemd. Die agenten zijn directe collega's van de opsporingsambtenaren. Zij hebben geen uitgezonderde, of relevante aparte status. Het is onduidelijk of de lijst van benoemde geautoriseerde opsporingsambtenaren in (nog) overeenstemming met de dagelijkse praktijk.

2.47 De geautoriseerde ambtenaren zijn onafhankelijk noch ter zake deskundig. Onduidelijk is op grond van welke criteria de minister opsporingsambtenaren heeft benoemd. De geautoriseerde agenten hebben geen bevoegdheid om opsporingsverzoeken van hun collega's te toetsen op doelmatigheid of rechtmatigheid. Ze hebben geen middelen om het bevel van de OvJ (indien aanwezig) te controleren op wat dan ook. De geautoriseerde agenten hoeven alleen maar de gegevens van de zoekvraag te vergelijken met de gegevens uit het centrale bestand. Of zij daartoe een extra opleiding hebben gevolgd, is onduidelijk.

2.48 De wet voorziet dus niet in een essentiële onafhankelijke toets van het bevel tot raadpleging door een onafhankelijke instantie, zoals de rechter-commissaris in strafzaken. Onafhankelijke rechterlijke toetsing vindt in het geheel niet plaats: niet voorafgaand aan de raadpleging plaats en ook niet achteraf.

2.49 De officier kan aldus zonder enige onafhankelijke controle opsporingshandelingen op grond van artikel 126 JJ Sv laten verrichten, waarbij de officier zonder verdere uitleg via het kenteken van iedere auto kan vaststellen welk persoon zich op welk moment in of bij die auto waar in Nederland bevond.

2.50 De "controle" door de geautoriseerde agent is een wassen neus. De geautoriseerde agent verstrekt alle gevraagde gegevens zolang het verzoek aan de formele vereisten voldoet en ook als de agent niet kan controleren of het verzoek voldoet, zoals bij een mondeling verzoek. De agent controleert niet of de officier enig rechtvaardig belang heeft bij het verzoek of dat het verzoek voldoet aan het doel van de wet: opsporing van voortvluchtigen of van ernstige misdaden.

2.51 Niemand controleert de formulering van de zoekvraag of de formulering van het bevel door de officier vooraf op doelmatigheid of rechtmatigheid.

2.52 Wel bepaalt artikel 8 Besluit dat ieder verzoek en iedere verstrekking wordt vastgelegd. Het besluit vermeldt niet wie dit vastlegt, waar de vastlegging plaatsvindt en wie kan en mag en zal controleren of de vastlegging adequaat geschiedt. Op niet-naleving van de verplichting staan geen sancties.

Onafhankelijke rechterlijke toetsing ontbreekt

2.53 Op geen enkel moment bestaat onafhankelijke rechterlijke toetsing in de procedure van het maken tot de foto tot de vernietiging van de gegevens in het databestand, met de aftakking van het verzoek om raadpleging van de gegevens door het OM.

2.54 Het ontbreken van rechterlijke toetsing op het gebruik van dataverkeer door overheidsdiensten en opsporingsdiensten is volgens vaste rechtspraak van het HvJ strijdig met artikel 7, 8 en 11 van het Europees Handvest.

2.55 Zo oordeelde het HVJ recentelijk, op 2 maart 2021 in de zaak van H.K in aanwezigheid van Prokuratuur: [18]

"Met name mag een nationale regeling die de toegang van de bevoegde instanties tot bewaarde verkeers- en locatiegegevens regelt, en die is vastgesteld op grond van artikel 15, lid 1, van richtlijn 2002/58, zich er niet toe beperken te eisen dat de instanties toegang tot de gegevens wordt verleend voor het doel dat met die regeling wordt nagestreefd, maar moet zij ook de materiële en procedurele voorwaarden voor dit gebruik bepalen (arresten van 6 oktober 2020, Privacy International, C623/17, EU:C:2020:790, punt 77, en 6 oktober 2020, La Quadrature du Net e.a., C511/18, C512/18 en C520/18, EU:C:2020:791, punt 176 en aldaar aangehaalde rechtspraak).

50 Aangezien een algemene toegang tot alle bewaarde gegevens los van enig – zelfs ook maar indirect – verband met het nagestreefde doel niet kan worden geacht tot het strikt noodzakelijke te zijn beperkt, moet de betrokken nationale regeling dus aan de hand van objectieve criteria bepalen in welke omstandigheden en onder welke voorwaarden aan de bevoegde nationale instanties toegang tot de gegevens van de abonnees of de geregistreerde gebruikers moet worden verleend. In dit verband kan in beginsel voor het doel van bestrijding van de criminaliteit slechts toegang worden verleend tot de gegevens van personen die ervan worden verdacht een ernstig misdrijf te plannen, te plegen of te hebben gepleegd of op de een of andere wijze betrokken te zijn bij een dergelijk misdrijf. In bijzondere situaties, zoals die waarin vitale belangen van nationale veiligheid, landsverdediging of openbare veiligheid door terroristische activiteiten worden bedreigd, zou echter ook toegang tot de gegevens van andere personen kunnen worden verleend, wanneer op grond

[18] ECLI:EU:C: 2021:152; HvJ in de zaak C-746/18 van H.K in aanwezigheid van Prokuratuur

van objectieve elementen kan worden geoordeeld dat deze gegevens in het concrete geval een daadwerkelijke bijdrage tot de bestrijding van dergelijke activiteiten zouden kunnen leveren (zie in die zin arrest Tele2, punt 119, en arrest van 6 oktober 2020, La Quadrature du Net e.a., C511/18, C512/18 en C520/18, EU:C:2020:791, punt 188).

51 Om te waarborgen dat deze voorwaarden in de praktijk ten volle in acht worden genomen, is het van wezenlijk belang dat de toegang van de bevoegde nationale instanties tot de bewaarde gegevens wordt onderworpen aan voorafgaande toetsing door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit, en dat deze rechterlijke instantie of deze entiteit haar beslissing geeft op een met redenen omkleed verzoek van deze instanties dat met name wordt ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten. In naar behoren gemotiveerde urgente gevallen dient die toetsing op korte termijn plaats te vinden (zie in die zin arrest van 6 oktober 2020, La Quadrature du Net e.a., C511/18, C512/18 en C520/18, EU:C:2020:791, punt 189 en aldaar aangehaalde rechtspraak).

52 Die voorafgaande toetsing vereist onder meer, zoals de advocaat-generaal in wezen heeft opgemerkt in punt 105 van zijn conclusie, dat de rechterlijke instantie of de entiteit die belast is met die toetsing, over alle bevoegdheden beschikt en alle noodzakelijke waarborgen biedt om ervoor te zorgen dat de verschillende betrokken belangen en rechten met elkaar in overeenstemming worden gebracht. In het specifieke geval van een strafrechtelijk onderzoek vereist een dergelijke toetsing dat die rechterlijke instantie of entiteit in staat is een juist evenwicht te verzekeren tussen, enerzijds, de belangen die verband houden met de behoeften van het onderzoek in het kader van de bestrijding van criminaliteit, en, anderzijds, de fundamentele rechten op eerbiediging van de persoonlijke levenssfeer en op bescherming van de persoonsgegevens van de personen op wier gegevens de toegang betrekking heeft."

Tegenover een grootschalige structurele inbreuk op door grondrechten beschermde persoonsgegevens hoort een deugdelijke nationale wettelijke regeling met adequate onafhankelijke rechterlijke toetsing. Die onafhankelijke rechterlijke toetsing ontbreekt (bewust) in de regeling van artikel 126 JJ Sv en verder.

<u>Gepubliceerde evaluatie van het systeem</u>

2.56 Of de bevoegdheid van meerwaarde is voor de opsporing is een discussiepunt geweest in het debat rondom 126jj. De Raad van State wijst er in een advies op dat uit de beschikbare evaluaties geen eenduidig beeld naar voren komt of ANPR een meerwaarde biedt voor de opsporing (Kamerstukken II, 33542, nr. 4, 2013). Daarbij wijst de Raad van State ook op de bevinding uit het rapport Hits en Hints dat: '*de*

meerwaarde voor opsporing alleen [kan] worden verzilverd als daar bewust aan wordt gewerkt en als die inspanningen ten koste mogen gaan van ander politiewerk' (Flight & van Egmond, 2011, p. 89). Het risico bestaat dat meer ANPR-camera's leiden tot meer hits, wat het lastiger maakt voor de politie om capaciteit vrij te maken om deze hits op te volgen en ANPR effectief in te zetten in de opsporing.

2.57 Deze bevindingen staan niet op zich. In eerdere (internationale) onderzoeken naar de inzet van technologie door de politie komt naar voren dat nieuwe technologieën doorgaans worden toegepast binnen bestaande werkwijzen, wat niet noodzakelijkerwijs leidt tot grote veranderingen binnen de organisatie wat betreft effectiviteit en efficiëntie.

2.58 Een goed voorbeeld van het suboptimaal gebruik betreft de ophef van het gebruik van de foto's bij bestrijding van de winkeldiefstel in het Outletcenter Roermond[19]

2.59 De inzet van ANPR bij de bestrijding van winkeldiefstal in het Outletcenter Roermond heeft veel aandacht van de politiek, media en burgerrechtenbewegingen gekregen. Er zijn diverse vragen hierover in de Tweede Kamer gesteld en heeft Amnesty International een uitgebreid rapport gepubliceerd over deze methodiek. De AP heeft specifiek over deze inzet 50.000 klachten ontvangen.

2.60 De FG heeft gesprekken met de verantwoordelijke van het programma Sensing gevoerd. Dit ANPR-initiatief maakt daar deel van uit. De FG oordeelde dat het gebruik van ANPR op deze wijze niet aan de vereisten van de Wpg voldeed en heeft de programmamanager geadviseerd te stoppen met deze pilot. Het project is na schorsing definitief gestopt. Verder is afgesproken dat binnen het programma Sensing een Wpg beoordeling zal plaatsvinden voordat een nieuw initiatief daadwerkelijk wordt gestart.

2.61 Sterker nog, in sommige gevallen lijkt de introductie van nieuwe technologie juist averechts te werken. Dit komt onder meer doordat de extra werklast oplevert, onjuist wordt gebruikt of leidt tot een overdaad aan informatie (information overload), wat de efficiëntie en effectiviteit niet ten goede komt.

2.62 De Minister van Justitie en Veiligheid stelt in de memorie van toelichting dat na inwerkingtreding van de wet op basis van een evaluatie meer inzicht kan worden verkregen in de eventuele meerwaarde van de bevoegdheid en dat daarom in het wetsvoorstel een evaluatie- en horizonbepaling zijn opgenomen.[20]

---

[19] Jaarverslag 2021 Functionaris voor de gegevensbescherming Politie d.d.22 maart 2022, pagina 5 onder het kopje Toezichtactiviteiten van de FG

[20] Kamerstukken II,33542, nr. 3, 2013

2.63 Centraal daarbij staat de aanname die aan de bevoegdheid ten grondslag ligt, namelijk dat ‘de bevoegdheid effectief is voor de opsporing van strafbare feiten’ (Kamerstukken II, 33542, nr. 3, 2013, p. 9), wat aan de hand van een evaluatie kan worden bevestigd of ontkracht, en dat op basis daarvan kan worden besloten of de bevoegdheid al of niet wordt gehandhaafd.[21]

2.64 De Staat zou ieder jaar een jaarverslag publiceren. De staat heeft over het eerste jaar van de werking van de wet op 11 februari 2020 een jaarverslag gepubliceerd.

2.65 Het jaarverslag over 2020 en 2021 is nog niet gepubliceerd.

2.66 Wel heeft het WODC (onderdeel van Justitie en Veiligheid) in 2020 een onderzoek gepubliceerd in de vorm van cahier 2020-13 het gebruik van bewaarde kentekengegevens in de opsporing[22]. Het rapport is uitsluitend gebaseerd op gesprekken met agenten en officieren van justitie.[23] Het WODC-rapport bezit geen jaarverslag of een onafhankelijke evaluatie.

2.67 Het eenzijdig WODC-rapport biedt niettemin een aardig inkijkje in de praktijk van het systeem. De samenvatting en de conclusie strookt met het beeld van Privacy First. Men heeft in ruim twee jaar tijd nog geen enkele voortvluchtige opgepakt of zwaar misdrijf opgelost met behulp van artikel 126JJ Sv. Er is geen enkel bewijs van nut en noodzaak, al helemaal niet afgezet tegen de stelselmatige inbreuk van de verzameling van miljoenen foto's per dag, iedere dag van het jaar.

2.68 Een onafhankelijke evaluatie heeft niet plaats gevonden.

2.69 In oktober 2021 heeft het WODC een evaluatierapport gepubliceerd*: Cahier 2021-19 Evaluatie ANPR-wetgeving 126jj Wetboek van Strafvordering*. Het WODC is onderdeel van het ministerie van Justitie en Veiligheid en kan niet als een onafhankelijke partij worden beschouwd als het gaat om een evaluatie van een regeling van datzelfde ministerie.

2.70 Ondanks het gebrek aan onafhankelijkheid biedt het evaluatierapport een treurigstemmende inkijk in de structuur en het nut en de noodzaak van het systeem van artikel 126 JJ Sv. Op alle vlakken rammelt de uitvoering, controle ontbreekt, en ondanks de miljoenen foto's per maand is er nog geen voortvluchtige opgepakt of ook maar een misdaad opgelost door gebruik van de foto's De evaluatie is helder:

---

[21] WODC-rapport pagina 18

[22] WODC-rapport Cahier 2020-13 "Het gebruik van bewaarde kentekengegevens in de opsporing. De wet ‘vastleggen en bewaren van kentekengegevens door de politie’ een jaar in werking

[23] Het rapport is dus opgesteld door de een afdeling van Veiligheid en justitie op basis van gesprekken met andere afdelingen van Veiligheid en Justitie over de werking van een opsporingsmiddel. Dit cahier is niet gelijk te stellen met een onafhankelijke evaluatie. Niettemin is het zeer lezenswaardig.

sommige opsporingsambtenaren vinden de foto's "nice to have" maar van enig nut of noodzaak blijkt niets.

Tussenconclusie: krakkemikkig systeem in alle onderdelen

2.71 De conclusie is dat geen van de onderdelen van het systeem van artikel 126 JJ Sv de toets van de "end-to-end safeguards" doorstaat.

- De verzameling van de foto's is niet adequaat geregeld (cameraplan voldoet niet)
- De verzameling van de ANPR-gegevens voldoet niet (geen autorisatie, geen controle, geen adequate bescherming tegen misbruik)
- De opslag van de gegevens voldoet niet
- Het gebruik en de verstrekking van de gegevens voldoet niet
- De vernietiging van de gegevens voldoet niet;
- Het onafhankelijk toezicht bestaat niet
- De evaluatie wordt niet adequaat uitgevoerd.

Nut en noodzaak na twee jaar: noodzaak niet bewezen

2.72 De parlementaire geschiedenis besteedt heel weinig aandacht aan nut en noodzaak van de registratie van miljoenen gegevens per dag of per week voor het opsporingsdoel. De motivering komt erop neer dat het centrale bestand handig is voor de opsporing van voortvluchtigen en ernstige misdrijven. Maar "handig" is onvoldoende grondslag voor de invoering van een dergelijk systeem als inbreuk op het recht van privacy van artikel 8 EVRM.[24]

2.73 Al in 2011 heeft de voorganger van de Autoriteit Persoonsgegevens in het advies op het conceptwetsvoorstel gewezen op de noodzakelijkheid van de onderbouwing van noodzaak in het licht van artikel 8 EVRM.

2.74 Het CBP kwam ten aanzien van het conceptwetsvoorstel uit 2011 tot de conclusie dat het conceptwetsvoorstel voorzag in een bevoegdheid voor de politie om, in de geschetste mogelijkheid van een landelijke dekkend ANPR-cameranetwerk, alle passanten op Nederlandse wegen als potentiële verdachten in politiebestanden op te nemen. Mede door de onbepaaldheid van het doel “opsporing van strafbare feiten” in samenhang met de bewaartermijn en de geopperde mogelijkheid van centrale

[24] In de uitspraak Handyside van EHRM (para 48) heeft het Hof nadrukkelijk uitgelegd dat het vereiste van ‘noodzakelijkheid’: ‘neither has it the flexibility of such expressions as "admissible", "ordinary" (cf. Article 4 para. 3) (art. 4-3), "useful"’

opslag zou een hooiberg van politiegegevens betreffende veelal niet-verdachte personen gecreëerd worden. Het wettelijk mogelijk maken van deze verwerking, die inbreuk maakt op de persoonlijke levenssfeer van een groot aantal burgers, zou alleen te rechtvaardigen zijn wanneer de noodzaak daartoe is aangetoond. Het CBP kwam echter tot de conclusie dat dit noch wat betreft de subsidiariteit, noch wat betreft de proportionaliteit het geval was.

2.75 De subsidiariteit en proportionaliteit van de wet, als grondslag voor de inbreuk op mensenrechten moet afdoende en overtuigend zijn. Dit was en is niet het geval met het stelsel van artikel 126 JJ Sv en de op het artikel gebaseerde besluiten en regeling.

2.76 Bij de inwerkingtreding van de wet was juist uit eerdere proeven met raadpleging van kentekenregistratie met ANPR-gegevens, gebleken dat het nut uiterst beperkt is.

2.77 Uit het jaarverslag en uit de WODC-rapporten blijkt ook dat geen enkele voortvluchtige is opgepakt met behulp van artikel 126 JJ SV. Het blijkt niet mogelijk om vast te stellen of het gebruik van artikel 126 JJ SV daadwerkelijk heeft bijgedragen aan de opsporing van ook maar een enkel ernstig misdrijf.

2.78 Wel is duidelijk dat het inherente risico van misbruik van het systeem ook daadwerkelijk plaatsvindt: Het OM en de politie hebben daadwerkelijk gebruik gemaakt van foto's en gegevens die men volgens het stelsel van de wet niet mocht hebben.

2.79 De voorlopige conclusie na drie jaar werking is dat artikel 126 JJSV voor politie en OM hooguit een "nice to have" methode is. Maar het systeem is geen enkele keer noodzakelijk gebleken. En die tussenconclusie maakt dat de massale inbreuk van miljoenen foto's per dag op de grondrechten niet gerechtvaardigd kan worden.

Minder vergaande alternatieven: opvragen camerabeelden bij derden

2.80 Justitie beschikt in de praktijk al over minder vergaande alternatieven voor de opsporing van voortvluchtigen en van strafbare feiten. Een belangrijk middel is het opvragen van camerabeelden van particuliere dienstverleners en andere overheden naar aanleiding van concrete incidenten of vermoedens. Het grote voordeel voor justitie is dat de gemaakte beelden volledig zonder aanpassing kan gebruiken.

2.81 Een ander minder verstrekkend alternatief is het door de hoge raad in 2014 (ten onrechte) gedoogde alternatief van het gebruik en de opslag voor de duur van zeven dagen van ANPR-gegevens (hits en no hits), zonder wettelijke basis, in het kader van een strafrechtelijk onderzoek.[25]

[25] HR 11 november 2014, ECLI: NL:HR:2014:3142

Geen adequate maatregelen tegen misbruik

2.82 Noch de wet noch de uitvoering bevat adequate maatregelen ter preventie van misbruik van de gegevens op ieder moment van het proces. De Staat is vergeten om audits te doen op het gebruik. Zeker geen onafhankelijk onderzoek naar de inherente gevaren van misbruik door derden en door gebruikers. De combinatie de ondeugdelijke wet en de ondeugdelijke uitvoering en het gebrek aan onafhankelijke controle levert een ontoelaatbare inbreuk op de mensenrechten.

3. EUROPEESRECHTELIJK TOETSINGSKADER

3.1 Het recht op bescherming van persoonsgegevens is een grondrecht en de eerbiediging ervan vormt een belangrijk doel voor de Europese Unie.

3.2 Het recht is verankerd in artikel 8 van het Handvest van de grondrechten van de Europese Unie (hierna: „Handvest"), Dit grondrecht houdt voorts nauw verband met het recht op eerbiediging van het privéleven en van het familie- en gezinsleven, dat is vervat in artikel 7 van het Handvest.

3.3 Het recht op bescherming van persoonsgegevens is ook vastgelegd in artikel 16, lid 1, van het Verdrag betreffende de werking van de Europese Unie (VWEU).

3.4 Het Europeesrechtelijk raamwerk voor de beoordeling van dit geschil wordt gevormd door:

- Het VWEU
- Artikel 8 EVRM
- Artikel 7 en 8 Europees Handvest
- Rechtspraak Europees Hof voor de Rechten van de Mens (EHRM)
- Rechtspraak Hof van Justitie van de Europese Unie (HvJ)

4. VWEU

4.1 Artikel 16 VWEU: eenieder heeft recht op bescherming van zijn persoonsgegevens.

4.2 Artikel 21 VWEU: iedere burger van de Unie heeft het recht vrij op het grondgebied van de lidstaten te reizen en te verblijven, onder voorbehoud van de beperkingen en voorwaarden die bij de Verdragen en de bepalingen ter uitvoering daarvan zijn vastgesteld.

5. EVRM

5.1 Artikel 8 EVRM: recht op eerbiediging van privéleven, familie- en gezinsleven.

5.2 lid 1: eenieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

5.3 lid 2 Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in de democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

6. EUROPEES HANDVEST

6.1 **Artikel 7 van het Europees Handvest:**

Eerbiediging van het privéleven en het familie- en gezinsleven.

Eenieder heeft recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.

Artikel 8 van het Europees Handvest:

Bescherming van persoonsgegevens.

6.2 **Lid 1**: eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.

Lid 2: deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet.

Lid 3: Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.

Lid 4 Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.

6.3 Het EVRM voorziet in minimumbescherming van het fundamentele recht op eerbiediging van de persoonlijke levenssfeer. De inhoud en de reikwijdte van de EU-grondrechten in het Handvest zijn dezelfde als die van de EVRM-rechten voor zover het Handvest rechten bevat die corresponderen met het EVRM (artikel 52 lid 3 Handvest).

6.4 De door het EVRM gewaarborgde rechten maken ook als algemene beginselen deel uit van het Unierecht (artikel 6 lid 3 EU-Verdrag). Unierechtelijk is daarom ten minste sprake van eenzelfde minimumbeschermingsniveau als dat van het EVRM. Het Unierecht kan evenwel een ruimere bescherming bieden (artikel 52 lid 3 Handvest).

6.5 Kernvereisten voor inbreuk op de mensenrechten:

- wettelijke grondslag;
- noodzakelijkheid

- proportionaliteit

7. DE WET STRIJDT MET EUROPEES RECHT (ZOWEL EVRM ALS HANDVEST/VWEU).

7.1 De Staat hanteert als uitgangspunt bij de wet dat: "*een bevoegdheid tot het bewaren van passagegegevens dient te voldoen aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit, die voortvloeien uit het Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM)*"[26]

7.2 De Staat accepteert (terecht) dat de wet getoetst wordt aan de bepalingen van het EVRM. De wet is in strijd met artikel 8 EVRM.

7.3 Ook moet de wet getoetst worden aan het Unierecht. Het EVRM maakt ook deel uit van het Unierecht.

7.4 Privacy First stelt voorop dat het in onderhavige zaak draait om het in bulk maken en in bulk verzamelen van miljoenen foto's per dag. Van iedere onschuldige ontvanger, niet om een later technische verzameling van locatiedata.

7.5 Het HvJ hanteert als uitgangspunt in de vaste rechtspraak dat de wettelijk uitzonderingen op de bescherming van persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven en moeten voldoen aan het doelmatigheidsvereiste en aan het proportionaliteitsvereiste.[27]

7.6 Om gerechtvaardigd te zijn, moet een dergelijke aantasting bij wet zijn voorzien, de wezenlijke inhoud van die rechten eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang, en moeten de afwijkingen en beperkingen op die rechten binnen de grenzen van het strikt noodzakelijke blijven (punt 65 HvJ Volker und Markus Schecke Eifert;).

---

26 Pagina 4 onder 4.1 van de Memorie van toelichting nr.3 bij het wetsvoorstel 33.542

27 (zie in die zin arresten Afton Chemical, C-343/09, EU:C:2010:419, punt 45; Volker und Markus Schecke en Eifert, EU:C:2010:662, punt 74; Nelson e.a., C-581/10 en C-629/10, EU:C:2012:657, punt 71; Sky Österreich, C-283/11, EU:C:2013:28, punt 50, en Schaible, C-101/12, EU:C:2013:661, punt 29)

Recente rechtspraak van Grote Kamer EHRM over "end-to-end-safeguards" bij massasurveillance: Nederlands systeem voldoet niet

7.7 Op 25 mei 2021 heeft de Grote kamer van het EHRM twee uitspraken gedaan over het standaard in bulk verzamelen van persoonsgegevens door de overheid, waarbij preventief allerlei persoonsgegevens worden verzameld van onschuldige burgers.[28]

7.8 Het EHRM besloot dat een zogenaamd "bulk interception regime" op zich geen schending oplevert van het EVRM. Maar, zo vervolgde het EHRM, een dergelijk systeem moest wel voldoen aan zogenaamde “end-to-end safeguards”.

7.9 Dat houdt in dat men op nationaal niveau per onderdeel van het systeem beoordeelt op subsidiariteit en proportionaliteit, en dat de bulk interception van af het begin onderworpen is aan onafhankelijke autorisatie en dat de gehele operatie onderworpen is aan onafhankelijk toezicht.

7.10 De Grote Kamer van het EHRM besloot dat noch het systeem van de VK noch het systeem van Zweden voldeed aan de vereisten van artikel 8 EVRM.

Rechtspraak HvJ over schending proportionaliteit/evenredigheid

7.11 Het HvJ heeft in een aantal uitspraken duidelijk uitgelegd op welke wijze men een wettelijke regeling moet toetsten aan de grondrechten van artikel 7 en 8 Europees Handvest en aan artikel 8 EVRM.

7.12 De hoekstenen zijn vervat in de zogenaamde Digital Rights uitspraken[29] en in de Tele2 uitspraken[30]

Digital Rights zaken

7.13 Het HvJ formuleert in de uitspraak van Digital Rights/Ireland de volgende criteria voor een inbreuk op het recht op bescherming van persoonsgegevens:

- Beperking tot verzameling van strikt noodzakelijke persoonsgegevens;
- Verwerking van persoonsgegevens houdt verband met Europese doelstelling;
- (Voorafgaande) rechterlijke toetsing van toegang tot verzameling persoonsgegevens
- Duidelijke duur bewaring;

[28] the case of Big Brother Watch and Others v. the United Kingdom (application nos. 58170/13, 62322/14 and 24969/15) en Centrum för rättvisa v. Sweden (application no. 35252/08)

[29] Arrest van 8 april 2014 (Grote kamer), Digital Rights Ireland en Seitlinger e.a. (gevoegde zaken C-293/12 en C-594/12, EU:C:2014:238)

[30] Arrest van 21 december 2016 (Grote kamer), Tele2 Sverige (gevoegde zaken C-203/15 en C-698/15, EU:C:2016:970)

- Adequate beveiliging.

7.14 In de Digital Rights zaak draaide het om de massale verzameling en verstrekking van dataverkeer door de aanbieders van elektronische communicatiediensten.

7.15 Het HvJ oordeelde of de verplichting van de aanbieders om gegevens betreffende het privéleven van een persoon en zijn communicatie, gedurende een bepaalde tijd te bewaren en toegang daartoe toe te staan aan de bevoegde nationale autoriteiten, een ongerechtvaardigde inmenging in die grondrechten impliceerde.

7.16 Het ging om persoonsgegevens die nodig zijn om de bron van een communicatie en de bestemming ervan te traceren en te identificeren, om de datum, het tijdstip en de duur van een communicatie alsmede het type communicatie te bepalen, om de communicatieapparatuur van de gebruikers te identificeren alsmede om de locatie van mobiele communicatieapparatuur te bepalen, tot welke gegevens onder meer behoren naam en adres van de abonnee of de geregistreerde gebruiker, het oproepende en het opgeroepen nummer en een IP-adres voor internetdiensten.

7.17 Aan de hand van deze gegevens kan met name worden nagegaan met welke persoon en via welke weg een abonnee of geregistreerde gebruiker heeft gecommuniceerd, hoelang de communicatie heeft geduurd en vanaf welke plaats zij heeft plaatsgevonden. Bovendien kan aan de hand van deze gegevens worden achterhaald hoe vaak de abonnee of de geregistreerde gebruiker gedurende een bepaalde periode met bepaalde personen heeft gecommuniceerd.

7.18 De overeenkomsten met de onderhavige situatie zijn aanzienlijk:

- Massale verzameling van opslag van persoonsgegevens
- Geen enkel onderscheid des persoons/ geen enkel verband tussen de opgeslagen gegevens en opsporing van voortvluchtigen of ernstige misdrijven
- Verstrekking aan opsporingsdiensten
- Afwezigheid van enige onafhankelijke rechterlijke toetsing
- Afwezigheid van adequate materiele en procedurele voorschriften die veiligheid en toegang of preventie van misbruik reguleren

7.19 Het HvJ oordeelde dat verplichtingen van de aanbieders een bijzonder zware inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten op eerbiediging van het privéleven en op bescherming van persoonsgegevens vormden.

7.20 Het HvJ heeft geoordeeld dat het systeem van het bewaren van gegevens in strijd was met het evenredigheidsbeginsel.

7.21 Het HvJ heeft de bepalingen uit de richtlijn die de basis vormden voor het wettelijk systeem ongeldig verklaard met de overweging dat de zeer ruime en bijzonder zware inmenging in de grondrechten die zij impliceerde, niet toereikend was gereguleerd om te garanderen dat deze inmenging beperkt was tot het strikt noodzakelijke (punt 65).

7.22 Bovendien stelde het HvJ vast dat een onafhankelijke autoriteit ontbreekt die toezicht houdt op de eerbiediging van de vereisten inzake bescherming en beveiliging, zoals het Handvest evenwel uitdrukkelijk voorschrijft (punten 66-68).

Tele2 Sverige zaak[31]

7.23 Het HvJ oordeelt dat artikel 15, lid 1, van richtlijn 2002/58/EG, gelezen tegen de achtergrond van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, zich verzet tegen een nationale regeling zoals die van Zweden, die, ter bestrijding van criminaliteit, voorziet in algemene en ongedifferentieerde bewaring van alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronische communicatiemiddelen.

7.24 Volgens het Hof gaat een dergelijke regeling verder dan strikt noodzakelijk is, en kan zij niet worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals genoemd artikel 15, lid 1, gelezen tegen de achtergrond van voornoemde artikelen van het Handvest, vereist (punten 99-105, 107, 112, dictum 1).

7.25 Diezelfde bepaling, gelezen tegen de achtergrond van dezelfde artikelen van het Handvest, verzet zich tevens tegen een nationale regeling die de bescherming en de beveiliging van de verkeersgegevens en de locatiegegevens en in het bijzonder de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens regelt zonder, in het kader van de bestrijding van criminaliteit, te bepalen dat die toegang alleen wordt verleend ter bestrijding van ernstige criminaliteit, dat die toegang aan een voorafgaand toezicht door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit is onderworpen, en dat de betrokken gegevens op het grondgebied van de Unie moeten worden bewaard (punten 118-122, 125, dictum 2).

7.26 Het HvJ heeft overwogen dat artikel 15, lid 1, van richtlijn 2002/58/EG zich daarentegen niet verzet tegen een regeling op grond waarvan dergelijke gegevens ter bestrijding van zware criminaliteit preventief gericht kunnen worden bewaard, op voorwaarde dat die bewaring, wat de categorieën van betrokken gegevens, de betrokken communicatiemiddelen, de betrokken personen en de duur van de bewaring betreft, tot het strikt noodzakelijke wordt beperkt.

---

[31] Arrest van 21 december 2016 (Grote kamer), Tele2 Sverige (gevoegde zaken C-203/15 en C-698/15, EU:C:2016:970)

7.27 Om aan deze eisen te voldoen, moet deze nationale regeling in de eerste plaats duidelijke en nauwkeurige regels bevatten, zodat persoonsgegevens doeltreffend kunnen worden beschermd tegen het risico van misbruik.

7.28 Zij moet in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel van bewaring van gegevens preventief kan worden genomen, en aldus waarborgen dat een dergelijke maatregel tot het strikt noodzakelijke wordt beperkt.

7.29 In de tweede plaats moet – wat de materiële voorwaarden betreft waaraan de nationale regeling moet voldoen om te waarborgen dat zij tot het strikt noodzakelijke is beperkt – de bewaring van de gegevens steeds voldoen aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel.

7.30 In het bijzonder moeten dergelijke voorwaarden in de praktijk van dien aard blijken te zijn dat zij de omvang van de maatregel, en dus de kring van betrokken personen, daadwerkelijk afbakenen.

7.31 Wat deze afbakening betreft, moet de nationale regeling zijn gebaseerd op objectieve elementen waarmee kan worden gedoeld op een groep mensen wier gegevens, althans indirect, een band met handelingen van zware criminaliteit aan het licht kunnen brengen, waarmee op de een of andere wijze kan worden bijgedragen tot de bestrijding van zware criminaliteit of waarmee een ernstig risico voor de openbare veiligheid kan worden voorkomen (punten 108-111).

7.32 Verzameling en bewaring van verkeersgegevens moet een uitzondering zijn, en niet de regel, aldus het HvJ[32].

7.33 De Nederlandse wetgever was terdege op de hoogte van deze door het Hof opgelegde verplichtingen tijdens het redigeren en de behandeling van het wetsvoorstel. De Staat heeft bewust deze verplichtingen genegeerd.

Privacy International[33]

7.34 Het HvJ benadrukt in dit arrest nog eens de noodzaak van de waarborgen van een inbreuk op het grondrecht van eerbiediging van het privéleven:

"In dit verband zij eraan herinnerd dat de bescherming van het grondrecht op eerbiediging van het privéleven volgens vaste rechtspraak van het Hof vereist dat de

[32] In dit verband dient enerzijds erop te worden gewezen dat een dergelijke regeling, gelet op de in punt 97 van het onderhavige arrest beschreven kenmerken ervan, tot gevolg heeft dat de bewaring van de verkeersgegevens en van de locatiegegevens de regel is, terwijl het bij richtlijn 2002/58 ingevoerde stelsel eist dat deze bewaring van gegevens de uitzondering vormt."

[33] Hof EU 6 oktober 2020, zaak C-623/17 Privacy International vs Secretary of State

uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven.

Bovendien kan een doelstelling van algemeen belang niet worden nagestreefd zonder rekening te houden met het feit dat deze doelstelling moet worden verzoend met de door de maatregel aangetastegrondrechten, zulks via een evenwichtige afweging tussen de doelstelling en de op het spel staande belangen en rechten [zie in die zin arresten van 16 december 2008, Satakunnan Markkinapörssi en Satamedia, C-73/07, EU:C:2008:727, punt 56; 9 november 2010, Volker und Markus Schecke en Eifert, C-92/09 en C-93/09, EU:C:2010:662, punten 76, 77 en 86, en 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punt 52; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 140]."[34]

7.35 Het HvJ beschrijft ook de vereisten van de evenredigheidstoets:

Om aan het evenredigheidsvereiste te voldoen, dient een regeling duidelijke en nauwkeurige regels te bevatten over de reikwijdte en de toepassing van de betrokken maatregel, zodat degenen van wie de persoonsgegevens aan de orde zijn, over voldoende waarborgen beschikken dat die gegevensdoeltreffend worden beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar intern recht en in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke waarborgen te beschikken is des te groter wanneer de persoonsgegevens op geautomatiseerde wijze worden verwerkt, met name wanneer er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd. Deze overwegingen gelden in het bijzonder wanneer het gaat om de bescherming van een bijzondere categorie persoonsgegevens, te weten gevoelige gegevens [zie in die zin arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 54 en 55, en 21 december 2016, Tele2, C-203/15 enC-698/15, EU:C:2016:970, punt 117; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017,EU:C:2017:592, punt 141].[35]

7.36 Verder benadrukt het HvJ nog eens het inherente risico van misbruik bij massa opslag van (telecommunicatie) gegevens. Maar dat inherente risico is hetzelfde voor de opslag van miljoenen digitale foto's, al dan niet bewerkt:

---

[34] R.O. 67 van het arrest

[35] RO 68 Arrest.

[36]*Ten slotte is het zo dat, gelet op de aanzienlijke hoeveelheid verkeers- en locatiegegevens die continukunnen worden bewaard op grond van een algemene bewaringsmaatregel, en op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, het enkele feit dat die gegevens dooraanbieders van elektronische communicatiediensten worden bewaard, risico's van misbruik en onrechtmatige toegang tot de gegevens inhoudt.*

7.37 Het HvJ oordeelde dan ook dat de verplichting tot verstrekking van de bulktelecommunicatiegegevens aan de Britse geheime diensten in strijd is met artikel 7 en 8 (en 11) van het Europees Handvest :

"*Wat in het bijzonder de toegang van een autoriteit tot persoonsgegevens betreft, mag een regeling zich niet ertoe beperken te eisen dat de toegang tot deze gegevens wordt verleend voor het met die regeling beoogde doel, maar moet zij ook de materiële en procedurele voorwaarden voor dit gebruik bepalen[zie naar analogie advies 1/15 (PNR Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592,punt 192 en aldaar aangehaalde rechtspraak].*

78 Een nationale regeling die de toegang tot locatie en verkeersgegevens regelt, moet dus aan de hand van objectieve criteria bepalen in welke omstandigheden en onder welke voorwaarden aan de bevoegde nationale autoriteiten toegang tot de betrokken gegevens moet worden verleend, aangezien een algemene toegang tot alle bewaarde gegevens, los van enig – zelfs maar indirect – verband met het nagestreefde doel, niet kan worden geacht tot het strikt noodzakelijke te zijn beperkt, (zie in die zin arrest van 21 december 2016, Tele2, C203/15 en C698/15, EU:C:2016:970, punt 119 en aldaar aangehaalde rechtspraak).

79 Die vereisten zijn a fortiori van toepassing op een wettelijke maatregel als aan de orde in het hoofdgeding, op grond waarvan de bevoegde nationale autoriteit aanbieders van elektronische communicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen. Een dergelijke doorzending heeft immers tot gevolg dat die gegevens ter beschikking worden gesteld aan overheidsinstanties [zie naar analogie advies 1/15 (PNR Overeenkomst EU-Canada) van 26 juli 2017,EU:C:2017:592, punt 212].

[36] Ro 72 arrest

80 Het feit dat de doorzending van de verkeers- en locatiegegevens geschiedt op algemene en ongedifferentieerde wijze, betekent dat die doorzending algemeen alle personen betreft die gebruik maken van elektronische communicatiediensten, dat wil zeggen zelfs personen voor wie er geenenkele aanwijzing bestaat dat hun gedrag – zelfs maar indirect of van ver – een verband vertoont met de doelstelling van bescherming van de nationale veiligheid. Met name is er geen enkel verband vereist tussen de gegevens die moeten worden doorgezonden en een bedreiging van de nationale veiligheid(zie in die zin arresten van 8 april 2014, Digital Rights Ireland e.a., C293/12 en C594/12,EU:C:2014:238, punten 57 en 58, en 21 december 2016, Tele2, C203/15 en C698/15,EU:C:2016:970, punt 105). Gelet op het feit dat de doorzending van dergelijke gegevens aan overheidsinstanties – overeenkomstig de vaststelling in punt 79 van het onderhavige arrest – gelijk staat aan het verlenen van toegang tot deze gegevens, moet worden geoordeeld dat een regeling die dealgemene en ongedifferentieerde doorzending van gegevens aan overheidsinstanties mogelijk maakt een algemene toegang tot die gegevens impliceert.

81 Daaruit volgt dat een nationale regeling die aanbieders van elektronische communicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten oplegt, verder gaat dan strikt noodzakelijk is en niet kan worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15,lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist. "

7.38 Als verstrekking van dit soort massale gegevens aan de veiligheidsdiensten niet is toegestaan (zelfs niet in het kader van het nationaal belang), dan is verwerking en massaverstrekking van dit een vergelijkbaar soort gegevens (digitale foto's met auto's met kentekens en alles wat op de foto zichtbaar is) in het kader van strafrechtelijke opsporing helemaal niet toegestaan.

7.39 Het HvJ heeft recentelijk in het arrest in de zaak C-817/19 ASBL "Ligue des droits humains" nog eens benadrukt dat de inbreuk op de mensenrechten niet alleen beperkt moet worden uitgelegd maar dat een rechtelijke of onafhankelijke toetsing van het systeem essentieel is. En dat onafhankelijk toezicht ontbreekt in deze structuur van artikel 126 jj Sv.

Aard van de ANPR-gegevens behoeft bescherming en rechtvaardigt de inbreuk niet

7.40 Het systeem van artikel 126 jj SV vormt een inbreuk op de mensenrechten. De Staat heeft in kort geding ten onrechte betoogt dat de aard van de gegevens, in essentie een vorm van locatiegegevens (waar was die persoon op dat moment) een minder verregaande bescherming zou moeten hebben dan bijvoorbeeld communicatiegegevens, waarbij de staat de inhoud van de communicatie leest.

7.41 Privacy First benadrukt dat deze zaak draait om het maken en bewaren van miljoenen foto's per dag van ieder die voor de honderden camera's verschijnt. Die onbewerkte foto's worden aangevuld met data en locatiegegevens en die pakketjes worden in bewaard in een weinig veilig databestand. Het gaat in deze zaak dus om veel meer dan "alleen locatiegegevens". De vergelijking met enkel locatiegegevens gaat mank. Niet valt in te zien waarom de bescherming tegen inbreuken op de mensenrechten bij locatiegegevens minder ver zou moeten strekken dan de beschermingen tegen inbreuk op de mensenrechten bij communicatiedata. De jurisprudentie van het HvJ en van het EHRM is ook van toepassing op deze zaak.

7.42 Daarbij gaat de Staat voorbij aan het feit dat de Staat dagelijks miljoenen gegevens van onschuldige burgers verzamelt in het kader van een vermeende opsporing van verdachten en voortvluchtigen zonder enige verdenking of enige aanleiding tot verdenking.

<u>Toepassing van Europese rechtspraak op het systeem van artikel 126 JJ SV</u>

7.43 De Grote Kamer heeft in de zaak van Big Brother Watch and Others/VK en in de zaak van Centrum för Rättvisa/ Zweden benadrukt dat ieder onderdeel van een systeem van het systematisch verzamelen, opslaan en verwerken en gebruik van persoonsgegevens moet voldoen aan de toets van het EHRM van de minimumvereisten.

7.44 Het EHRM herhaalt de standaard jurisprudentie ten aanzien van de toets van legaliteit en voorzienbaarheid van de wetgeving voor de burger:

In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements. The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse (see Roman Zakharov, cited above, § 236; see also Kennedy, cited above, § 155).

7.45 Het EHRM somt de minimumvereisten nog eens op voor bulk interception:

In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised and the circumstances in which an individual's communications might be intercepted.

The remaining four minimum safeguards defined by the Court in its previous judgments — that is,

- *that domestic law should set out a limit on the duration of interception,*
- *the procedure to be followed for examining, using, and storing the data obtained,*
- *the precautions to be taken when communicating the data to other parties, and*
- *the circumstances in which intercepted data may or must be erased or destroyed — are equally relevant to bulk interception.*[37]

7.46 Daarbij herhaalt het EHRM nog de minimumvereisten bij opsporing van strafbare feiten en voor zaken van nationale veiligheid[38]:

In this regard it should be reiterated that in its case-law on the interception of communications in criminal investigations, the Court has developed the following minimum requirements that should be set out in law in order to avoid abuses of power:

(v) the nature of offences which may give rise to an interception order.

(vi) a definition of the categories of people liable to have their communications intercepted.

(vii) a limit on the duration of interception.

(viii) the procedure to be followed for examining, using and storing the data obtained;

(ix) the precautions to be taken when communicating the data to other parties; and

(x) the circumstances in which intercepted data may or must be erased or destroyed

(see Huvig, cited above, § 34; Kruslin, cited above, § 35; Valenzuela Contreras, cited above, § 46; Weber and Saravia, cited above, § 95; and

[37] Ro 349 Big Brother and Others/VK

[38] Ro 335 Big Brother Watch and Others/ VK

Association for European Integration and Human Rights and Ekimdzhiev, cited above, § 76).

7.47 Deze aanpak noemt het EHRM de toets van de *"end-to-end safeguards"*

7.48 Toepassing van de test leert dat het systeem van artikel 126 JJ SV is in strijd met de grondrechten van artikel 7,8 en 16 Europees Handvest, artikel 8 EVRM op onder meer de volgende punten:

- Onafhankelijke rechtelijke toetsing ontbreekt op de raadplegingsaanvraag van/namens de officier van justitie en op de werking van het systeem als geheel; het is mogelijk om zonder enige toetsing mondeling gegevens op te vragen, zonder enige schriftelijke bevestiging achteraf; op het ontbreken van de schriftelijk bevestiging staat geen enkele sanctie. Controle achteraf is niet goed mogelijk.
- De status van de originele digitale foto's en de bewerkingen van de foto's voor opslag is niet geregeld, hetgeen misbruik in de hand werkt (hetgeen in praktijk ook al is gebeurd)
- Geen enkele controle op de beweerdelijke vernietiging van de opgeslagen data na afloop van de 4 weken;
- Geen onafhankelijke evaluatie van (de werking van) het systeem van foto tot vernietiging;
- Onvoldoende bescherming tegen het inherente risico van misbruik
- Schending van het voorzienbaarheidsvereiste/legaliteitsvereiste
- Schending van het evenredigheidsvereiste
- Schending van het noodzakelijkheidsvereiste

7.49 Het systeem is ook in strijd met het evenredigheidsvereiste en het noodzakelijkheidsvereiste. Na twee jaren heeft het systeem geleid tot nihil aanhoudingen van voortvluchtigen. Er is geen objectief onafhankelijk bewijs dat het systeem heeft geleid tot opsporing van ook maar 1 concreet ernstig misdrijf.

7.50 Daartegenover registreert het systeem zonder enig onderscheid ten minste 4,5 tot 5 miljoen personen per dag op locaties in Nederland met vermelding van datum en tijd.

7.51 Officieren zijn volgens de WODC-rapporten[39] zelf ook kritisch op het systeem. Het systeem is onder omstandigheden best aardig om te hebben, maar noodzakelijk is het allerminst.

7.52 Liever maken de opsporingsdiensten gebruik van cameraregistraties van commerciële partijen, die het OM dan gewoon kan vorderen zonder verdere verplichtingen.

8. ARTIKEL 126 JJ SV ONVERBINDEND

Belangenafweging in voordeel van Privacy First en de burger in Nederland

8.1 Het systeem van artikel 126 JJ Sv is onverbindend wegens strijd met de grondrechten en het Unierecht.

8.2 De verzameling en opslag van miljoenen digitale foto's en de ongecontroleerde raadpleging en verstrekking van die foto's aan opsporingsambtenaren door de 17 aangestelde collega's vormt een inbreuk op het grondrecht van de bescherming van het privéleven van iedereen die in Nederland in of bij een gefotografeerde auto is.

8.3 Die inbreuk wordt niet gerechtvaardigd door een gammel wettelijk systeem met een gammel computernetwerk dat geen adequate beveiligingen bevat tegen misbruik door de organisatie of buiten de organisatie.

8.4 Het wettelijk systeem van artikel 126 JJ Sv is in strijd met de rechtspraak op het gebied van artikel 8 EVRM en artikel 7 en 8 van het Europees Handvest.

8.5 Het praktisch nut van het systeem is nihil (opsporing van voortvluchtigen) of niet waarneembaar (opsporing van ernstige misdrijven)[40].

8.6 Het systeem van artikel 126 JJ Sv is "nice to have" maar absoluut niet noodzakelijk voor wat dan ook. Aan de vereisten van subsidiariteit en proportionaliteit wordt niet voldaan

8.7 Daarbij komt dat politie en justitie gebruik kunnen maken, en ook maken van alternatieve opsporingsmiddelen die beter aansluiten bij het doel van opsporing, zonder het fotograferen en bewaren van miljoenen burgers per dag, iedere dag weer.

8.8 De Staat heeft voor de opsporing van serieuze misdaden al de toevlucht gezocht tot accuratere, minder belastende maatregelen voor de individuele burger:

- Het opvragen van private camerabeelden ter plaatse van professionele dienstverleners; Justitie hoeft die foto's niet te redigeren voor gebruik

[39] Zie onder meer Pagina's 60-65 en 83 van het WODC-rapport

[40] Zie onder meer pagina 91 samenvatting rapport: de bijdrage aan het onderzoeksproces is moeilijk te bepalen.

- Het gebruik van camerabeelden van andere overheidscamera's die niet onder het wettelijk regime van artikel 126 JJ Sv vallen.

8.9 De afweging van belangen van de Staat valt uit in het voordeel van Privacy First en de burger in Nederland.

8.10 De remedie is simpel: de rechter kan het inefficiënte niet-noodzakelijke, inbreuk makende systeem buiten werking stellen door middel van een ongeclausuleerd verbod op verder verzamelen van de foto's van de kentekens en/ of de verstrekking van de verzamelde gegevens aan de opsporingsdiensten. Met een controle door een onafhankelijke partij op de loggegevens van de databestanden om te bezien of men zich aan het verbod houdt.

8.11 Subsidiair kan de rechter het gebruik van het systeem schorsen of opschorten totdat de Staat aan de belangrijkste bezwaren van Privacy First heeft voldaan opdat de wettelijke inbreuk op de mensenrechten voldoet aan het proportionaliteitsvereiste en het subsidiariteitsvereiste.

8.12 Daarom bepleit Privacy First primair een ongeclausuleerd verbod, subsidiair een schorsing/ opschorting van het systeem totdat de wetgever een aantal waarborgen heeft toegevoegd aan de wet of de besluiten of de regeling waardoor de inbreuk op de mensenrechten van de burger meer gebalanceerd en meer en beter gerechtvaardigd wordt.

9. WEERLEGGING VAN DE VERWEREN VAN DE STAAT

9.1 De Staat heeft in de besprekingen met Privacy First en tijdens het kort geding de volgende kenbare verweren gevoerd:

9.1.1 Het Unierecht is niet van toepassing omdat artikel 126 JJ Sv niet tot het Unierecht behoort;

9.1.2 De uitspraken van het HvJ en van het EHRM over telecommunicatie zaken is niet van toepassing op de massale verzameling van locatiegegevens

9.1.3 De wet voldoet -kort gezegd- wel aan de vereisten van proportionaliteit en subsidiariteit.

9.2 Artikel 126 JJ Sv behoort wel tot het Unierecht. De volgens artikel 126 JJ Sv. opgeslagen gegevens zijn volgens de Staat politiegegevens in de zin van artikel 3 Wet Politiegegevens. Die wet komt voort uit de implementatie van Europese richtlijnen.

9.3 Artikel 126 JJ Sv ziet op de bulkverzameling en bulkopslag van foto’s aangevuld met data- en locatiegegevens en vormt daarmee een rechtstreekse inbreuk op de

privacy van personen, zowel vanwege de kentekenplaten als van de mensen die op de foto zijn te herkennen.

9.4 Niet valt in te zien waarom bescherming tegen deze massale inbreuken een lichtere toets zou moeten doorstaan dan de bulkverzameling en opslag van communicatiegegevens.

9.5 Het HvJ EU heeft in de uitspraak van 5 april 2022 in de zaak C-140/20,van C.D. tegen Commissioner of An Garda Síochána,vMinister for Communications, Energy and Natural Resources, Attorney General,[41] geoordeeld dat het Unierecht (waaronder het EVRM) tegen wettelijke maatregelen die met het oog op de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens. In het onderhavige geval verzamelt de Staat de gegevens niet ter voorkoming van zware criminaliteit of bescherming van nationale veiligheid, maar in een lichter kader van opsporing van voortvluchtigen en misdrijven. Als algemene en ongedifferentieerde bewaring al niet mag binnen het zwaardere kader, dan mag deze vorm van bewaring al helemaal niet in het kader van artikel 126 JJ Sv.

9.6 Hiervoor heeft Privacy First al uitvoerig aangegeven dat en waarom artikel 126 JJ Sv. en de daarop gebaseerde regelgeving niet aan de eigen regels, of aan de vereisten van proportionaliteit en subsidiariteit voldoen.

10. ONTVANKELIJKHEID PRIVACY FIRST

10.1 Privacy First is een Stichting die volgens haar statuten op komt voor het privacybelang van alle burgers in Nederland. Privacy First kan daartoe volgens artikel 3 optreden in rechte. Privacy First is een collectieve belangenorganisatie in de zin van artikel 3:305 a BW.

10.2 Privacy First heeft in een eerder stadium over deze zaak in kort geding gedagvaard. De voorzieningenrechter heeft bij vonnis d.d. 1 december 2021 Privacy First ontvankelijk geacht en de vorderingen van Privacy First afgewezen. De Staat heeft terecht niet betoogd dat Privacy First niet-ontvankelijk zou zijn.

10.3 De ingestelde vorderingen dienen het algemeen belang. Privacy First is ontvankelijk in diens vorderingen.

10.4 Privacy First komt in deze procedure op voor een ideëel doel. Privacy First hoeft op grond van het toepasselijke artikel 3:305a lid 6 BW niet te voldoen aan de per 1 januari 2020 voor financiële collectieve acties aangescherpte ontvankelijkheidseisen, zoals opgenomen in artikel 3:305a lid 2 en lid 5 BW. Eiseres

[41] https://curia.europa.eu/juris/document/document.jsf?text=&docid=257242&pageIndex=0&doclang=NL

vordert geen vergoeding van (massa)schade en heeft geen financieel belang bij deze procedure.

10.5 De bestuurders van eiseres hebben geen winstoogmerk dat via eiseres wordt gerealiseerd. De in dit kort geding ingestelde rechtsvorderingen hebben een nauwe band met de Nederlandse rechtssfeer.

10.6 Op grond van artikel 1018c lid 5 Rv vindt inhoudelijke behandeling van de collectieve vordering slechts plaats als en nadat de rechtbank heeft beslist:

10.6.1 dat de belangenbehartigers voldoen aan de ontvankelijkheidseisen van artikel 3 :305a lid 1 tot en met 3 BW of dat niet aan deze eisen behoeft te worden voldaan op grond van lid 6 van dit artikel;

10.6.2 dat de belangenbehartigers voldoende aannemelijk hebben gemaakt dat het voeren van deze collectieve vordering efficiënter en effectiever is dan het instellen van een individuele vordering, doordat de te beantwoorden feitelijke en rechtsvragen in voldoende mate gemeenschappelijk zijn, het aantal personen tot bescherming van wier belangen de vordering strekt voldoende is en, indien de vordering strekt tot schadevergoeding, dat zij alleen dan wel gezamenlijk een voldoende groot financieel belang hebben

10.6.3 dat niet summierlijk van de ondeugdelijkheid van de collectieve vordering blijkt op het moment waarop het geding aanhangig wordt.

10.7 Aan de tweede uitzonderingsgrond van artikel 3:305a lid 6 BW is voldaan: de vordering dient een ideëel doel. De aard van de vordering geeft geen aanleiding om te toetsen aan de vereisten van de leden 2 en 5 van artikel 3:305a BW.

10.8 Overigens voldoet Privacy First ook aan die vereisten: Zo is Privacy First een stichting met een algemeen bestuur en een raad van advies en heeft zij voldoende middelen om de kosten van de onderhavige procedure te dragen. Op de website van Privacy First is daarnaast informatie beschikbaar over de organisatiestructuur, het beleid, de doelstellingen en werkwijze van Privacy First de stand van zaken in andere lopende procedures. Privacy First heeft ruime ervaring met procederen tegen de Staat.

10.9 Ten slotte geldt dat Privacy First voldoende overleg heeft getracht te voeren.

10.10 Het voeren van een collectieve vordering is in dit geval efficiënter en effectiever dan het instellen van individuele vorderingen, omdat voor iedere persoon in een motorvoertuig met kenteken in Nederland hetzelfde feitelijke kader en dezelfde juridische vragen van toepassing zijn.

10.11 Eiseres zal binnen twee dagen na dagvaarding aantekening daarvan laten maken in het centraal register voor collectieve vorderingen als bedoeld in artikel 1018c lid 2

Rv. Eiseres zendt deze dagvaarding aan het daartoe bestemde emailadres van de Raad voor de Rechtspraak met het verzoek deze in het register aan te tekenen

10.12 Privacy First heeft het standpunt meerdere malen kenbaar gemaakt dat de wet in strijd is met artikel 7 & 8 van het Handvest en artikel 8 van het EVRM. [42]

10.13 Privacy First heeft op 9 januari 2018 overlegd met het Ministerie van Justitie over de bezwaren van Privacy First mede naar aanleiding van een brief van de advocaat van Privacy First aan de minister d.d. 23 november 2017. Het overleg heeft slechts geresulteerd in het uitwisselen van standpunten. Een oplossing werd niet bereikt. Verder heeft Privacy First naar aanleiding van een concept van deze dagvaarding op … november 2023 overlegd. Tot een oplossing heeft dat overleg niet geleid.

10.14 De civiele rechter fungeert ten dezen als restrechter: er bestaat geen adequate rechtsgang bij de bestuursrechter; geen van de handelingen van de staat in de zin van artikel 126 JJ SV en het daarop gebaseerde systeem bevat een voor bezwaar en beroep vatbare handeling. Bovendien wordt iedere automobilist in Nederland door art. 126 JJ SV direct en voortdurend geraakt.

MET CONCLUSIE: Dat de rechtbank bij vonnis, uitvoerbaar bij voorraad:

Primair:

Privacy First aanwijst als Exclusieve Belangenbehartiger met opdracht om het vonnis te laten aantekenen in het centraal register van de collectieve vorderingen

En:

Artikel 126 JJ Sv en de daarop gebaseerde besluiten en regelingen onverbindend verklaart

EN/OF: De Staat verbiedt:

Na 24 uur na betekening van dit vonnis nog enig gegeven toe te voegen aan het databestand (of databestanden) die zijn gebaseerd op artikel 126 JJ Sv en de daarop gebaseerde besluiten en regelingen;

EN/OF

na 24 uur na betekening van het vonnis nog enig gegeven te raadplegen uit het databestand/ de databestanden die zijn gebaseerd op artikel 126 JJ Sv en de daarop gebaseerde besluiten en regelingen;

[42] Onder andere tijdens een deskundigenbijeenkomst met de vaste commissie voor Veiligheid en Justitie van de Eerste Kamer op 20 juni 2017 in het kader van het wetgevingstraject.

Subsidiair

De Staat te verbieden om de kentekengegevens als bedoeld in artikel 126 JJ lid 1 Sv te verzamelen; en/of

De Staat te verbieden om de kentekengegevens als bedoeld in artikel 126 JJ lid 3 Sv en verder te raadplegen, totdat de Staat artikel 126 JJ SV zodanig heeft gewijzigd dat het totale systeem, van het maken van de foto, het bewerken van de foto, het opslaan van de foto, het raadplegen van de gegevens, het verstrekken van de gegevens en de vernietiging van de gegevens onderworpen is aan onafhankelijk toezicht

Met veroordeling van de Staat in de kosten van deze procedure, te vermeerderen met wettelijke rente te rekenen vanaf 21 dagen na datum van het vonnis .

De kosten dezes zij voor mij, deurwaarder €

Privacy First kan de BTW niet verrekenen.

Behandeld door	:	mr. L.J. Böhmer
Correspondentie	:	Postbus 94700 1090 GS Amsterdam
Telefoon	:	+31 30 2121 710
E-mail	:	Leonard.Böhmer@cms-dsb.com